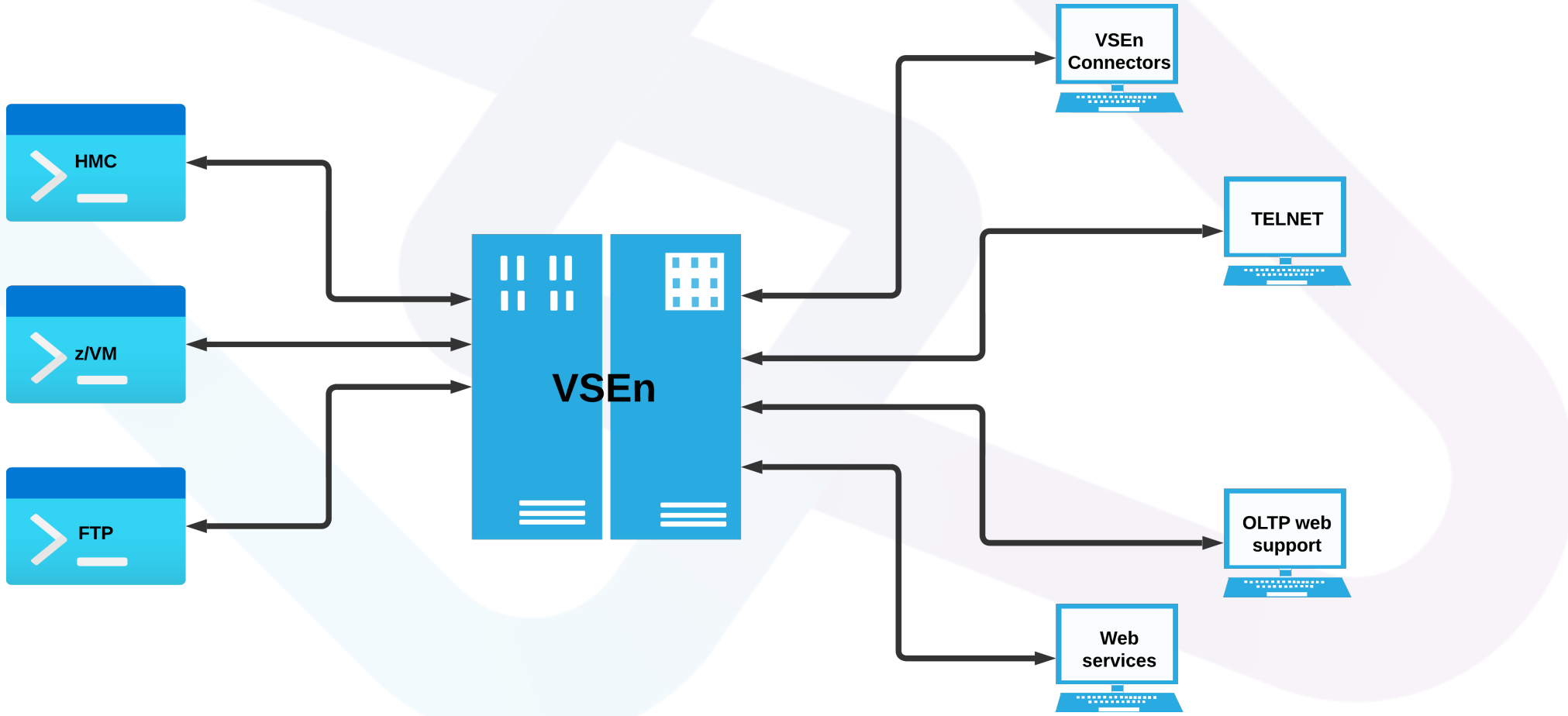
Securing 21CS SMDMU (DITTO) ...the right way

