

CICS Security – The Basics

Mark Wilson
Technical Director



July 2024



1

Agenda

- Introduction
- Objectives
- CICS Security
- Summary



2

2

Introduction – Mark Wilson

Technical Director at
Vertali
www.Vertali.com

I am a mainframe
technician with some
knowledge of
Mainframe Security
and other Mainframe
Stuff

I have been doing
this for over 44 years!



3

3

In My Spare Time



4

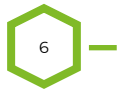
4

4

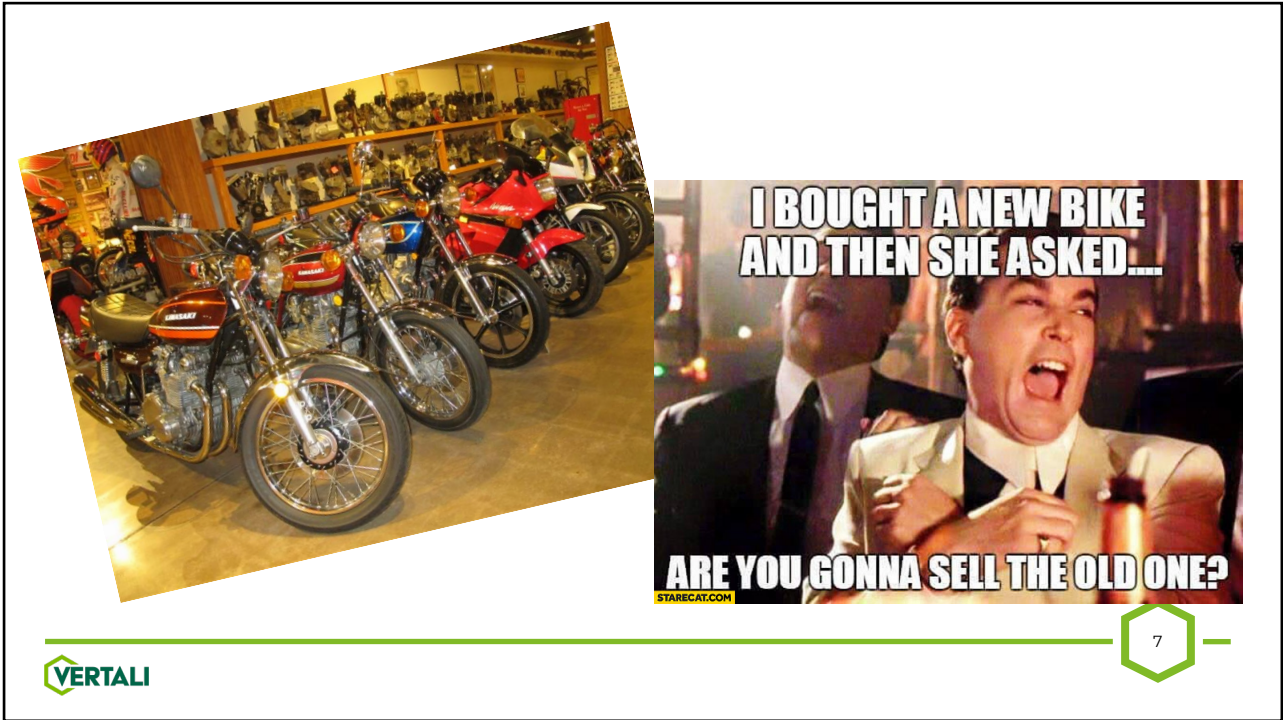


5

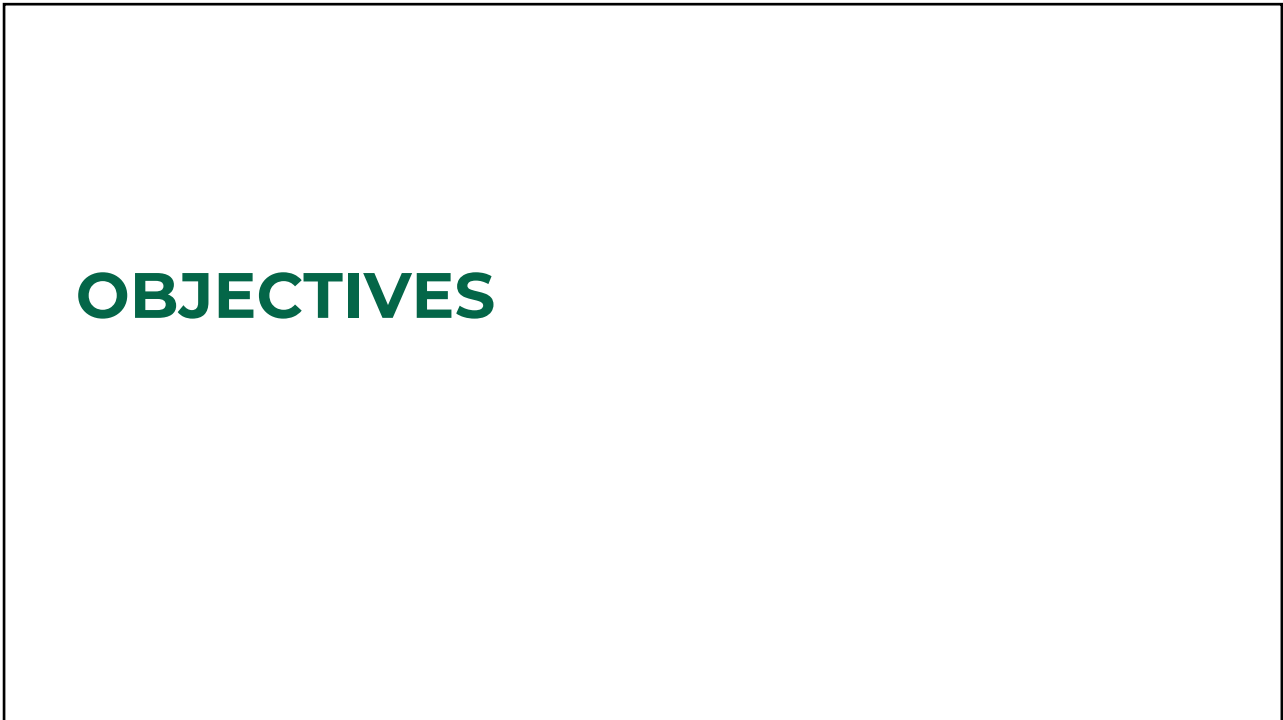
In My Spare Time



6



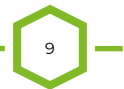
7



8

Objectives

- This is an introduction, CICS security is a one day class in its own right
- This session will delve a little into CICS security and give you, hopefully enough information to go and thoroughly audit or understand your own CICS implementation



9

CICS BASICS

10

What is CICS?

- **C**ustomer **I**nformation **C**ontrol **S**ystem (CICS)
- A transaction processing system, that for some reason has become quite popular over the years, who's role is to provide online transaction processing (OLTP)
- Not the only transaction processing subsystem that IBM has:
 - IMS and Websphere and there are others
- Specialised infrastructure that supports multiple users and processes multiple application programs concurrently



11

11

What is CICS?

- CICS regions can communicate and share resources
 - Multi-Region Operation (MRO) - within one z/OS system or Sysplex
 - Inter-System Communication (ISC) – within and between MVS images
- Provides interface to other systems - DB2, IMS, IDMS
- First commercial release July 8th 1969
 - What happened 13 days later?



12

12

21st July 1969



VERTALI

13

13

THE GOOD STUFF!

14

The CSD (CICS System Definition)

- CICS System Definition (CSD) is a VSAM dataset where resource definitions are stored
- Access to this file and the transactions and batch utilities that manipulate and list its contents need to be strictly controlled
- The CSD is updated using transactions CEDDA and CEDB
- The CSD is viewed using CEDC
- DFHCSDUP a CICS supplied batch utility can be used to list the contents of the CSD



15

15

The SIT!



