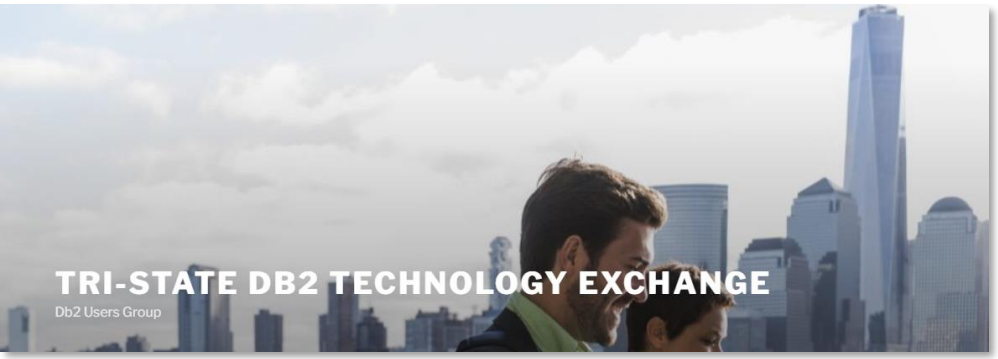
Safeguarding Your Data: A Comprehensive Guide to Db2 for z/OS Security Exit Routines

Emil Kotrc, Vit Gottwald

Broadcom



BROADCOM

Agenda

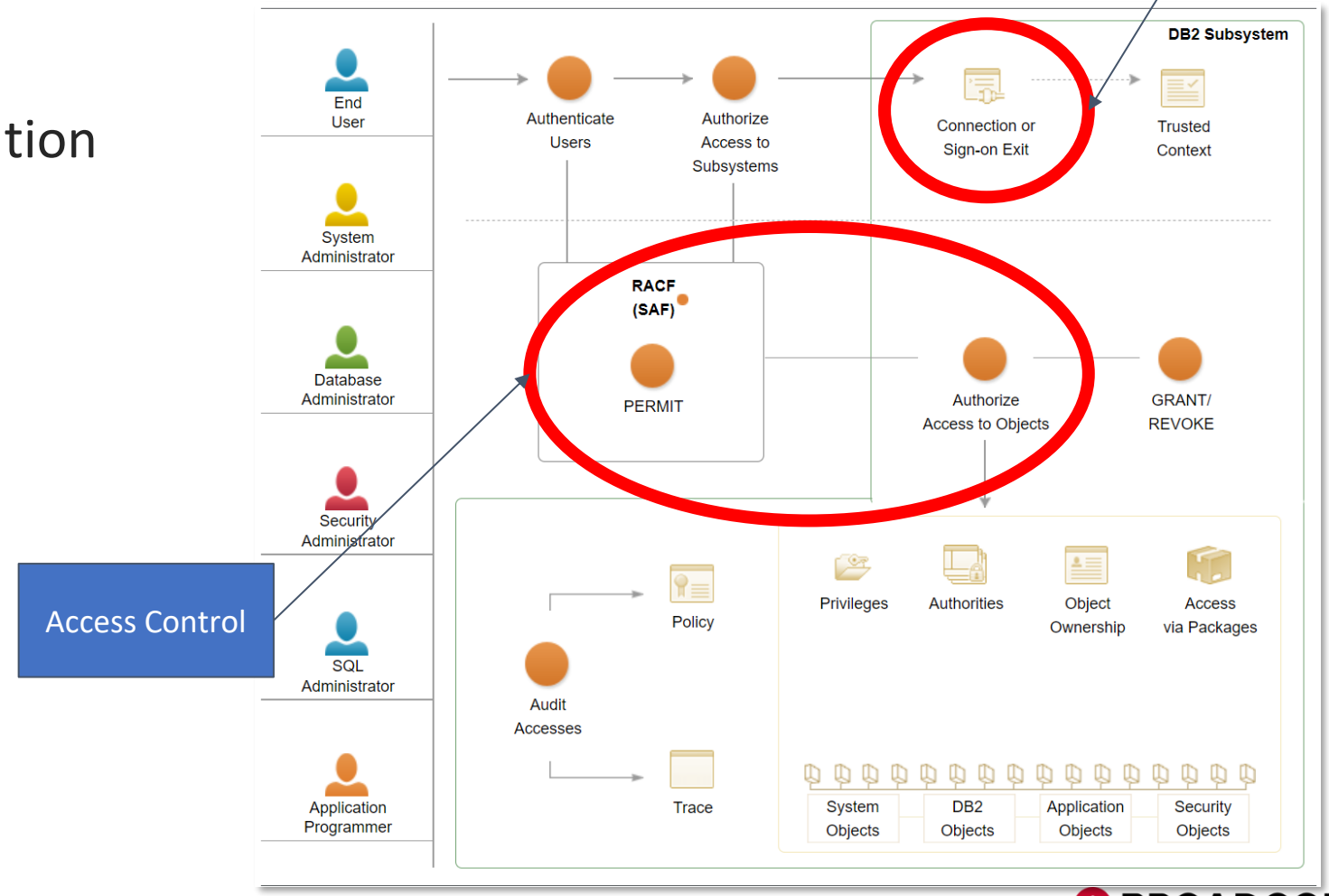
- Db2 Security in a Nutshell
- Db2 Security Exits Basics
- VSCode HLASM Extension
- Db2 Security Exits Deep Dive
  - Connection and Sign-on Exits
  - Access Control Authorization Exit
- Links

Db2 Security in a Nutshell

BROADCOM

Db2 Security in a Nutshell

- https://www.ibm.com/docs/en/db2-for-zos/13?topic=securing-db2
- User **authentication**
  - Identification and verification
- User **authorization**
  - Access to Db2
  - Access to Db2 resources
- Db2 native (**internal**) vs ESM (**external**) security



BROADCOM

Db2 Security in a Nutshell – Basic terms

- **Authentication**
  - Identification and verification of the user id
  - Userid + password, MFA, digital certificates, …
- **Authorization**
  - Permitting or rejecting the access to resources (including Db2 itself)
- **Primary** auth id
  - Identifies a process (usually represents user's authorization ID)
- **Secondary** auth id
  - Collection of associated authorization IDs (typically groups) and can hold additional privileges
- **SQL ID**
  - Privileges that are checked for certain dynamic SQL (DYNAMICRULES Run)
  - **Primary** ID or any of the **secondary** IDs

Db2 Security in a Nutshell – Exits

- Db2 connection/identification (**DSN3@ATH**) and sign-on (**DSN3@SGN**) exits
  - Assignment of values to **primary IDs**, **secondary IDs**, and **SQL IDs**
  - Process depends on the originating environment
  - If you want to use **secondary authorization IDs**, you must replace the default routines with the sample routines, or with routines of your own.
- External Access Control exit (**DSNX@XAC**)
  - Default exit disables external security
  - Authorization checks
  - Permitting or rejecting the access to resources

Connection and Sign-on Exits

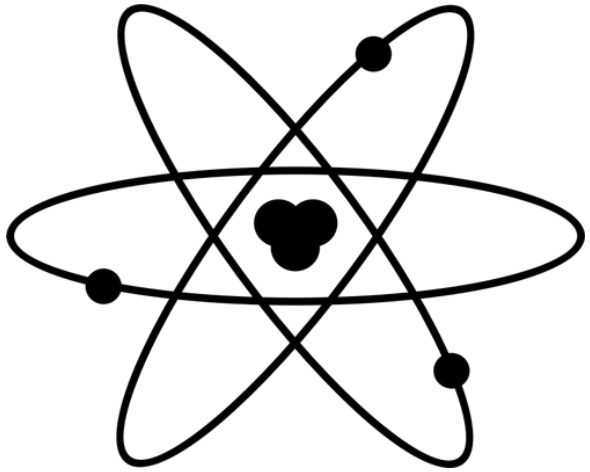
Environment	Connection Exit (DSN3@ATH)	Sign-on Exit (DSN3@SGN)
TSO foreground/background	Yes	No
Batch jobs	Yes	No
Started Tasks	Yes	No
IMS Control Region	Yes	Yes
CICS	Yes	Yes
DL/I batch	Yes	Yes
RRSAF	Yes	Yes
DDF	Yes	Yes
IMS Dependent Region	No	Yes
CICS subtasks	No	Yes
Db2 administrative tasks	No	Yes