Aleksa Medakovic

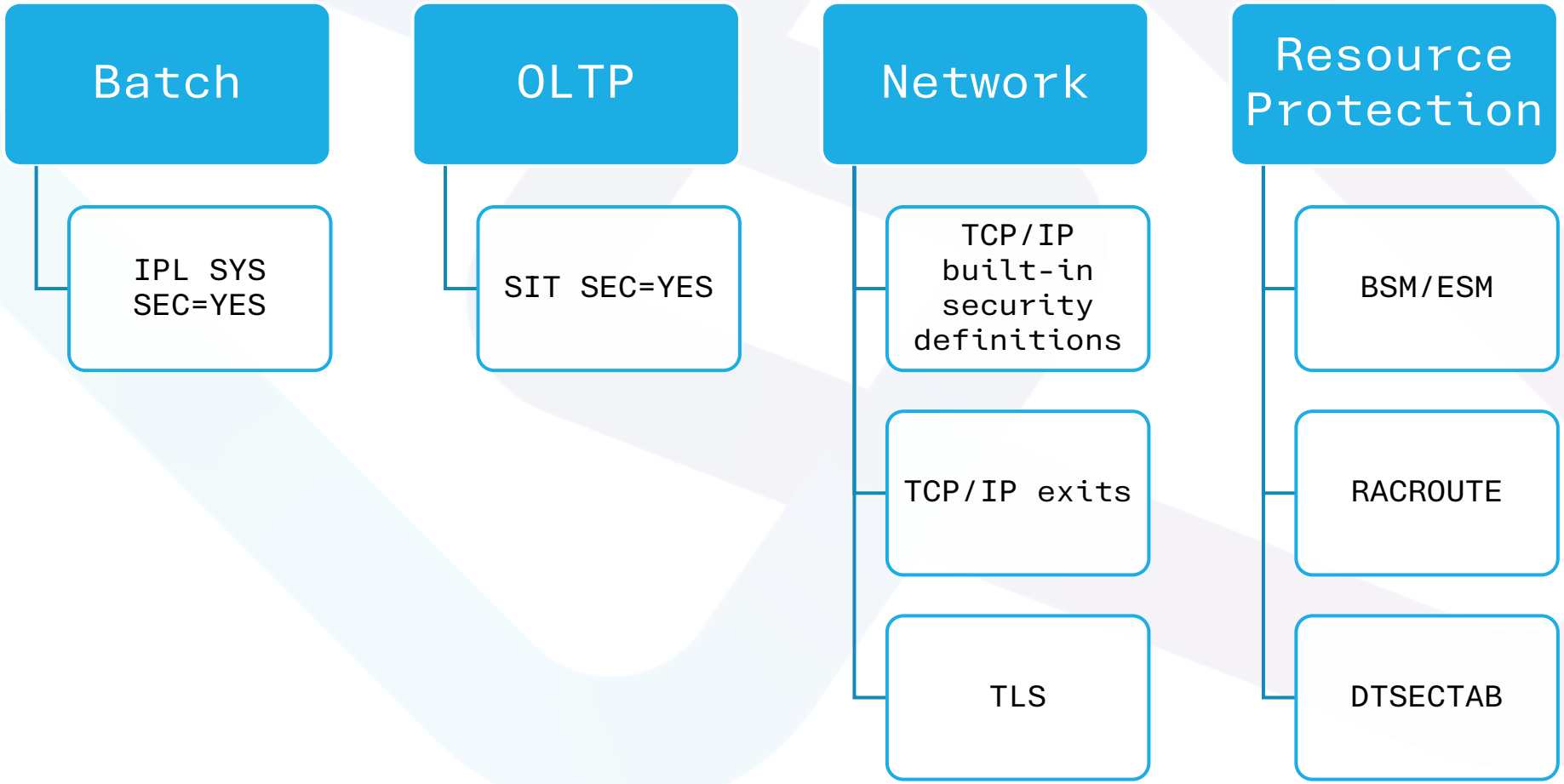
Access Paths to VSEⁿ



VSE^{n} Security Components

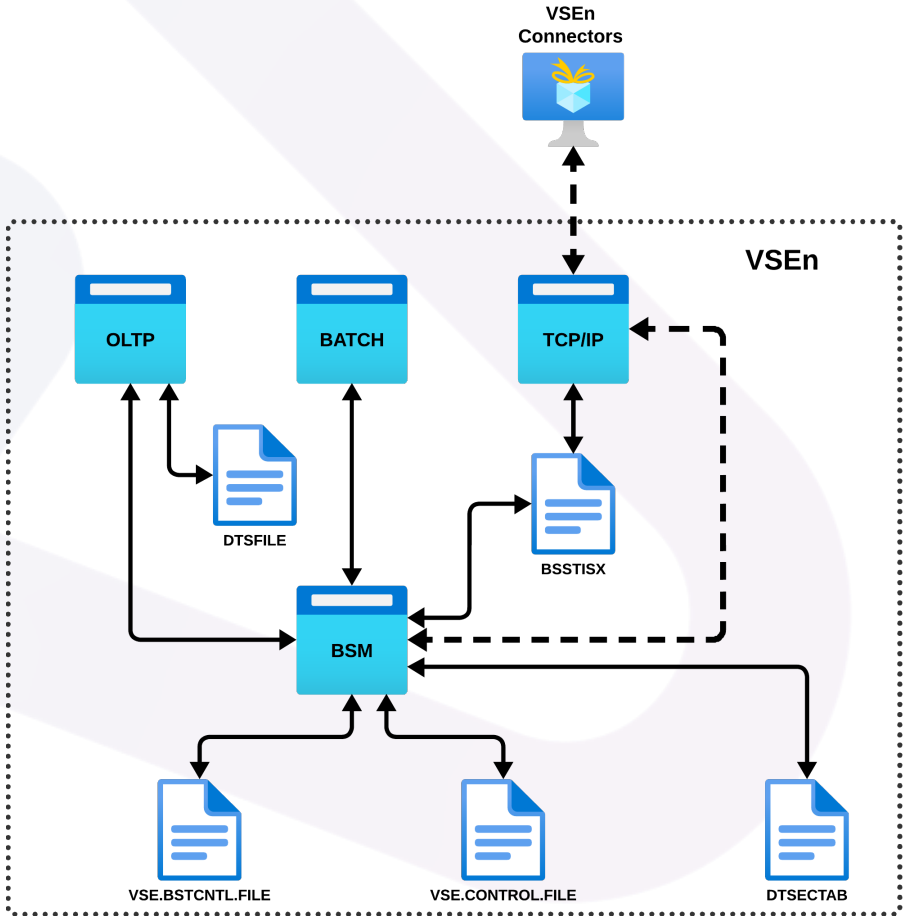
- **Basic Security Manager (BSM)**
- System Authorization Facility (SAF)
- RACROUTE (interface to SAF)
- DTSECTAB
- DTSFILE (ICCF)
- LDAP utilities

How to Secure?



Basic Security Manager (BSM)

- Default Security Manager in VSE^n
- Built to provide basic security functions
- Receives & processes RACROUTE requests from SAF
- Always activated during start, independent of SYS SEC=YES|NO



Batch Security

IPL: SYS SEC=YES

- * $$ JOB JNM=MYJOB,….,SEC=(user,password)
- // ID USER=user,PWD=password
  - User ID & Passwords are verified against
    - DTSECTAB
    - RACROUTE (Security Manager)
- Subsystems like VSAM,LIBR, etc., will use DTSECTAB to verify the access rights
- When submitted from ICCF