16

16

System Initialisation Table(SIT)

- Defines configuration options for a CICS region
- SIT parameters govern the RACF interface
- ACF2 and TSS are different

Systems Initialisation Table(SIT)

- Parameter settings obtained from:
 - Built-in CICS defaults
 - DFHSITxx Macro assembly modules (default DFHSIT)
 - SYSIN DD Statement
 - EXEC Statement PARM
 - Console commands; However you cannot change security parameters via the console
- Last parameter definition found is the one used

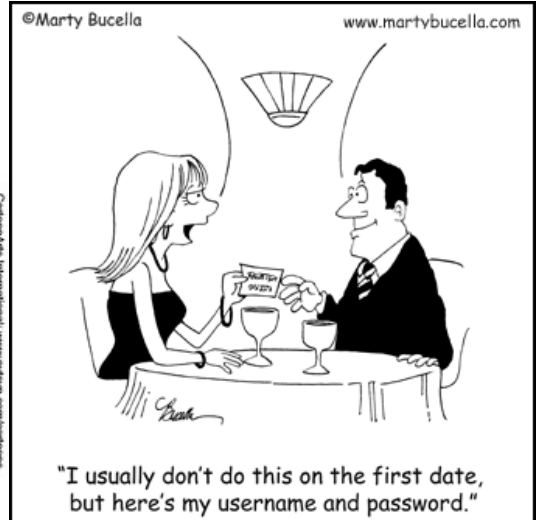
Example SIT

SIT TITLE 'DFHSIT - CICS DEFAULT SYSTEM INITIALIZATION TABLE'

DFHSIT TYPE=CSECT,	
APPLID=VRTCICS,	VTAM APPL identifier
CMDSEC=ASIS,	API command security checking
DFLTUSER=CICSUSER,	Default user
PLTPISEC=NONE,	No PLT security checks on PI programs
PLTPIUSR=,	PLT PI userid = CICS region userid
SEC=YES,	External security manager option
SECPRFX=NO,	Security prefix
USRDELAY=30	Delay before ACEE refresh
XCMD=YES,	Use default RACF class name
XDCT=NO,	Do not perform RACF check
XFCT=\$UKFCT,	FCT use UK class for RACF check
XJCT=NO,	Do not perform RACF check
XPCT=YES,	Use default RACF class name
XPPT=YES,	Use default RACF class name
XPSB=YES,	Use default RACF class name
XTRAN=YES,	Use default RACF class name
XUSER=YES	Surrogate user checking to be done



Time for some security?



What the ESM does for us?

- CICS relies on an ESM (RACF, ACF2 or TSS) to provide security
 - The ESM controls
 - Who can logon to CICS
 - Who can execute a transaction
 - Who can use a transaction resource
 - Started Transaction
 - Program, File or Journal
 - Transient Data Destination
 - Temporary Storage Queue
 - Who can execute a CICS command (CMDSEC)



21

21

CICS SECURITY

22

CICS and External Security

- CICS when configured to do so will call an External Security Manager (ESM)
- The ESM can be RACF, CA-ACF/2 or CA-Top Secret
- CICS has no mechanism today for internal security
- If you don't use an ESM, you have NO security!



23

23

THE BOOK TO READ!

