8.1 SECURING CICS

The System Initialisation Table has many options that affect security

Some affect the whole security environment

Some affect individual resources

Care should be taken as to which ones to include

8.1 SECURING CICS

Options that affect the whole CICS system :

- SEC
- SECPRFX
- DFLTUSER
- RESSEC

8.1 SECURING CICS

```
ACTIVE CLASSES = DATASET USER GROUP ACCTNUM
ACICSPCT BCICSPCT CBIND CCICSCMD
                  DCICSDCT DSNR ECICSDCT
FACILITY FCICSFCT GCICSTRN GXFACILI
                  HCICSFCT JCICSJCT KCICSJCT
LOGSTRM MCICSPPT NCICSPPT
                  PCICSPSB PTKTDATA PTKTVAL
QCICSPSB RCICSRES SCICSTST
                  SERVER STARTED SURROGAT
TCICSTRN TSOAUTH TSOPROC UCICSTST
                  VCICSCMD WCICSRES XFACILIT
```

8.1 SECURING CICS

For transactions that are Attached :

XTRAN

TCICSTRN GCICSTRN

A user Classname can be defined but must be in the RACF User Class Descriptor Table

8.1 SECURING CICS

For DL1 PSBs

XPSB

PCICSPSB QCICSPSB

For Transient Data Queues

XDCT

DCICSDCT ECICSDCT

8.1 SECURING CICS

For File Control Table entries

XFCT

FCICSFCT HCICSFCT

For Journal Control Table entries

XJCT

JCICSJCT KCICSJCT

8.1 SECURING CICS

For Transactions that are Started

XPCT

ACICSPCT BCICSPCT

For Programs and Mapsets

XPPT

MCICSPPT NCICSPPT

8.1 SECURING CICS

For Temporary Storage Queues

XTST

SCICSTST UCICSTST

For Session security with Binding LUTYPE6.2 sessions

XAPPC

XCMD For Command Security

CCICSCMD VCICSCMD

8.1 SECURING CICS

For Document Templates Resources

XRES

RCICSRES WCICSRES

8.1 SECURING CICS

Access to the CICS Application during Logon

The Applid needs to be defined in the APPL Class

All Users need READ access in order to Logon

VTAMAPPL allows CICS to open the VTAM ACB

8.1 SECURING CICS

During Logon CICS will invoke the Good Morning Transaction

CSGM is the default

CESN is provided for Signon

CESF is provided for Signoff

CICS DFLTUSER is assigned to every terminal before signon

8.1 SECURING CICS

Access to the Terminal is provided by :

TERMINAL GTERMINL

System wide TERMINAL (READ)

CICS does not restrict logon and signon

8.2 PROTECTING CICS TRANSACTIONS

Protecting CICS resources requires definitions to be made to RACF

RACF command RDEFINE is used to define transactions to either :

TCICSTRN GCICSTRN

The PERMIT command allows the group or User access

8.3 RESOURCE LEVEL SECURITY

Lower level resources can be protected

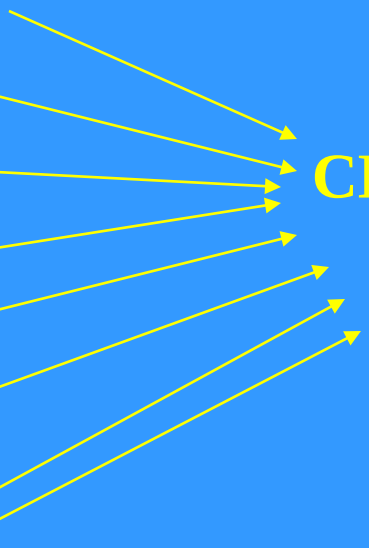
The Transaction definition must specify RESSEC = YES

The appropriate resource Class is checked for access to that resource

Access to Files or any resource is controlled by the RDEFINE/PERMIT commands

8.3 RESOURCE LEVEL SECURITY

- XTRAN = YES
- XDCT = YES
- XFCT = YES
- XPCT = YES
- XPPT = YES
- XPSB = YES
- XRES = YES
- XTST = YES



CHECKED BY RACF

8.4 PROGRAM LIST TABLE SECURITY PROCESSING

Programs that execute in the PLTPI need consideration

These options are specified in the SIT :