  - No need to specify userid or password explicitly (unless required to access a restricted resource)
  - Inherits the userid &* password of the ICCF user

RACROUTE Interface

- External Interface to SAF
- Used by Resource Managers & Subsystems
  - OLTP
  - VSE^n Connector Server
  - SMDMU for VSE^n
  - TCP/IP Security Exits
  - Interactive Interface Sign on

BSM Resource Profiles – Class: FACILITY

JCL

- ❑ IBMVSE.JCL.ASSGN.PERM
- ❑ IBMVSE.JCL.LIBDEF.PERM
- ❑ IBMVSE.JCL.LIBDROP.PERM
- ❑ IBMVSE.JCL.OPTION.PARSTD
- ❑ IBMVSE.JCL.OPTION.STDLABEL

VSAM (IDCAMS)

- ❑ IDCAMS.GENERAL

SMDMU

- ❑ DITTO.DISK.INPUT
- ❑ DITTO.DISK.UPDATE
- ❑ DITTO.FUNCTION.*fn*
- ❑ DITTO.OAM.OUTPUT
- ❑ DITTO.OAM.UPDATE
- ❑ DITTO.OTHER.ALL
- ❑ DITTO.SPOOL.CONTROL
- ❑ DITTO.SPOOL.DISPLAY
- ❑ DITTO.TAPE.DUPLICATE
- ❑ DITTO.TAPE.INPUT
- ❑ DITTO.TAPE.OUTPUT
- ❑ DITTO.TAPE.UPDATE
- ❑ DITTO.VSAM.UPDATE