24

CICS Transaction Server for z/OS
Version 6

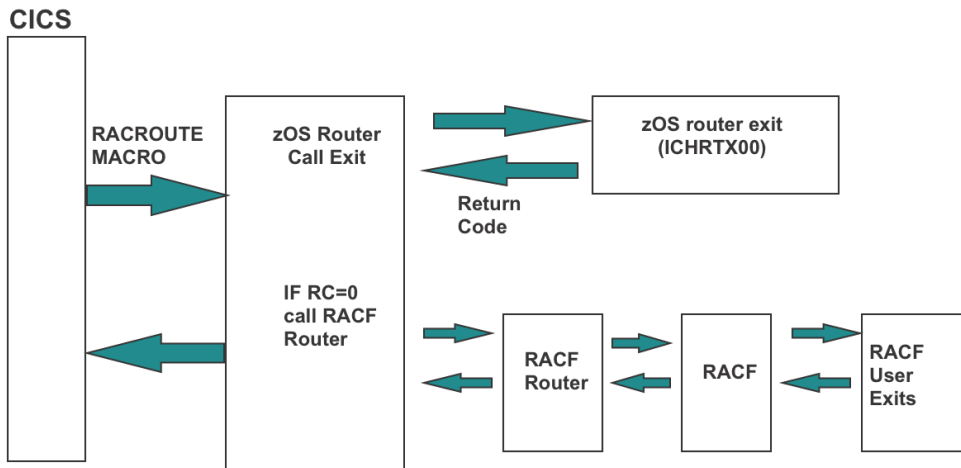
Security for CICS



25

25

The CICS RACF Interface



26

26

The role of CICS in security control

- To invoke SAF via RACROUTE to perform:
 - User Signon/Signoff
 - Access Authorisation

**ACCESS
DENIED**



SIT!

- The SIT as previously mentioned is where most of the good stuff happens!
- We must understand this in detail and all the parameters that are here!
- You need to strictly control the SIT
- I have seen some environments control it using Endeavor, ISPW or Changeman (there are others)



SIT Parms

```

APPLID= (VRTCICS) ,
FCT=NO ,
GMTEXT= 'Vertali CICS SYSTEM' ,
GRPLIST= (XYZLIST, CICSTS32) ,
IRCSTRT=YES ,
ISC=YES ,
STATRCD=ON ,
SEC=NO ,
TCT=NO ,
TRTABSZ=64 ,
XRF=NO

```

So what's the problem with these parameters?

Hint: Something to do with Security

Is security being used?

- SEC=NO
 - No External Security Manager being used
- SEC=YES
 - External Security Manager is being used

What is being protected?

- Controlled by several other parameters in sit in the form Xnnnn=
 - Where:
 - XTRAN = Transaction Security
 - XFCT = File Control Security
 - XCMD = Command Security
 - XTST = CICS Temp. storage control
 - XPCT = Started Transaction control
 - To name but a few!

A Pair of classes

- Member Class and a Grouping Class
- More on this later



RLIST CDT T&PRDTRN CDTINFO NORACF

```

CLASS NAME
-----
CDT T&PRDTRN
CDTINFO INFORMATION
-----
CASE = UPPER
DEFAULTRC = 004
DEFAULTUACC = NONE
FIRST = ALPHA, NUMERIC, NATIONAL, SPECIAL
GENLIST = DISALLOWED
GROUP = G&PRDTRN
KEYQUALIFIERS = 0000000000
MACPROCESSING = NORMAL
MAXLENGTH = 13
MAXLENX = NONE
MEMBER =
OPERATIONS = NO

```

You need a pair of classes



Xnnn SIT Parameters

- The majority of the Xnnn SIT parameters follow the form:
 - **NO**
 - Option is disabled
 - **YES**
 - Option is enabled with default IBM RACF classes
 - **Class_name**
 - The installation has created a site specific RACF class, normally a pair member & grouping