- PLTPIUSR

- PLTPISEC

The shutdown PLT programs run under the authority of the shutdown transaction

8.5 THE CICS/RACF SEGMENT

The CICS segment in the RACF Userid allows individual users to be assigned their own operational properties :

- **OPCLASS**
- **OPIDENT**
- **OPPRTY**
- **TIMEOUT**
- **SIGNOFF**

8.6 THE QUERY SECURITY COMMAND

CICS API supports the QUERY SECURITY command

Can check on resources defined to CICS :

- Resources in CICS Resources Classes
- Resources in User-Defined Resource Classes

8.6 THE QUERY SECURITY COMMAND

```
EXEC CICS QUERY SECURITY
        < RESTYPE(data-value) |
        RESCLASS)data-value) |
        RESIDLENGTH(data-value) >
        RESID(data-value)
        < LOGMESSAGE(cvda) | LOG | NOLOG >
        < ALTER(cvda) >
        < CONTROL(cvda) >
        < READ(cvda) >
        < UPDATE(cvda) >

END-EXEC.
```

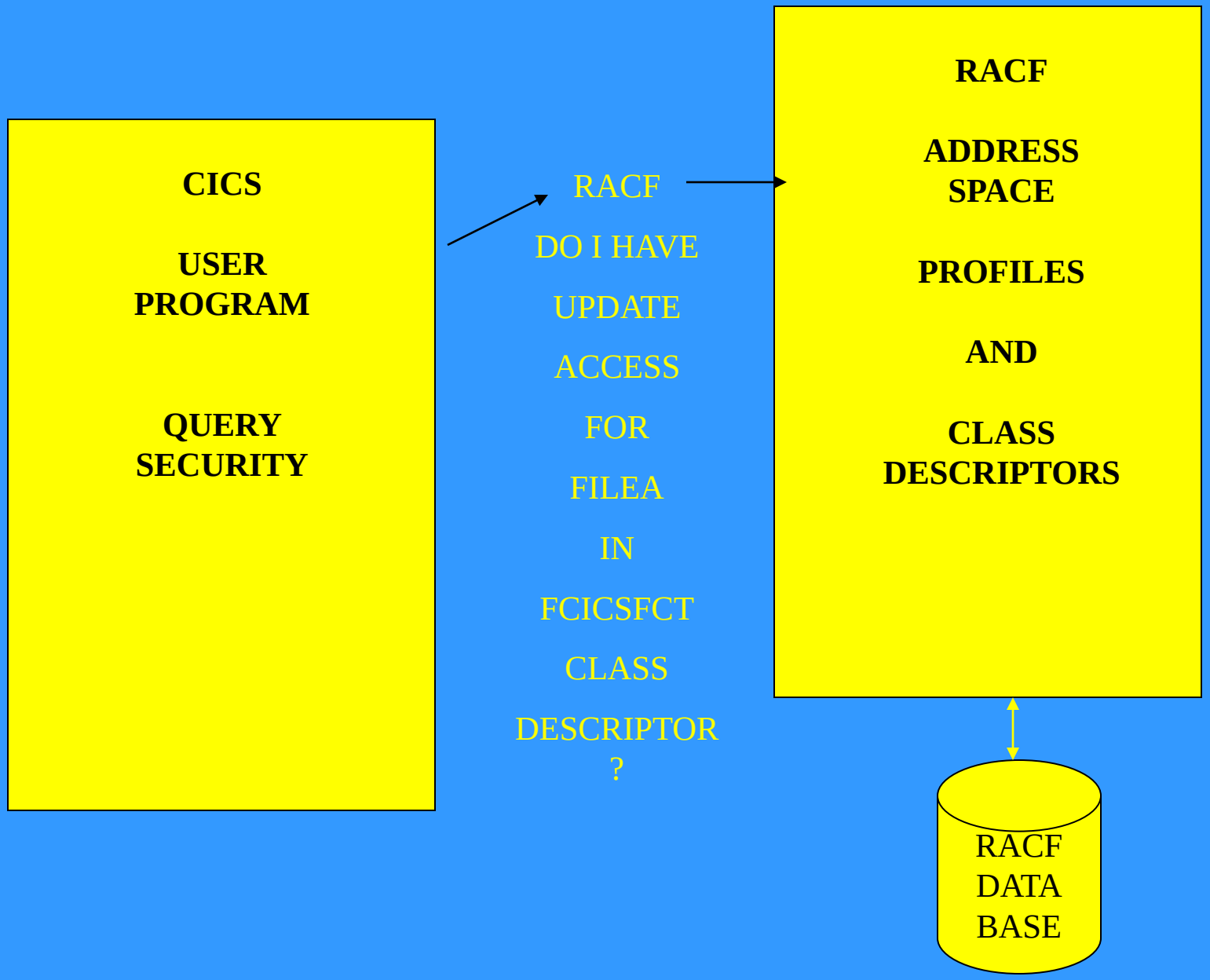
EXCEPTIONAL CONDITIONS
INVREQ LENGERR NOTFND QIDERR

8.6 THE QUERY SECURITY COMMAND

CICS resources that can be specified on the RESTYPE option :

- FILE
- JOURNALNUM
- PROGRAM
- PSB
- SPCOMMAND
- TDQUEUE
- TRANSACTION
- TRANSATTACH
- TSQUEUE

8.6 THE QUERY SECURITY COMMAND



8.6 THE QUERY SECURITY COMMAND

The CVDA is the CICS VALUE DATA AREA

It returns a status of the resource

The DFHVALUE defines the resource

Its included automatically by CICS during compile

8.7 THE SIGNON COMMAND

```
EXEC CICS SIGNON
          USERID
          < PASSWORD >
          < NEWPASSWORD >

END-EXEC.
```