VSEⁿ MQ

- ❑ MQADMIN
- ❑ MQCMDS
- ❑ MQCONN
- ❑ MQNLIST
- ❑ MQQUEUE
- ❑ MXTOPIC

OLTP

- ❑ TCICSTRN
- ❑ MCICSPPT
- ❑ FCICSFCT
- ❑ JCICSJCT
- ❑ SCICSTST
- ❑ DCICSDCT
- ❑ ACICSPCT
- ❑ SURROGAT

BSTADMIN

- Batch interface to BSM
  - From system console
  - A batch job
- BSM commands:-

Resource Class Management	Group Management	Information Display	Generic Commands
ADD | AD	ADDGROUP | AG	LIST | LI	USERID | ID
CHANGE | CH	CHNGROUP | CG	LISTG | LG	PERFORM | PF
DELETE | DE	DELGROUP | DG	LISTU | LU	
PERMIT | PE	CONNECT | CO	STATUS | ST	
	REMOVE | RE		

Ref: VSEn 6.3 Administration - Chapter 30

Audit-Logging & Reporting

- Access attempts to protected resources can be logged
- Failed logon attempts
- Who accessed what and when
- Summary of logs
- Detailed report of all access attempts
- Logging of BSTADMIN commands
- Logging of DTSECTAB resources

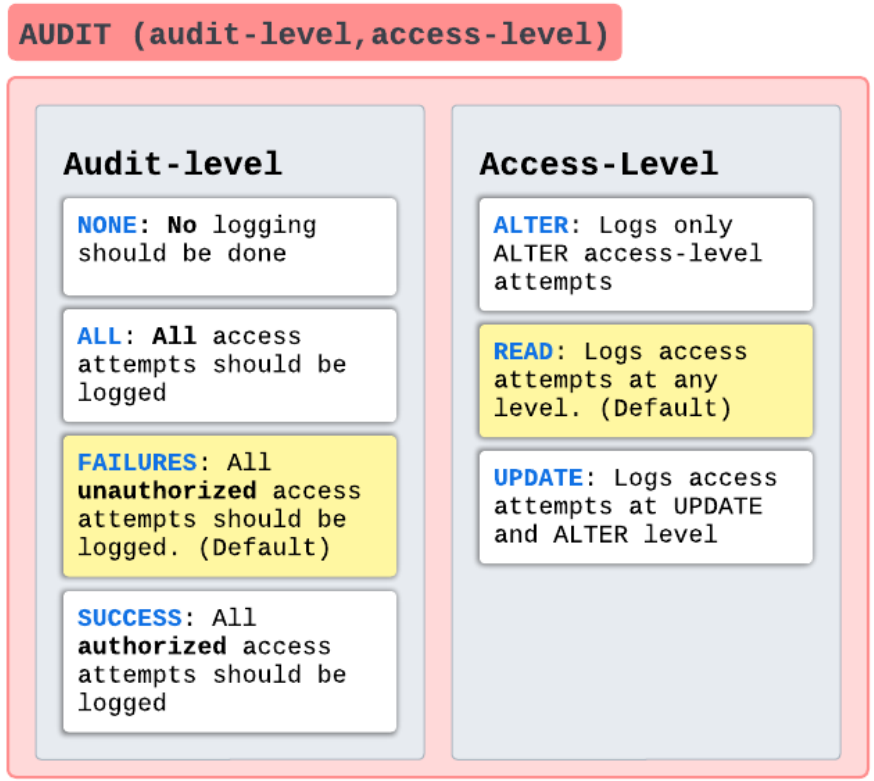
Ref: VSEn 6.3 Administration - Chapter 40

Audit-Logging & Reporting

- The OLTP issues a RACROUTE request each time a user wishes to access a resource.
- The BSM processes these RACROUTE requests and creates SMF80 records.
- The DMF, supplied with the OLTP for VSE^{n}, collects and stores these SMF80 records.
- Use utility DFHDFOU to dump audit records to an intermediate file (SMF80)
- Use utility BSM Report Writer (BSTPRWTR) to create report
  - A detailed listing of the processed records.
  - A summary of the user entries.
  - A summary of the resource entries.
  - A summary of security commands.
  - A general summary.

Audit-Logging & Reporting

- The BSM resource profile should be defined with AUDIT option.