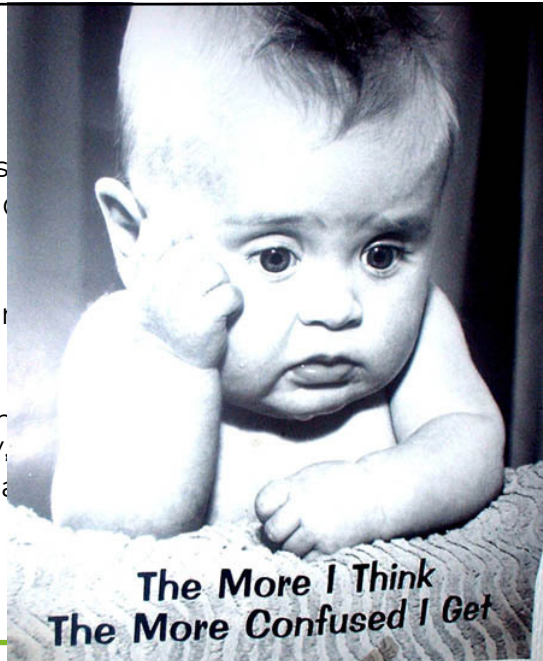
RACF Class Names

Member class	Resource grouping class	Description
TCICSTRN	GCICSTRN	CICS transactions, normal attach security
PCICSPSB	QCICSPSB	CICS PSBs
ACICSPCT	BCICSPCT	CICS-started transactions
DCICSDCT	ECICSDCT	CICS transient data queues
FCICSFCT	HCICSFCT	CICS files
JCICSJCT	KCICSJCT	CICS journals
MCICSPPT	NCICSPPT	CICS programs
SCICSTST	UCICSTST	CICS temporary storage queues
CCICSCMD	VCICSCMD	EXEC CICS SYSTEM commands
RCICSRES	WCICSRES	Document templates, bundles, EP adapters, EP adapter sets, event bindings, ATOMSERVICE definitions, and XML transforms



RACF Classes

- Share default class
 - TCICSTRN and CICSSTRN, CICSPRD2 and CICSSTRN3
 - Would all have same security
 - They could even be the same class
- Create locally defined regions (Prod, Dev, Test)
 - Eg TEPDRTRN and CICSSTRN3
 - Would all have same security



, CICSPRD2 and CICSSTRN3
 the SIT's dataset
 on or set of related
 PRD1, CICSPRD2 and