Access Control Exit

- Db2 internal vs external security vs no security
  - Database Administrator vs Security Administrator managed security
  - DSNZPARM SECURE=YES
- **Internal** security (Db2 Native)
  - Privileges and roles tracked in the Db2 **catalog**
- **External** security
  - Db2 calls the ESM (External Security Manager) to check the privileges
  - Access control authorization exit routine (**DSNX@XAC**)
  - Default exit disables external security
  - Sample exit **DSNXRXAC**
- Internal and External securities **can be combined!**
  - RC=4 (Unable to determine) from DSNX@XAC -> Internal security takes place

Db2 internal vs external security

	Internal	External
Managed by	Database admin	Security admin
Stored in	Db2 catalog (SYS*AUTH)	Security database
Controls	GRANT, REVOKE	Control statements (PERMIT)
Objects	Db2 objects (Tables, Packages, Tablespaces, …)	Resource classes
Privileges	SELECT, EXECUTE, …	Profile names



Db2 Security Exits Basics

BROADCOM

Db2 Exits – Integrity Considerations

- An exit routine runs as an **extension of Db2**
- Has to reside in an **authorized program library** (APF)
  - SDSNLOAD, SDSNEXIT
- Can only be modified when Db2 is down
- An exit routine has all the **privileges of Db2**
- An exit routine could also **expose the integrity** of z/OS

Db2 Exits – Coding Requirements

- Written in **assembler**
- Must **restore registers** before return
- Must be written to be **reentrant**
- Must be written and link-edited to execute **AMODE(31),RMODE(ANY)**.
- Must **not invoke any Db2 services** (no SQL statements)
- Must **not invoke any SVC services or establish ESTAE** routines.
  - Can establish functional recovery routine (FRR), specifying MODE=FULLXM and EUT=YES
- Samples shipped in **SDSNSAMP**

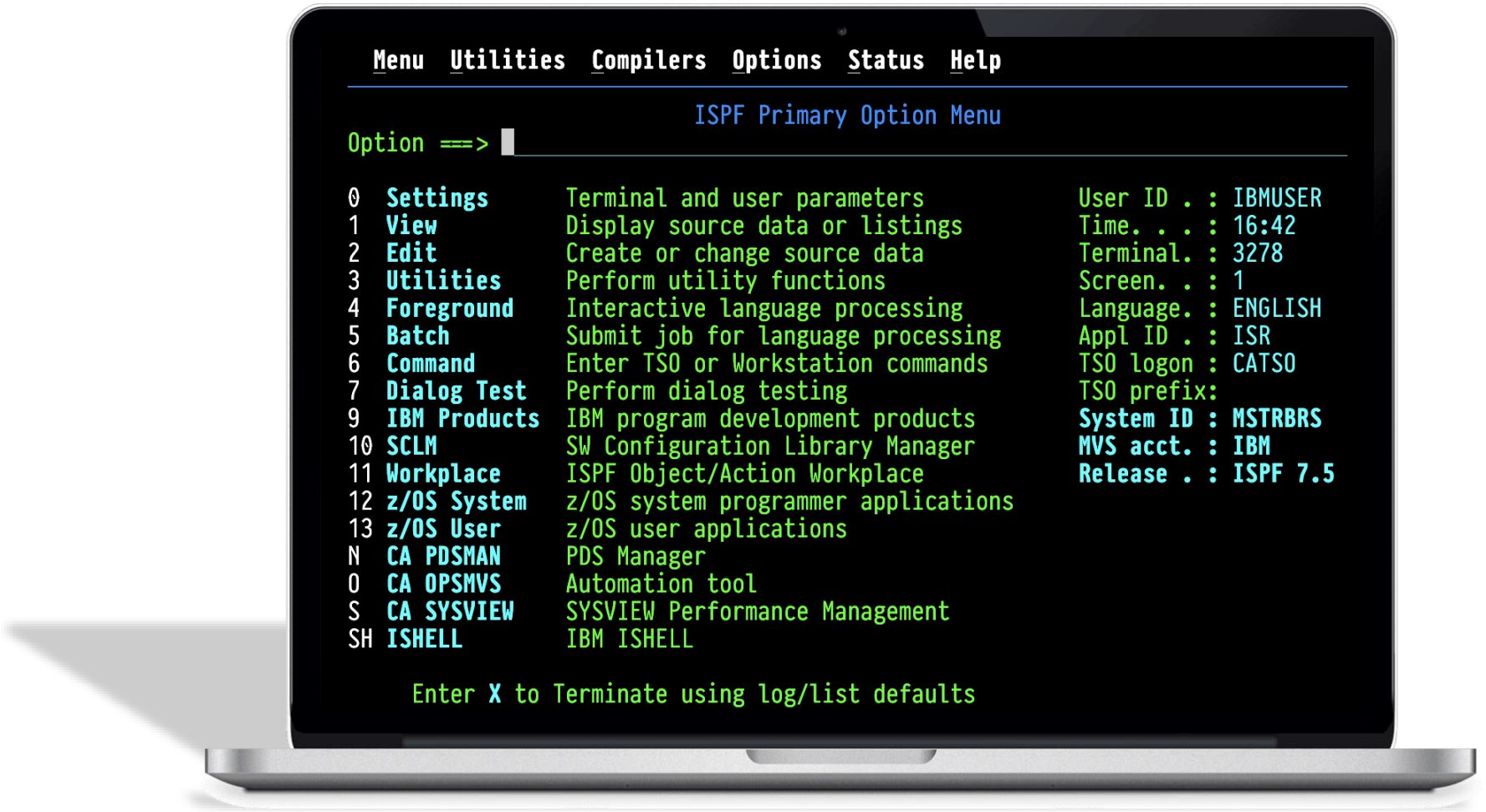
Db2 Exits – Execution Environment

- Invoked by a **standard CALL** (MVS calling convention)
  - For local requests, under the TCB of the application program that requested the Db2 connection
  - For remote requests, under a TCB within the Db2 distributed data facility address space
- **31-bit** addressing mode
- **Supervisor** state
- PSW **key 7**
- **Enabled** for interrupts
- **No MVS locks** held
- There is an **active FRR** established by DB2
- May run in **cross-memory** mode (XAC Routine)