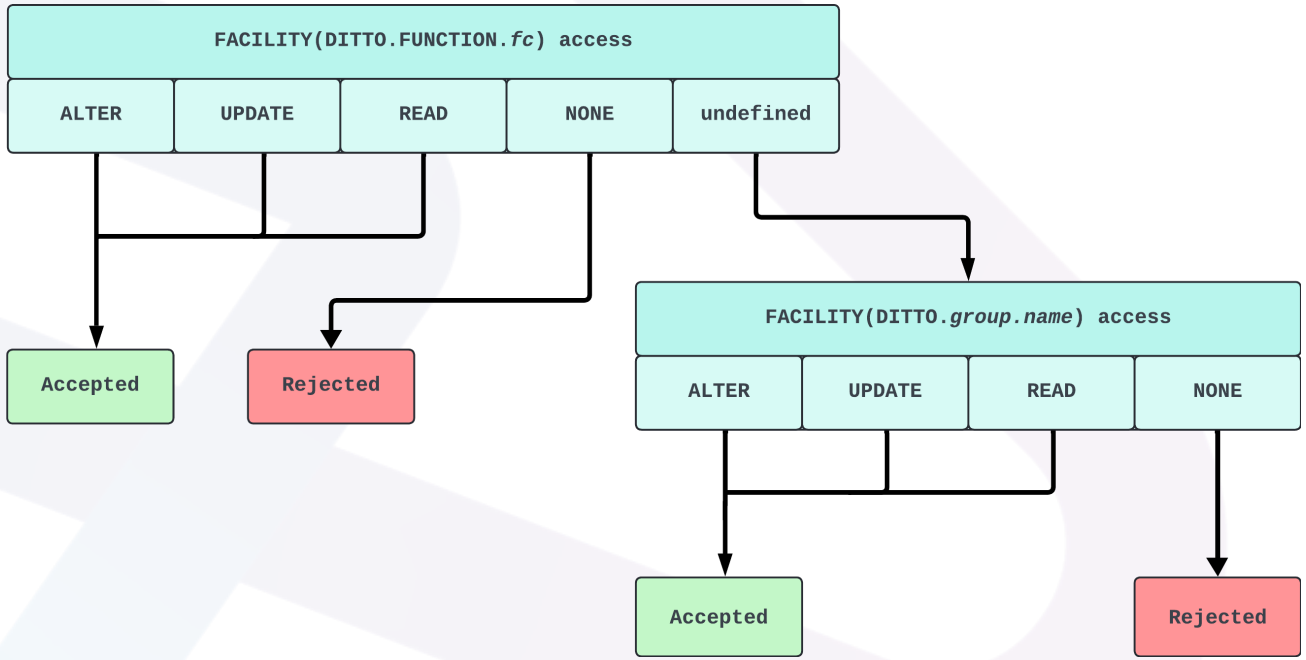


SMDMU Security

- Security either through
  - RACF (or equivalent security product)
  - DITSECUR exit
- SMDMU uses FACILITY profiles to protect resources
  - Ensure that batch security is active.

    IPL SEC=YES
  - Ensure that FACILITY profiles are defined

SAF controls access to SMDMU functions



SMDMU Security

SYS SEC=YES	SYS SEC=NO
SEC=YES;BSM FACILITY class active **BSM profiles used. DITSECUR ignored.**	**SEC=NO;BSM** FACILITY active, DITSECUR assembled with SYSPARM='CICSBSM' **BSM profiles for OLTP sessions. DITSECUR ignored.**
SEC=YES;DITSECUR FACILITY inactive, DITSECUR phase found **Session secured via DITSECUR definitions.**	**SEC=NO;DITSECUR** DITSECUR not assembled with SYSPARM='CICSBSM' **Session secured via DITSECUR definitions.**
SEC=YES;NONE FACILITY inactive, no DITSECUR phase **Session NOT secured.**	**SEC=NO;NONE** No DITSECUR phase found **Functions NOT secured.**

SMDMU Tape Facility Profiles

DITTO.TAPE.INPUT	DITTO.TAPE.OUTPUT
❑ Browse tape data ❑ Print tape data ❑ Locate tape data ❑ Summarize tape contents ❑ Print label summary ❑ Compare two tapes ❑ Print SYSLST Type A/D on tape	❑ Copy to tape (from VSAM, SAM, Library, Terminal input) ❑ Create tape data ❑ Library member copy to tape