EXCEPTIONAL CONDITIONS
INVREQ NOTAUTH USERIDERR

8.8 THE SIGNOFF COMMAND

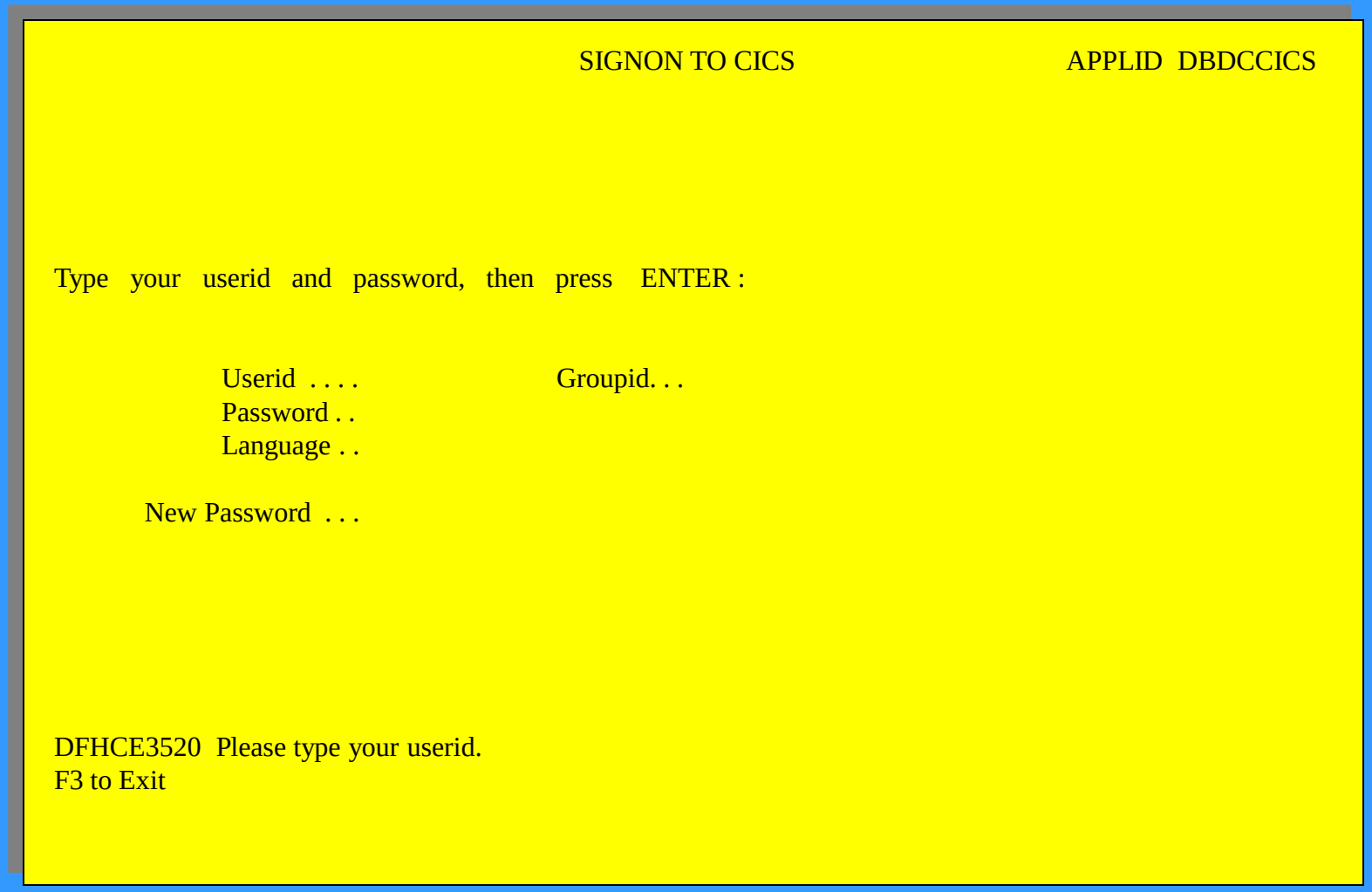
```
EXEC CICS SIGNOFF
END-EXEC.
```

EXCEPTIONAL CONDITIONS
INVREQ

8.9 THE SIGNON/SIGNOFF PROCESS

- The supplied Password is incorrect
- A new Password is required
- A new Password is not acceptable
- The Userid is revoked
- The Userid is not authorised to the Terminal
- The userid is not authorised to the Application

8.9 THE SIGNON/SIGNOFF PROCESS



8.10 THE MASTER TERMINAL TRANSACTION

The Master Terminal command can be protected, and the options it invokes

CEMT PERFORM SHUTDOWN

Access would be needed to all three

CECI should be established the same

Both transactions require : CMDSEC = YES
XCMD = YES in the SIT

8.11 INTERCOMMUNICATION SECURITY

- Bind-time security
- Link security
- Attach or user security
- Resource level security

8.11 INTERCOMMUNICATION SECURITY

```
DEF CONNECTION
OVERTYPE TO MODIFY
CICS RELEASE = 0650
 CEDA  DEFine CONnection(      )
  Queuelimit   ==> No                  No | 0-9999
  Maxqtime     ==> No                  No | 0-9999
 OPERATIONAL PROPERTIES
  AUtoconnect  ==> No                  No | Yes | All
  INService    ==> Yes                 Yes | No
 SECURITY
  SEcurityname ==>
  ATtachsec    ==> Local               Local | Identify |
Verify | Persistent
                                       | Mixidpe
  BINDPassword   :                     PASSWORD NOT SPECIFIED
  BINDSecurity ==> No                  No | Yes
  Usedfltuser  ==> No                  No | Yes