VSCode HLASM Extension

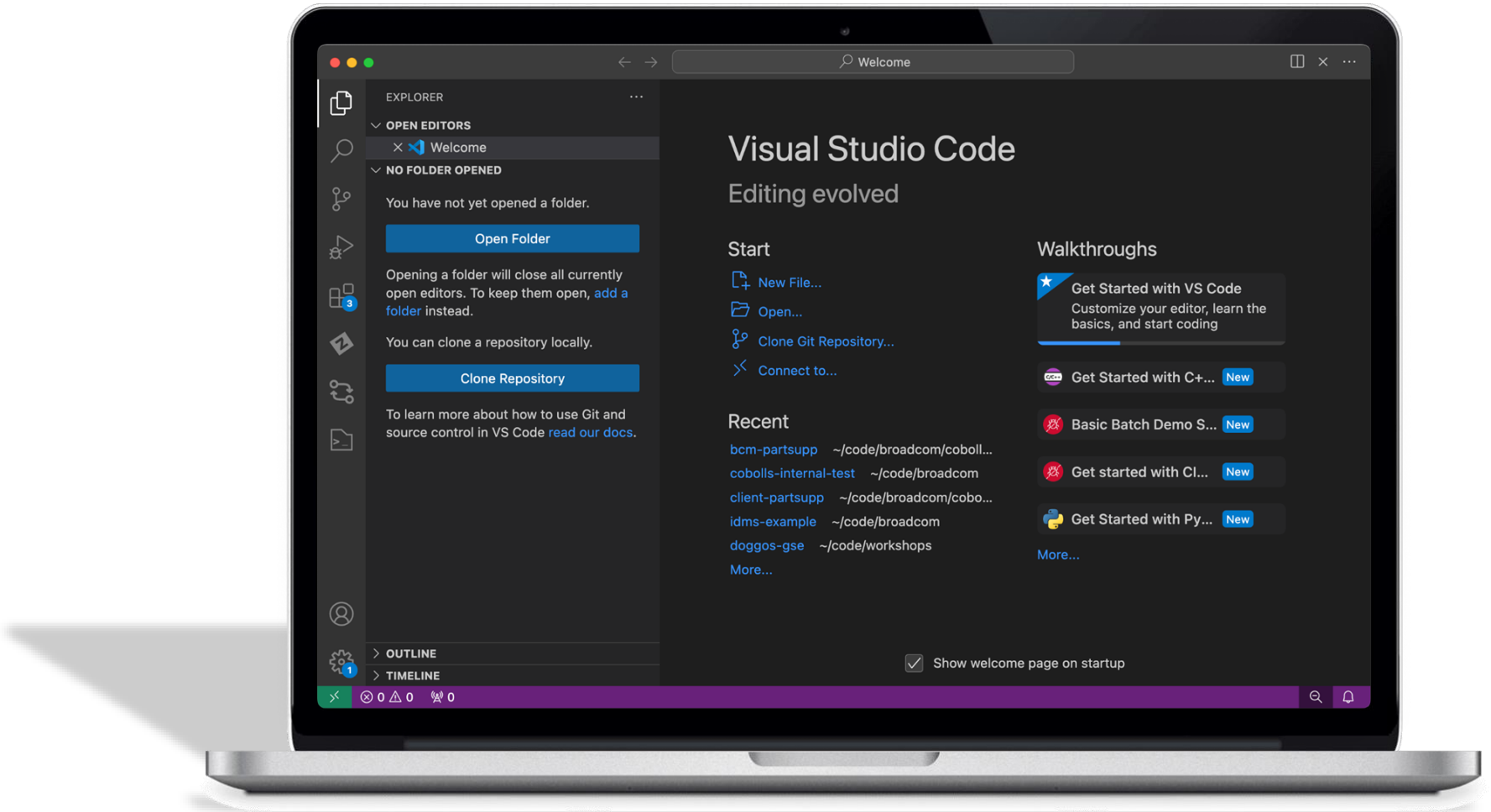
BROADCOM

Mainframers Love 3270 & ISPF



BROADCOM

College Graduates Love VS Code



BROADCOM

Mainframe Extensions for VS Code

https://marketplace.visualstudio.com/search?term=mainframe&target=VSCode&category=All%20categories&sortBy=Relevance

BROADCOM

HLASM Language Support

VS Code Basics

- **Large screen** estate
- Mouse wheel **scrolling**
- Source code **minimap**
- Search using **regular expressions**

Navigation

- Bread crumbs and **outline view**
- Hover and **go to definition**
- Peek and **go to references**

Code Analysis

- Syntax **highlighting**
- **Syntax** checking
- Branch **indicators**
- Macro **tracing**

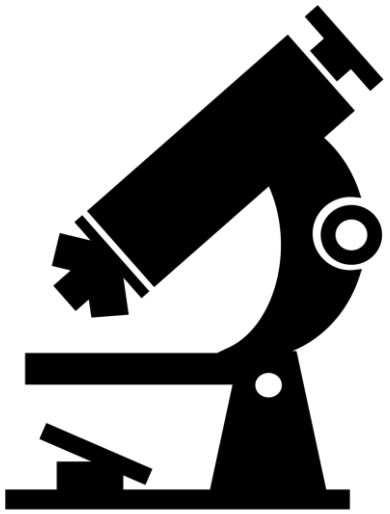
Editing

- Code **snippets**
- **Auto-complete**

Supported Languages: **HLASM** + preprocessors for **Db2** and CICS

BROADCOM

Db2 Connection/Sign-on Exits Deep Dive



BROADCOM

Sample Db2 Connection Exit (DSN3SATH)

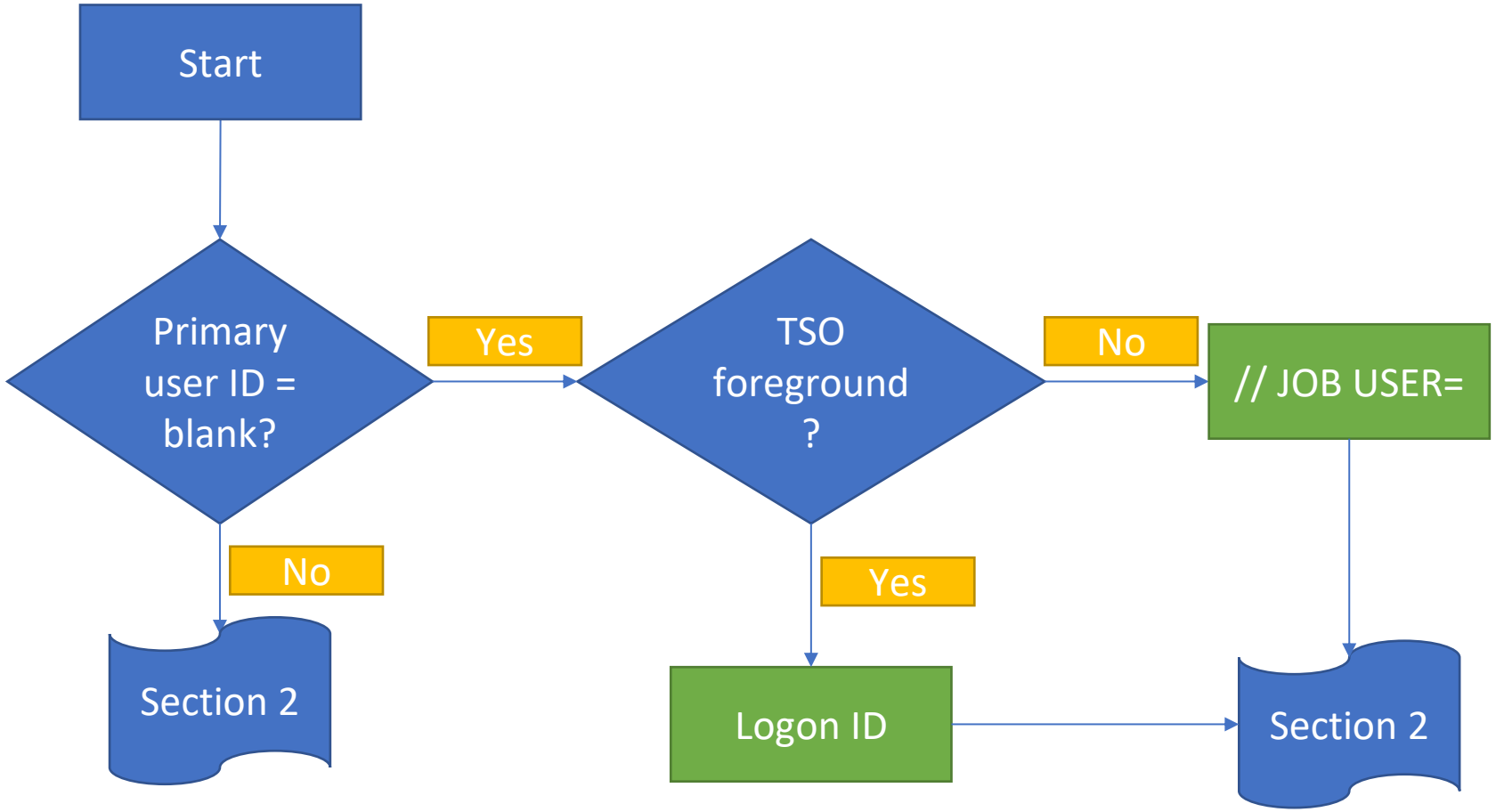
- CSECT **DSN3@ATH**
- **Input** values
  - The initial primary authorization ID
    - Comes from ASXBUSR8 (ATH)
  - The primary user id for a remote request
    - DRDA SECCHK
- **Output** values
  - Primary ID
  - SQL ID
  - List of secondary IDs - not returned from the default exit
    - Up to 1012