DITTO.TAPE.UPDATE	DITTO.TAPE.DUPLICATE
❑ Update tape data ❑ Change tape data ❑ Write tape marks ❑ Initialize tape ❑ Erase tape	❑ Create 1:1 tape copy ❑ Copy single file (change record format) ❑ Copy single file (specify data set name) ❑ Copy multivolume/multiple file tapes

SMDMU Disk & VSAM Facility Profiles

DITTO.DISK.INPUT	DITTO.DISK.UPDATE	DITTO.VSAM.UPDATE
❑ Browse physical disk data	❑ Edit disk track	❑ Edit VSAM data
❑ Print physical disk data	❑ Update physical disk data	❑ Update VSAM data
❑ Locate physical disk data	❑ Change physical disk data	❑ Change VSAM data
❑ Print VTOC entries	❑ Alter VTOC entry	
❑ Show single data set extents	❑ Delete VTOC entry	
	❑ Change disk volume ID	
	❑ Write disk EOF record	

DITTO.OTHER.ALL - General Access (1/2)

1. Browse Data

- ❑ VSAM data
- ❑ Library member
- ❑ POWER list queue
- ❑ AFP data
- ❑ User storage

2. Edit/Update Data

- ❑ Edit library member
- ❑ Update library member

3. Work with VTOC

- ❑ Display Label Area

4. VSAM Catalog

- ❑ List catalog contents
- ❑ Print catalog contents
- ❑ Define catalog entry
- ❑ Alter catalog entry
- ❑ Delete catalog entry

5. Libraries

- ❑ Display status
- ❑ List directory
- ❑ Rename/Delete members
- ❑ Browse/Edit/Print members
- ❑ Copy to VSAM/SAM/Library/SYSPCH
- ❑ Update member
- ❑ Define sublibrary

DITTO.OTHER.ALL - General Access (2/2)

6. Print Data

- ❑ VSAM data
- ❑ SAM data
- ❑ Library member
- ❑ Terminal input
- ❑ SYSLST Type A/B on disk
- ❑ Set DBCS data format for print

7. Copy Data

- ❑ Copy VSAM data (to VSAM/SAM/Library/SYSPCH)
- ❑ Copy SAM data (to VSAM/SAM/Library/SYSPCH)
- ❑ Copy Library member (to VSAM/SAM/Library/SYSPCH)
- ❑ Copy Terminal input (to VSAM/SAM/Library/SYSPCH)

10. Create Data

- ❑ VSAM data
- ❑ SAM data

11. Position a Tape

- ❑ Backspace file
- ❑ Forward space file
- ❑ Backspace record
- ❑ Forward space record
- ❑ Rewind
- ❑ Rewind and unload

Note: Categories 8 (Locate), 9 (Change), and 12 (Tape Specific) use only specialized facility profiles.

Customizing the Security Exit

- 1. Modify DITSECUR.A
- 2. Adapt member DITJOBSC.A. Can be compiled with SYSPARM(VSE)or SYSPARM(CICSBSM)
- 3. Submit DITJOBSC.A
- 4. If previously loaded, reload DITSECUR into SVA

DITSECUR examples

Protect group of faculties from all users

```
DITS CLASS=FACILITY,
     ENTITY=DITTO.DISK.*,
     ACESS=NONE,
     USERID=*,
     ENV=ALL
```

Allow specific function for VMWK user

```
DITS CLASS=FACILITY,
     ENTITY=DITTO.FUNCTION.TB,
     ACESS=READ,
     USERID=VMWK,
     ENV=ALL
```

Allow specific faculty to VMWK user

```
DITS CLASS=FACILITY,
     ENTITY=DITTO.TAPE.OUTPUT,
     ACESS=READ,
     USERID=VMWK,
     ENV=ALL
```

Protect specific faculty from all users

```
DITS CLASS=FACILITY,
     ENTITY=DITTO.TAPE.OUTPUT,
     ACESS=NONE,
     USERID=*,
     ENV=ALL
```

Protect specific function from all users

```
DITS CLASS=FACILITY,
     ENTITY=DITTO.FUNCTION.VE,
     ACESS=NONE,
     USERID=*,
     ENV=ALL
```