```

8.11 INTERCOMMUNICATION SECURITY

BIND Password defines a remote Password that must be the same with the local Password

This Password is specified on the Connection definition

This is optional

8.11 INTERCOMMUNICATION SECURITY

The **BIND PASSWORD** is protected in the following ways :

1. The **BIND PASSWORD** is never transmitted between systems

2. CICS does not store a readable copy of the password, either on the **CSD** or in internal control blocks

3. The **BIND PASSWORD** field in **CEDA DEFINED CONNECTION** is a non-display field.

8.11 INTERCOMMUNICATION SECURITY

An alternative is BINDSECURITY

This allows the definition of RACF Session Keys

Requires XAPPC = YES in the SIT

8.11 INTERCOMMUNICATION SECURITY

LINK SECURITY is handled by the SECURITYNAME option :

This option must specify the USERID of the incoming region

If Attachsec is LOCAL then its this name that is used for resource access in this region

8.11 INTERCOMMUNICATION SECURITY

For ATTACH or USER security the ATTACHSEC option is important :

ATTACHSEC :

LOCAL

IDENTIFY

VERIFY

Other options that affect LUTYPE6.2 are PERSISTANT and MIXIDPE

8.11 INTERCOMMUNICATION SECURITY

In every case where CICS is the incoming region then IDENTIFY should be specified

If the incoming region is not CICS and can give a Userid, then IDENTIFY should be specified

If the incoming region is a system that cannot give a Userid, then LOCAL should be specified

PERSISTANT should be used in LUTYPE6.2 where the User is signing on signing off many times