Sample Db2 Connection Exit (DSN3SATH)

- Sample connection routine logic
  - 3 sections
  - Plus section 4: set entries in the session variable array
  - No SAF calls
    - But calls for Broadcom ESM

Sample Db2 Connection Exit (DSN3SATH)

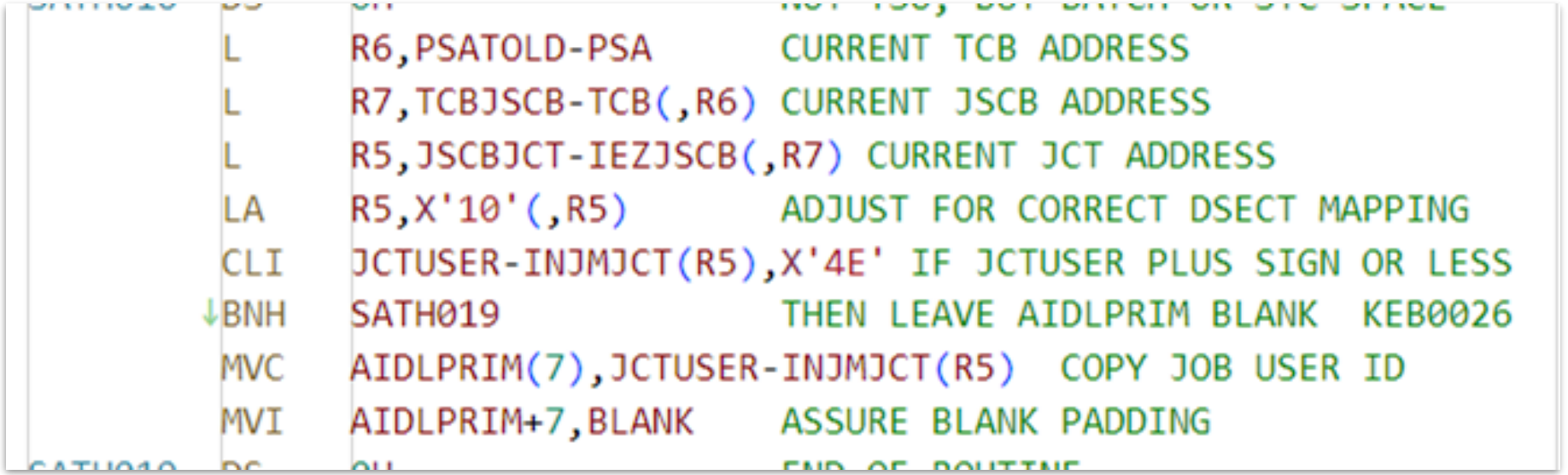
- Section 1:
  - Determine the primary authorization ID



BROADCOM

Sample Db2 Connection Exit (DSN3SATH)

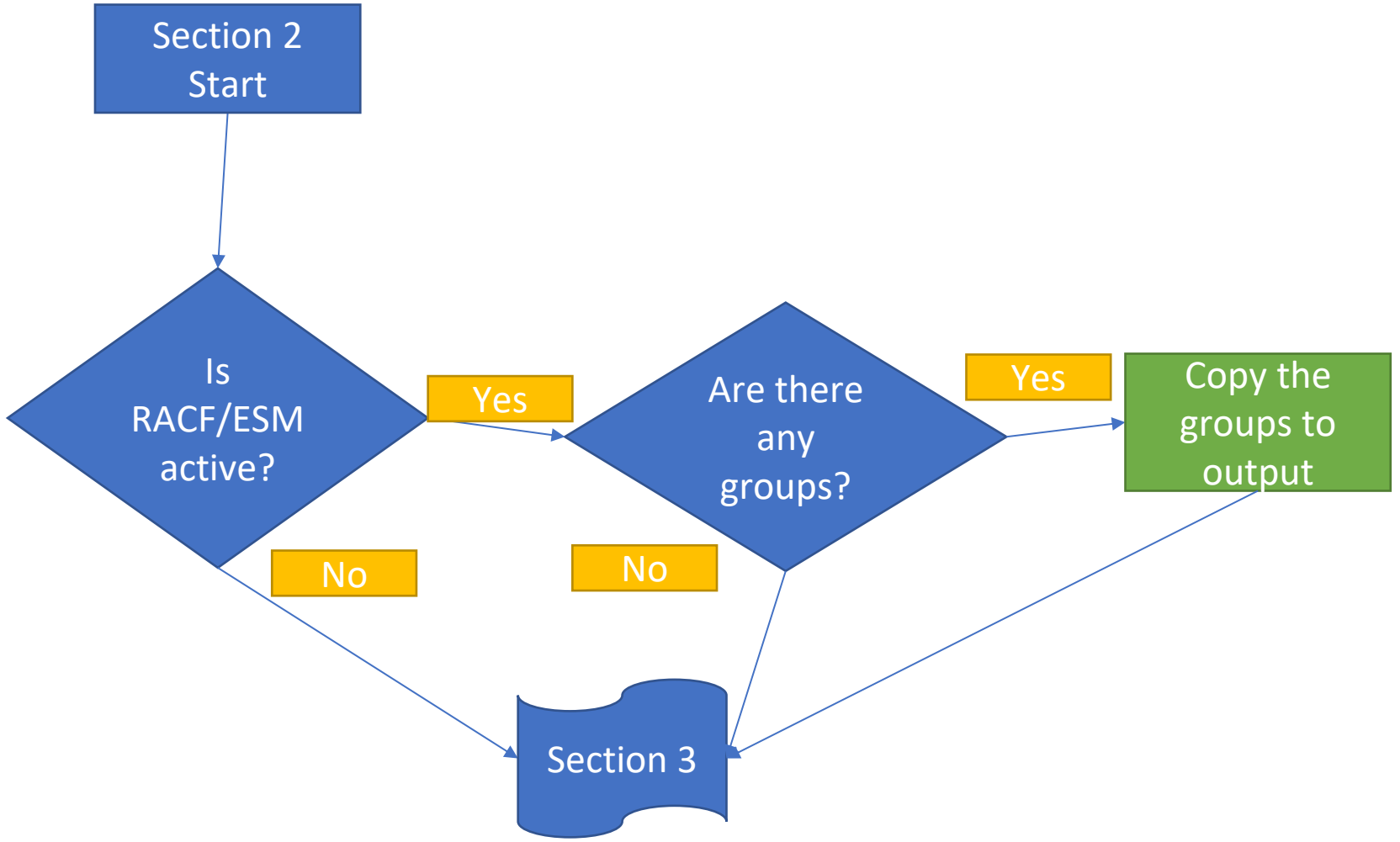
- Section 1 – VSCode sample



```
         L     R6,PSATOLD-PSA       CURRENT TCB ADDRESS
         L     R7,TCBJSCB-TCB(,R6) CURRENT JSCB ADDRESS
         L     R5,JSCBJCT-IEZJSCB(,R7) CURRENT JCT ADDRESS
         LA    R5,X'10'(,R5)        ADJUST FOR CORRECT DSECT MAPPING
         CLI   JCTUSER-INJMJCT(R5),X'4E' IF JCTUSER PLUS SIGN OR LESS
         BNH   SATH019              THEN LEAVE AIDLPRIM BLANK  KEB0026
         MVC   AIDLPRIM(7),JCTUSER-INJMJCT(R5)  COPY JOB USER ID
         MVI   AIDLPRIM+7,BLANK     ASSURE BLANK PADDING
```

Sample Db2 Connection Exit (DSN3SATH)