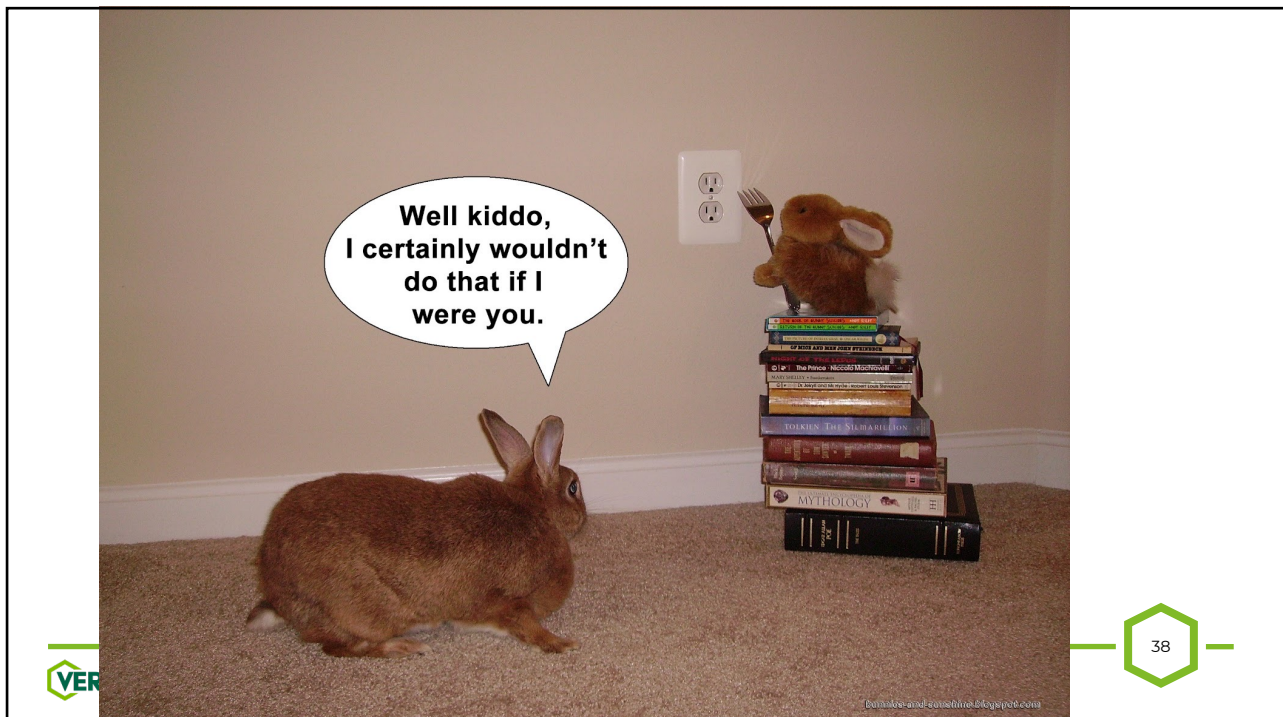
RACF Classes and Prefixing

- Classes shared by dissimilar CICS regions
 - May need to differentiate resources belonging to specific CICS regions
 - Resource names can be prefixed with CICS region's USERID
 - SIT Parameter - SECPRFX=YES | **NO**
 - TCICSTRN and GCICSTRN shared between CICSPRD1 and CICSDEV1
 - Would have XTRAN=YES defined in their respective SIT's
- CEMT in Prod needs to be locked down; but available in Dev
 - Prod userid is **PRODCICS** and Dev is **DEVICICS**
 - Two RACF profiles **PRODCICS.CEMT** and **DEVICICS.CEMT**



37

37



38

38

My Recommendation

- I would always go with separate RACF classes and not use prefixing
- It's easy now that we have the RACF CDT class
- But ultimately, you must do what is best for your organisation



CICS TRANSACTION SECURITY

XTRAN SIT Parameter

- If XTRAN=YES
 - then the IBM supplied RACF classes TCICSTRN & GCICSTRN are being used for transaction security
- If XTRAN=£PRDTRN
 - then the site defined RACF classes T£PRDTRN & G£PRDTRN RACF classes are being used for transaction security
 - Note that CICS enforces the first character of the RACF class for transaction profiles to be a T
 - Other resource types have their own rules



41

41

What RACF profiles do I have?

- Use the RACF SEARCH command to list all of the profiles in a given class:
 - SR CLASS(TCICSTRN) NOMASK
 - SR CLASS(GCICSTRN) NOMASK
- This only shows the profiles



42

42

Who has access to them?

- You need to list each profile and check:
 - UACC
 - Access List
 - Conditional Access List
- You can generate the required RACF commands with the SEARCH command and CLIST option



43

43

Example Search in batch

```
//SEARCH EXEC PGM=IKJEFT01
//SYSTSPRT DD SYSOUT=*
//SYSTSIN DD *
SR CLASS(TCICSTRN) NOMASK NOLIST -
  CLIST('RL TCICSTRN ' ' ALL')
//*
//EXEC EXEC PGM=IKJEFT01
//SYSTSPRT DD SYSOUT=*
//SYSTSIN DD *
EX EXEC.RACF.CLIST
```



44

44

CICS Transaction Security

- IBM supply many transactions as part of the basic CICS install
- They are categorised and all have different security requirements



Category 1

- CICS Internal use only
- Never associated with a terminal
- RACF (ESM) is NOT called for these transactions
- Some people define them to RACF for documentation purposes



Category 2

- CICS Administration transactions
- Very powerful
- Very restricted access lists
- All RACF profiles should have a UACC of NONE
- May be a good candidate for AUDIT(ALL(READ)) to log all access successful or not
- Check the manuals carefully there are additional security requirements/suggestions



47

Category 3

- All users require access to these transactions
- All Category 3 transactions are exempt from security checks
- Some people define them to RACF for documentation purposes



48

MEMBER AND GROUPING CLASSES

49

Member or Grouping Class?

- What are they?
- Two different ways to protect resources in CICS
- How does CICS use them?
 - Profile merge
 - In Storage profiles
- Who has access?

50

Example of Member Class Profiles

- The warehouse group of users need access to three transactions: INVC, ORDP & STO

```
RDEFINE TCICSTRN INVC OWNER (SECADM) UACC (NONE)
RDEFINE TCICSTRN ORDP OWNER (SECADM) UACC (NONE)
RDEFINE TCICSTRN STO OWNER (SECADM) UACC (NONE)
PERMIT INVC CLASS (TCICSTRN) ID (WHSEUSRS) ACCESS (READ)
PERMIT ORDP CLASS (TCICSTRN) ID (WHSEUSRS) ACCESS (READ)
PERMIT STO CLASS (TCICSTRN) ID (WHSEUSRS) ACCESS (READ)
```