Allow all faculties to VMWK user

```
DITS CLASS=FACILITY,
     ENTITY=*,
     ACESS=READ,
     USERID=VMWK,
     ENV=ALL
```

BSTADMIN batch exec

Give access to DITTO.DISK.INPUT facility to all users

```
ADD FACILITY DITTO.DISK.INPUT
UACC(ALTER)
```

Protect DITTO.FUNCTION.TB from all users

```
ADD FACILITY DITT.FUNCTION.TB
UACC(NONE)
```

Protect DITTO.TAPE.OUTPUT facility from all users

```
ADD FACILITY DITTO.DISK.UPDATE
UACC(NONE)
```

Allow DITTO.TAPE.OUTPUT facility to sysa

```
PERMIT DITTO.TAPE.OUTPUT ID(sysa)
ACCESS(UPDATE)
```

Allow DITTO.FUNCTION.VE to sysa user

```
PERMIT DITTO.FUNCTION.VE ID(sysa)
ACCESS(UPDATE)
```

Allow DITTO.TAPE.OUTPUT facility to group01

```
PERMIT DITTO.TAPE.OUTPUT
ID(group01) ACCESS(UPDATE)
```

Give access using IUI

- *Fast path 2819*
- *Protect SMDMU.TAPE.DUPLICATE facility from all users*

```
IESADMBSAE                  MAINTAIN SECURITY PROFILES
BSM RESOURCE CLASS:    FACILITY

Add Profile:

  PREFIX.............                  OLTP region

  RESOURCE NAME......                  Maximum length is 39 characters.
  ........ DITTO.TAPE.DUPLICATE

  GENERIC............ 2                (1=yes, 2=no)

  UNIVERSAL ACCESS... _                (_=None, 2=Read, 3=Update, 4=Alter)

  AUDIT-LEVEL 1 ..... 1                (_=None, 1=Failure, 2=Success, 3=All)
  ACCESS-LEVEL 1 .... 2                (2=Read, 3=Update, 4=Alter, _=default)

  AUDIT-LEVEL 2 .....                  (_=None, 1=Failure, 2=Success, 3=All)
  ACCESS-LEVEL 2 ....                  (2=Read, 3=Update, 4=Alter, _=default)
  DESCRIPTION........                      Optional remark
PF1=HELP                    3=END                       5=UPDATE
```

Give access to DITTO.OTHER.ALL facility to all users

```
IESADMBSAE                  MAINTAIN SECURITY PROFILES
BSM RESOURCE CLASS:    FACILITY

Add Profile:

  PREFIX.............                  OLTP region

  RESOURCE NAME......                  Maximum length is 39 characters.
  ........ DITTO.OTHER.ALL

  GENERIC............ 2                (1=yes, 2=no)

  UNIVERSAL ACCESS... 4                (_=None, 2=Read, 3=Update, 4=Alter)

  AUDIT-LEVEL 1 ..... 1                (_=None, 1=Failure, 2=Success, 3=All)
  ACCESS-LEVEL 1 .... 2                (2=Read, 3=Update, 4=Alter, _=default)

  AUDIT-LEVEL 2 .....                  (_=None, 1=Failure, 2=Success, 3=All)
  ACCESS-LEVEL 2 ....                  (2=Read, 3=Update, 4=Alter, _=default)
  DESCRIPTION........                      Optional remark
PF1=HELP                    3=END                       5=UPDATE
```

Specific user

```
_       DFHRCF.RSL24
6       DITTO.TAPE.DUPLICATE
_       IBMVSE.JCL.ASSGN.PERM
```

sysa can access
DITTO.TAPE.DUPLICATE

```
IESADMBSAA                                  MAINTAIN A
BSM CLASS:  FACILITY
PROFILE:    DITTO.TAPE.DUPLICATE

Add Userid or Groupid:

  NAME.............. sysa

  ACCESS............ 4
```

sysa can‘t access
DITTO.TAPE.DUPLICATE

```
IESADMBSAA                        MAINTAIN ACCESS LIST
BSM CLASS:  FACILITY
PROFILE:    DITTO.TAPE.DUPLICATE

Add Userid or Groupid:

  NAME.............. sysa_              Userid or Groupid

  ACCESS............ _                  (_=None,
                                         2=Read, 3=Update, 4=Alter)
```

APAR VA00135

is required (VSEn 6.3.0 and 6.3.1)

Thank You