- Section 2:
  - Determine the list of secondary authorization IDs



BROADCOM

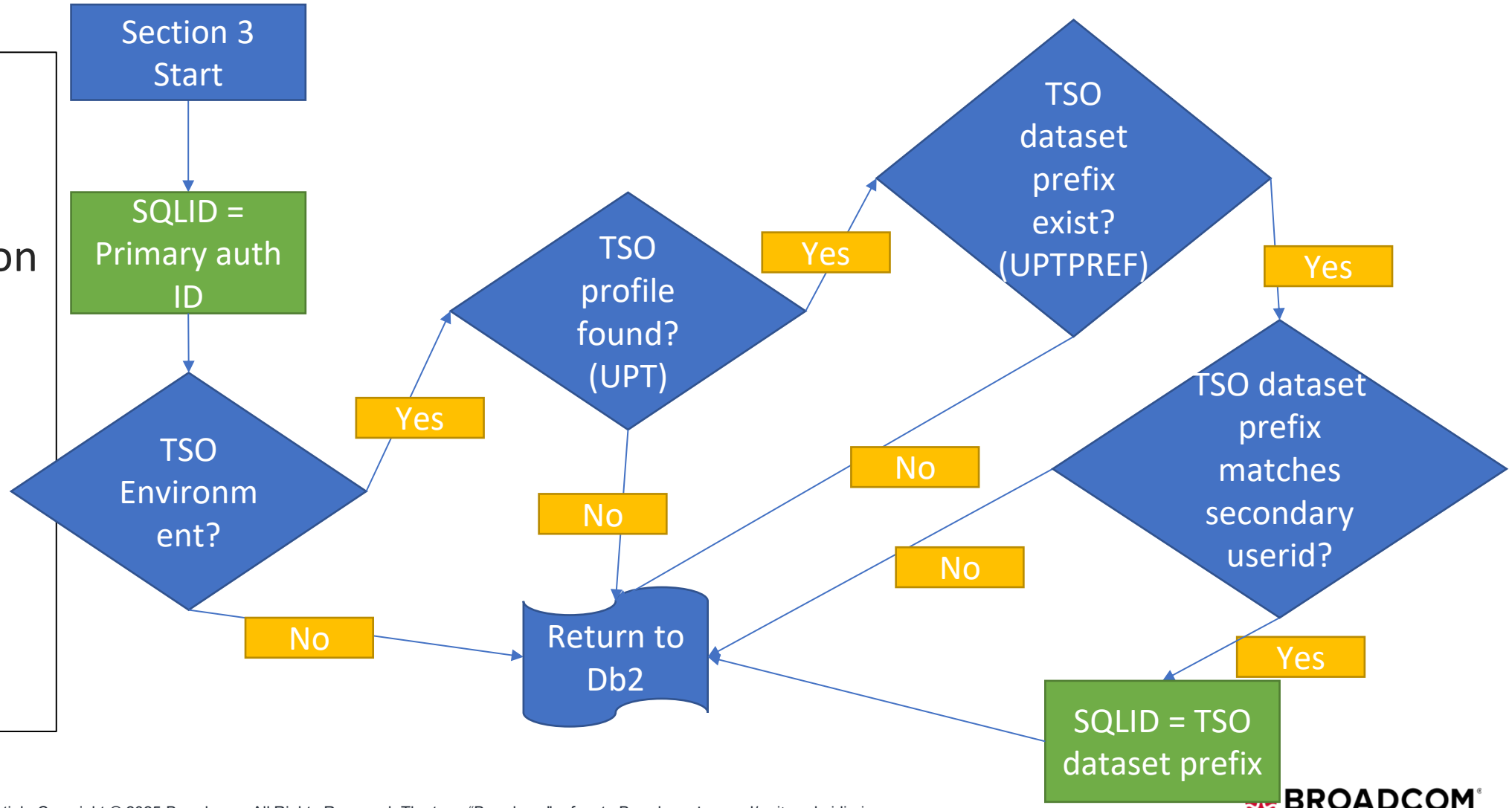
Sample Db2 Connection Exit (DSN3SATH)

- Section 2 – VSCode sample

```
         TM    CGRPNAME,X'BF'          SEE IF THE GROUP IS VALID
         BNM   SATH037                 BR IF NULL, BLANK, OR FF
         MVC   SGRPNAME,CGRPNAME       MOVE THE GROUP NAME
         LA    R4,SGRPNEXT             POINT TO NEXT SECONDARY AUTHID
         CR    R4,R0                   HAVE WE USED ALL THE SLOTS?
         BNL   SATH049                 YES, MOVING IS COMPLETED
SATH037  DS    0H                      BYPASS UPDATING SECONDARY LIST
         SPACE 1
         LA    R2,L'CGRPENT(,R2)       POINT TO NEXT CONNECT GROUP
         BCT   R3,SATH036              BR UNTIL ALL GROUP NAMES EXAMINED
         B     SATH049                 MOVING IS COMPLETED
```

Sample Db2 Connection Exit (DSN3SATH)

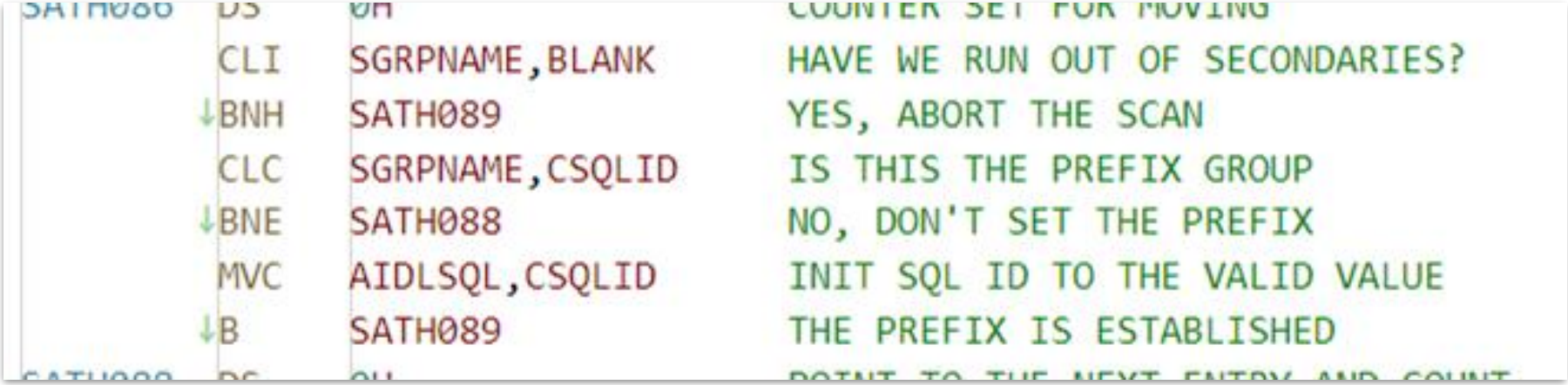
- Section 3:
  - Determine the SQL authorization ID (SQLID)



BROADCOM

Sample Db2 Connection Exit (DSN3SATH)

- Section 3 – VSCode sample



BROADCOM

Sample Db2 Signon Exit (DSN3SSGN)

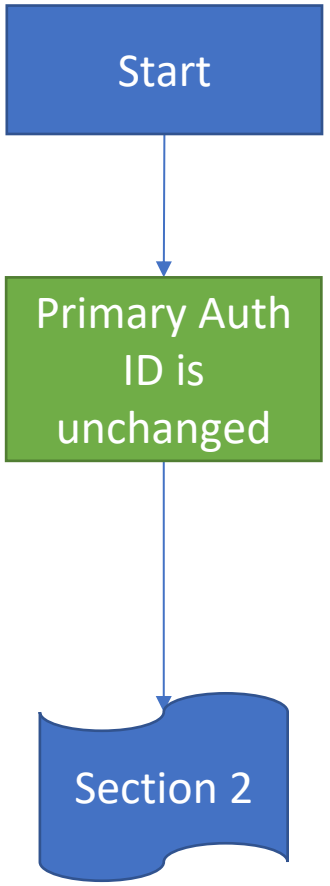
- CSECT **DSN3@SGN**
- **Input** values
  - The initial primary authorization ID
    - Comes from attachment facility (CICS, IMS, RRSAF, DDF)
- **Output** values
  - Primary ID - unchanged
  - SQL ID – set to the primary ID
  - List of secondary IDs - not returned from the default routine
    - Up to 1012
  - EXPLARC = 0: successful completion.
  - EXPLARC =12: access denied by the exit (ACEE not created)