51

51

Example Grouping Class Profiles

- The warehouse group of users need access to three transactions: INVC, ORDP & STO

```
RDEFINE GCICSTRN WARE_TRNS OWNER (SECADM) UACC (NONE)
RALTER GCICSTRN WARE_TRNS ADDMEM (INVC ORDP STO)

PERMIT WARE_TRNS CLASS (GCICSTRN) ID (WHSEUSRS) ACCESS (READ)
```



52

52

How RACF merges Profiles

- Member / grouping classes must be loaded into memory
- Applies only to member / grouping classes
- Merge applies only if a resource name appears in more than one profile
- UACC: The most restrictive UACC is chosen from the profiles that are merged
- Access list: If a user or group appears in the access lists of multiple profiles, that user or group is given the highest access



53

53

Who has access to STO H?

- We must find and analyse all member and grouping profiles that protect STO H
- Is STO H protected by a member class profile?

```
RLIST TCICSTRN STO H AUTH
```



54

54

Who has access to STOH?

- Is STOH protected by a grouping class profile(s)?

```
RLIST TCICSTRN STOH RESGROUP
```

- Use RLIST to display any grouping class profiles identified



55

55

OTHER BITS

56

User Logon at Terminal

- RACF logon
 - CESN sign-on transaction
 - Program with EXEC CICS SIGNON command
 - CICS Supports MFA, just saying
- At RACF logon
 - Userid and Password
 - TERMINAL terminal-id or CONSOLE console-name
- APPL applid - as determine by SIT parameters
 - APPLID= Region's application ID
 - READ access required



57

57

User Logon at Terminal

- CICS concurrent logon restrictions
 - SNSCOPE=NONE | CICS | MVSIMAGE | SYSPLEX
 - NONE No restriction
 - CICS Only once in each CICS region
 - MVSIMAGE Only once for entire MVS image
 - SYSPLEX Only once for entire Sysplex
- Only effects user logon via CESN
- Does not affect pre-set terminal logons



58

58

Default User

- Is used for transactions when the user is unknown
- SIT Parameter **DFLTUSER**=userid – is how to set the userid
- If not specified, the default is **CICSUSER**
- The default userid will require access to certain resources:
 - The applid for the region
 - CICS Transactions intended for everyone's use (without logon)
 - Trigger-transactions (if TD defined with no ATI USERID)
- If specifying XUSER=YES then READ access will be required to default_Userid.DFHINSTL

RACLISTing and Refreshing

- CICS automatically RACLISTs its resource classes
- CICS uses RACROUTE REQUEST=LIST with GLOBAL=YES at address space initialisation
- However, if the dataspace for the class has already been built this is simply referenced
- Profiles are loaded into a shared dataspace in memory
- Once RACLISTed, CICS uses Fast RACF Checking for access authorisation
- Classes appear in SETROPTS LIST - GLOBAL=YES RACLIST ONLY

RACLISTing and Refreshing

- How to refresh the Dataspace(s)
 - Changes made with RACF commands only effect profiles in the database, not those in memory
 - To implement changes the RACLISTed dataspace must be replaced
 - Issue a SETROPTS RACLIST(member-class) REFRESH
 - This is Non-disruptive as a new dataspace is built and then all relevant CICS regions are notified of the new dataspace
 - Need to perform refresh in each Monoplex/Sysplex where the class is RACLISTed
 - Be aware of classes that share the same POSIT value

POSIT Values.....



Miscellany

- Internal application security: Still used today
- CICS segment on a RACF user profile
- PLTPI – **P**rogram **L**oad **T**able **P**ost **I**nitialisation Userid
- Pre-set Terminal Userids; without a Password Check!
- Started Transactions and Associated Userids
- ATI – **A**utomatic **T**ransaction **I**nitiation
- SURROGAT class profiles; different ones used; depends on what is set and what is being checked
- Resource Security coupled with SIT Parameters
 - RESSEC, CMDSEC and PLTPISEC
- Command Security



63

63

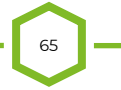
SUMMARY

64

Summary



KEEP CALM AND AUTOMATE ALL THE THINGS



Contact Details

Markwilson@Vertali.com

Mobile: +44 (0) 7768 617006