Sample Db2 Signon Exit (DSN3SSGN)

- Sample connection routine logic
  - 3 sections
  - Plus section 4: set entries in the session variable array

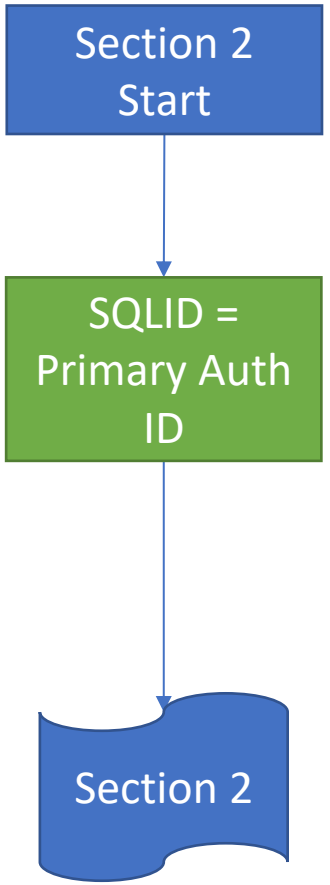
Sample Db2 Signon Exit (DSN3SSGN)

- Section 1:
  - Determine the primary authorization ID



Sample Db2 Signon Exit (DSN3SSGN)

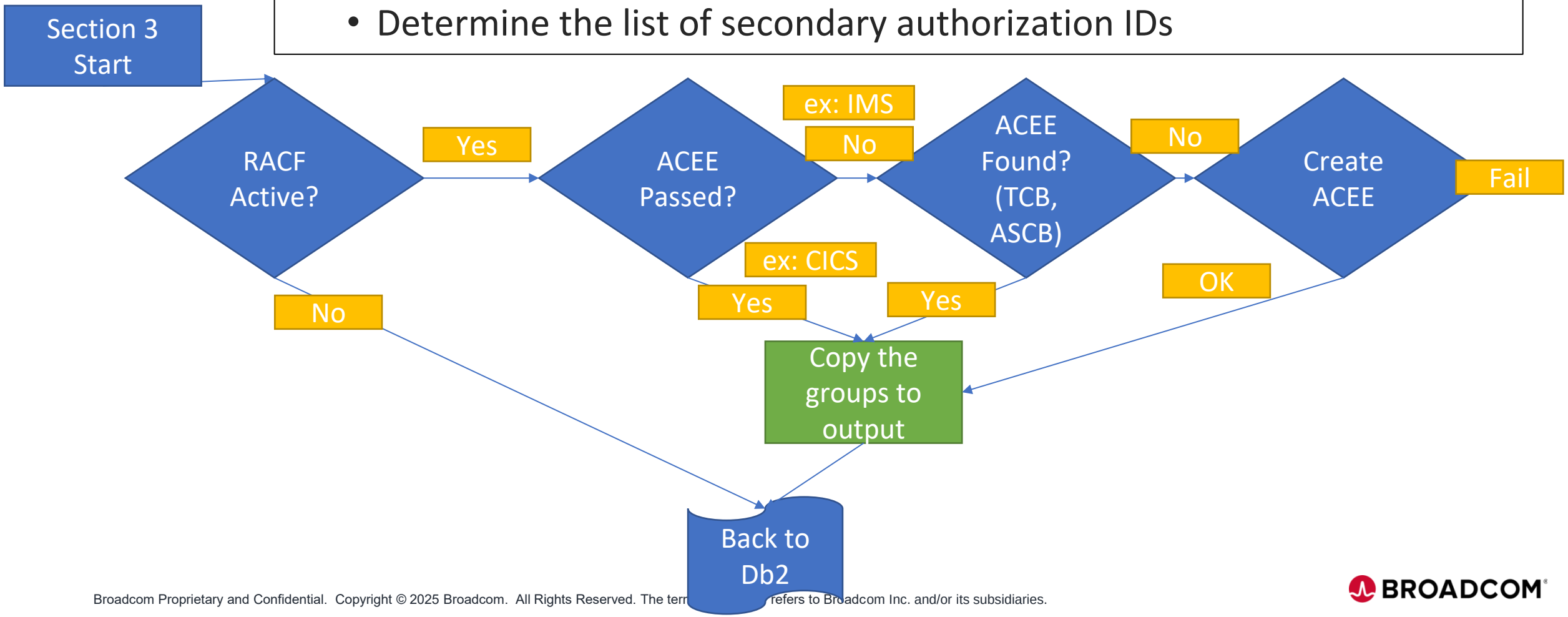
- Section 2:
  - Determine the SQL authorization ID



BROADCOM

Sample Db2 Signon Exit (DSN3SSGN)

- Section 3:
  - Determine the list of secondary authorization IDs



BROADCOM

Sample Db2 Signon Exit (DSN3SSGN)

- Section 3 – VSCode sample

```
SSGN030   DS     0H
          L      R5,CVTPTR              ADDRESS MVS CVT
          L      R7,CVTRAC-CVT(,R5)     RACF CVT ADDRESS
          LTR    R7,R7                  IF RACF CVT ADDRESS ZERO,
          BZ     SSGN090                RACF IS NOT EVEN INSTALLED
          USING  RCVT,R7                SET BASE FOR RACF CVT
          TM     RCVTSTAT,RCVTRNA       IS RACF ACTIVE
          BO     SSGN090                SKIP AROUND IF NOT
```

External Access Control Exit Deep Dive

BROADCOM

Db2 External Security Exit

- Default **DSNXSXAC** (do not use external security)
- or sample **DSNXRXAC** (external security)
- CSECT name **DSNX@XAC**
- 3 types of calls
  - **Initialization** - at Db2 startup
    - If the exit **returns -1** the exit is not called again (DSNXSXAC) - only the internal security will be used
  - **Authorization** - at authorization check
    - Auth call can be **bypassed**, examples:
      - install SYSADM, install SYSOPR
      - Db2 cached the authorization - see **AUTHEXIT_CACHEREFRESH**
  - **Termination** - at Db2 shutdown, cleanup

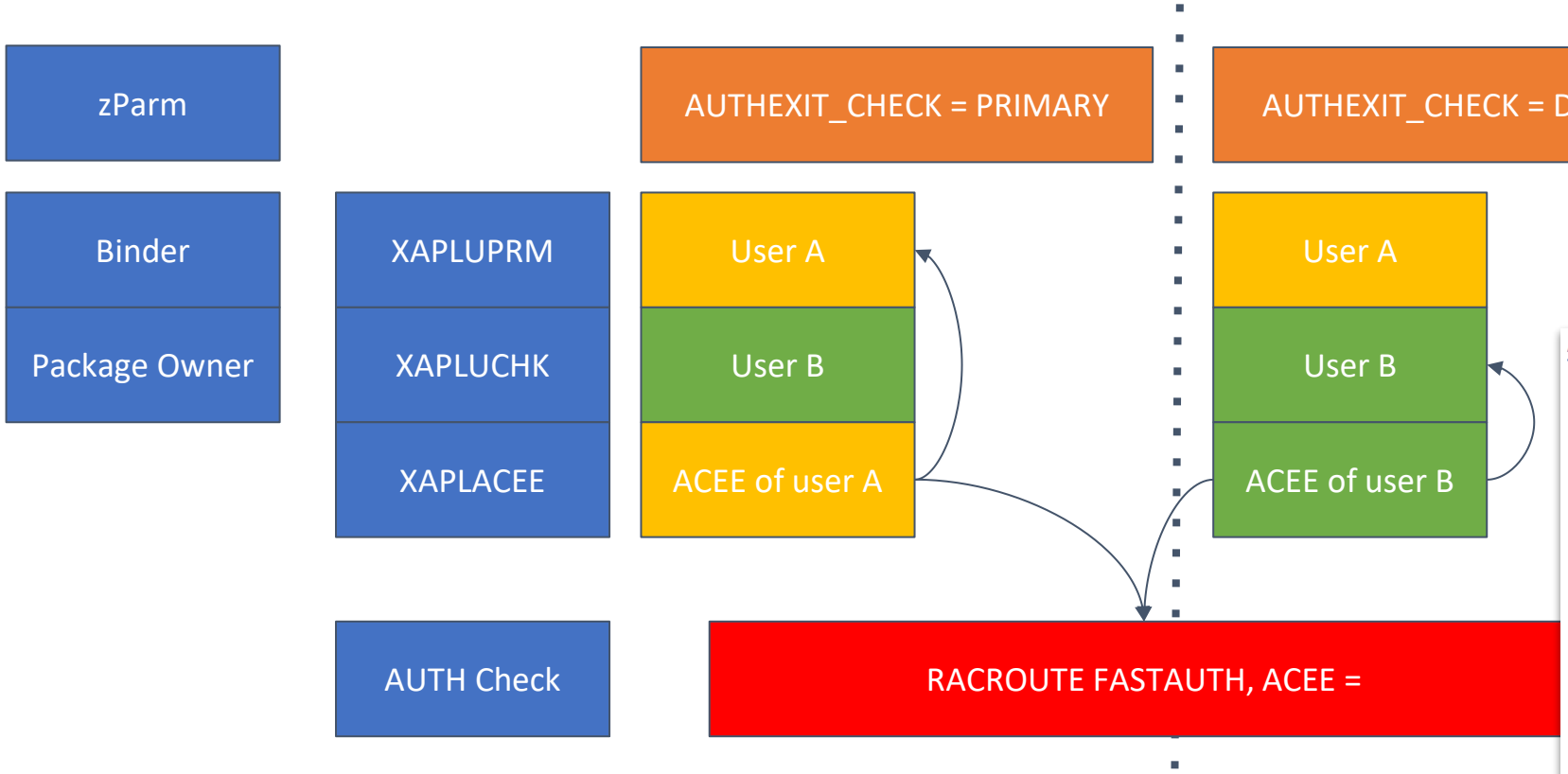
Sample Db2 External Security Exit (DSNXRXAC)

- **Inputs**
  - **User ID** of the requester, ACEE address and STOKEN of the owning address space if not HOME AS
    - identity of the requester (**XAPLUPRM**, XAPLACEE)
    - used for authorization checks
  - **SQL Authorization ID** (primary or secondary) (**XAPLUCHK**)
    - can be used for ownership check
  - Db2 ssid, group
  - Type of object (example: Table)
  - Object name and its qualifier (example: DSN81310.EMP)
  - Privilege being checked (example: SELECT)
  - Control information
- **Outputs** (auth call)
  - RC = 0 - Access allowed
  - RC = 4 - Cannot determine
  - RC = 8 - Access denied

Db2 External Security Exit (DSNXRXAC)

- **User ID** (XAPLUPRM) of the requester and **authorization ID** (XAPLUCHK) may differ!
- **ACEE** (XAPLACEE) is used by the RACROUTE FASTAUTH
- Example: BIND:
  a. BIND check - XAPLUPRM = XAPLUCHK = authorization of the binder
  b. Db2 resource checks in the package -
     - XAPLUPRM - authorization of the binder
     - XAPLUCHK - authorization of the package owner
  c. Which ACEE will be used is controlled by the zParm setting
     - **AUTHEXIT_CHECK = PRIMARY** (default):
       - ACEE associated with XAPLUPRM
     - **AUTHEXIT_CHECK = DB2**:
       - ACEE associated with XAPLUCHK

Db2 External Security Exit (DSNXRXAC) ACEE usage based on AUTHEXIT_CHECK



ACEE heading information

Common name:	Accessor Environment Element (ACEE)
Macro ID:	IHAACEE
DSECT name:	ACEE
Owning component:	Resource Access Control Facility (SC1BN)
Eye-catcher ID:	ACEE (Offset: 0, Length: 4)
Storage attributes:	**Subpool** 255 (or as specified by the issuer of RACROUTE REQUEST=VERIFY) **Key** 0 **Residency** May reside above 16M
Size:	192 bytes (does not include any data pointed to by ACEE)
Created by:	RACF or MVS™'s system authorization facility (SAF), depending on the parameters specified on RACROUTE REQUEST=VERIFY
Pointed to by:	A field supplied by the issuer of RACROUTE REQUEST=VERIFY. Or, for MVS only: ASXBSENV or TCBSENV. ACEEs pointed to by ASXBSENV or TCBSENV always reside below 16M.
Serialization:	See the notes that follow Function.
Function:	Maps the ACEE; represents the authorities of a single accessor in the address space.

BROADCOM

Db2 External Security Exit (DSNXRXAC) AUTH Check logic

- Two methods:
  - **Implicit** Privileges of Ownership
  - **RACF profiles** for Db2 resource
- Logic is **table-driven** - Uses Authority Checking tables:
  - **Privilege Table** - locate the authority checking rules
  - Authority checking **rules**
    - associated with resource table
  - **Resource** table entries define
    - Whether perform an implicit check
    - RACF resource class name
    - RACF resource name
    - typically multiple resources (example: owner, SELECT, DBADM, SQLADM, …)
- Rules/Resources executed in **a loop**
- **Implicit** check is first followed by RACF **RACROUTE** calls

Db2 External Security Exit (DSNXRXAC) Privilege Table, Rules, Resources Example

```
PRIVILEGE PRVCODE=0050,PRVNAME=SELCTAUT,OBJECT=(T,V)
PRIVILEGE PRVCODE=0051,PRVNAME=INSRTAUT,OBJECT=(T,V)
PRIVILEGE PRVCODE=0052,PRVNAME=DELETAUT,OBJECT=(T,V)
PRIVILEGE PRVCODE=0053,PRVNAME=UPDTEAUT,OBJECT=(T,V)
PRIVILEGE PRVCODE=0054,PRVNAME=REFERAUT,OBJECT=(T)
```

Privileges

```
*-------------------------------------------------------------
* SELCTAUT Authority Rules Table
*-------------------------------------------------------------
        RULE  PRIV=(0050),OBJECT=T,
              RES=(OWNER_T,SELECT,DBADM_T,SQLADM,
              SYSDBADM,DATAACCESS,ACCESSCTRL,
              SYSCTRL,SYSADM,SECADM)
*-------------------------------------------------------------
* INSRTAUT Authority Rules Table
*-------------------------------------------------------------
        RULE  PRIV=(0051),OBJECT=T,
              RES=(OWNER_T,INSERT,DBADM_T,SQLADM,
              SYSDBADM,DATAACCESS,ACCESSCTRL,
              SYSCTRL,SECSYSADM,SECADM)
*-------------------------------------------------------------
* DELETAUT Authority Rules Table
*-------------------------------------------------------------
        RULE  PRIV=(0052),OBJECT=T
              RES=(OWNER_T,DELETE,DBADM_T,SQLADM,
              SYSDBADM,DATAACCESS,ACCESSCTRL,
              SYSCTRL,SECSYSADM,SECADM)
```

Rules

```
RESOURCE NAME=OWNER_T,
         OWNER=XAPLOWNR
RESOURCE NAME=OWNER_V,
         OWNER=XAPLOWNR
```

Resources

SELECT … FROM table

SELECT

XAPLPRIV value: **SELCTAUTT**

Privcode 50 (x'32')

Does the user or the role associated with the user own the table?

If so, XAPLUPRM must match the owner name passed from Db2 by the XAPLOWNR parameter when XAPLONRT indicates an authorization ID, or XAPLUCHK must match XAPLOWNR and XAPLUCKT must match XAPLONRT.

If XAPLACAC is enabled (XAPLFLG2 bit 5 is '1'B) and XAPLUCHK is an authid, suppress the ownership check for XAPLUCHK.

If not, the user must have sufficient authority to:

One of these resources:	**In class:**
Db2-subsystem.table-qualifier.table-name.SELECT	MDSNTB or GDSNTB
Db2-subsystem.database-name.DBADM	DSNADM
Db2-subsystem.SQLADM	MDSNSM or GDSNSM

This check is bypassed for user tables.

Db2-subsyste	
This check is	
Db2-subsyste	
Db2-subsyste	
This check is	

```
.*   For Classification Model II (&ClassOpt = 2):
.*
.*    prefix !! &CLASSNMT !! class_abbreviation !! &CHAROPT
.*
.*    where,
.*         prefix             = M (except for ADM class)
.*         &CLASSNMT          = Customer defined class root
.*                              (Default value is 'DSN')
.*         class_abbreviation = two or three character object type
.*                              abbreviation
.*         &CHAROPT           = Customer defined suffix character
.*                              (Ignored if using default &CLASSNMT)
```

Class

BROADCOM

Db2 External Security Exit (DSNXRXAC) RACROUTE calls

```
RACROUTE REQUEST=FASTAUTH,
        WORKA=RACROUTE_worka,
        REQSTOR=XAC,
        SUBSYS=XAPLGPAT,
        DECOUPL=YES,
        WKAREA=FAST_wkarea,
        ENTITYX=FAST_ENTX,
        CLASS=FAST_CLASS,
        ACEE=(R4),
        ACEEALET=(R5),
        ATTR=(R8),
        LOG=NOFAIL,
        MSGSUPP=NO,
        LOGSTR=LOGSTR,
        CRITERIA=(R6),
        AUTHCHKS=CRITONLY,
        RELEASE=7730,
        MF=(E,FASTD)
```

Resource

CLASS

ACEE

Success - audited

```
Active USINGs: STATAREA,R12 XAPL,R3 @DATD,R11 RESENTRY,R10 RCVT,R8
&NAME    RACROUTE &REQUEST=,                                          *
               &REQSTOR=,                                             *
               &SUBSYS=,                                              *
               &WORKA=,                                               *
               &RELATED=,                                             *
               &MF=S,       PARAMS BELOW ARE USED IN FOLLOWING MACROS: *
               &ACCESS=,       DIRAUTH                          @LOA*
               &ACCLVL=,       RACHECK,RACDEF                   @L7A*
               &ACEE=,   RACHK/AUD/DEF/DIR/INIT/LIST/XTRT/TKSRV,FRAC@LOC*
               &ACEEALET=,     FRACHECK,DIRAUTH                 @LOC*
               &ACTINFO=,      RACINIT                                *
               &APPL=,    RACHECK,FRACHECK,RACLIST,RACINIT,SIGNON   @N6C*
RACROUTE REQUEST=FASTAUTH,                                  @L4AX26195940
    WORKA=RACROUTE_worka                                    @L4AX26196030
```


BROADCOM

Db2 External Security Exit (DSNXRXAC) RACROUTE audit failure

- If access not granted, the **first** RACROUTE request with RC 8 is reran and audited with LOG=ASIS

```
RACROUTE REQUEST=FASTAUTH,
         WORKA=RACROUTE_worka,
         REQSTOR=XAC,
         SUBSYS=XAPLGPAT,
         DECOUPL=YES,
         WKAREA=FAST_wkarea,
         ENTITYX=AUDIT_ENTX,
         CLASS=AUDIT_CLASS,
         ACEE=(R4),
         ACEEALET=(R5),
         ATTR=(R8),
         LOG=ASIS,
         LOGSTR=LOGSTR,
         CRITERIA=(R6),
         AUTHCHKS=CRITONLY,
         RELEASE=7730,
         MF=(E,FASTD)
```

ASIS

RACF performs auditing if its authorization check results in success (RC=0) or failure (RC=8), and determines whether auditing is necessary based on the following conditions:

- The user's UAUDIT setting
- The AUDIT, GLOBALAUDIT, and WARNING options in effect for the resource
- If SETR SECLABELAUDIT is in effect, then the AUDIT options in the resource SECLABEL profile
- The pre- or postprocessing installation exit's indication of whether or not to do auditing.

BROADCOM

DSNXRXAC Exit Options

- **&CLASSOPT** - scope
  - 1 – single-subsystem scope
    - **The class names identify with the SSID**, e.g., class name M<ssid>TB1
  - 2 – multiple-subsystem scope, default
    - **Same class is used for all Db2s**; resource name includes the SSID
      - Example: class name MDSNTB, resource name <ssid>.<something>
- **&CLASSNMT** (for &CLASSOPT=2 only) – class name root
  - Default is DSN, e.g., MDSNTB
- **&CHAROPT** (ignored for &CLASSMNT=DSN) – class name suffix
  - Default is 1: M<ssid>TB1
- **&ERROROPT** – error option
  - What to do if exit initialization fails, unexpected return codes during authorization checking, or if # abends exceed "**AUTH EXIT LIMIT**"
  - 1 – fallback to Db2 native auth
  - 2 – stop Db2
- **&PCELLCT, &SCELLCT** – CPOOL primary and secondary cell count

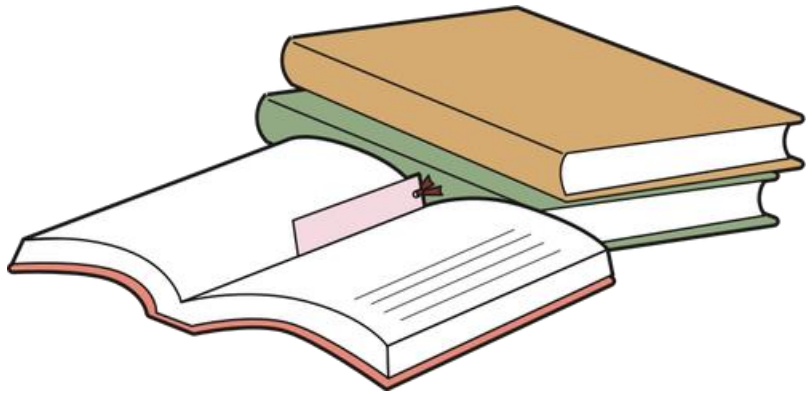
BROADCOM
MAINFRAME SOFTWARE

Broadcom ESM Considerations

Connection, Signon, Authorization Exits

- Obtaining the secondary user IDs in Connection/Sign-On exits
  - **Top Secret** uses samples shipped with Db2
  - **ACF2** ships sample exits
    - **ACF3@ATH**
    - **ACF3@SGN**
- Authorizing the access to Db2 resources
  - The **CAIENF/Db2 Common Service** installs intercepts in Db2 regions
  - Intercepts call Broadcom ESM (**ACF2, Top Secret**) directly for authorizations
  - Authorization exit **CADB2XAC** can be linked as DSNX@XAC
    - Protects against a Db2 subsystem executing without using ESM
    - Validates resource checks for external callers (outside of Db2)
    - Works for both - Top Secret and ACF2
    - Proprietary code. No sample shipped.

Links



BROADCOM

Links

- IBM
  - General guidelines for writing exit routines
  - Connection routines and sign-on routines
  - Access control authorization exit routine
  - Managing security with the RACF access control module
- Broadcom
  - ACF2: Evaluate Use of Exits
  - Top Secret: Evaluate Use of Exits
  - CAIENF/Db2: CAIENF/Db2 Operation
- VS Code
  - Visual Studio Code
  - Mainrame Extensions
    - Db2
    - HLASM
- IDUG
  - SEC02 - Considerations for Migrating Db2 Security to RACF, IDUG NA 2024, Ray Overby, Jørn Thyssen

Thank you

- I hope you enjoyed and had fun ☺

BROADCOM