What's New in CICS Security

Colin Penfold
Leader of CICS TS Security at IBM Hursley

Virtual CICS User Group
13 July 2021

What's New in

CICS TS 5.6

CICS TS Open Beta

Enhancements to TLS

Scenarios and Best Practices

Monitoring and Preventing Threats

Simplification and Improved Diagnostics

Outbound SNI Support

TLS 1.3†

Replacing outbound default ciphers

† CICS TS Open Beta

Enhancements to TLS

Scenarios and Best Practices

Monitoring and Preventing Threats

Simplification and Improved Diagnostics

Outbound SNI Support

SNI allows a server with a single ip address and port to host multiple secure websites, each with their own server certificate.

E.g. Amazon (AWS)

CICS TS supports SNI as a client

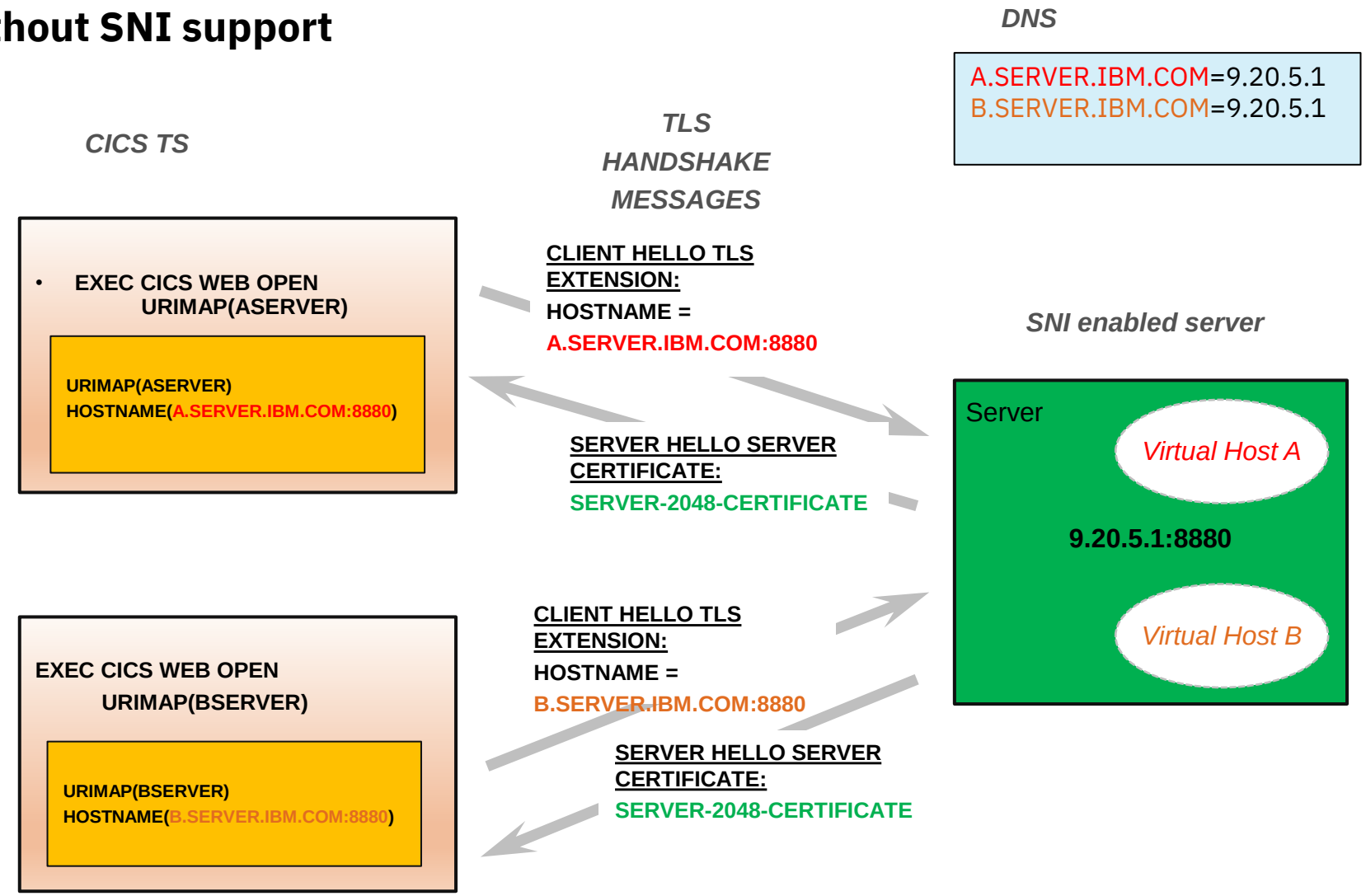
SNI supported rather than required
- Used if server supports it
- No configuration

Server Name Indication (SNI) was introduced with Internet Engineering Task Force RFC 6066

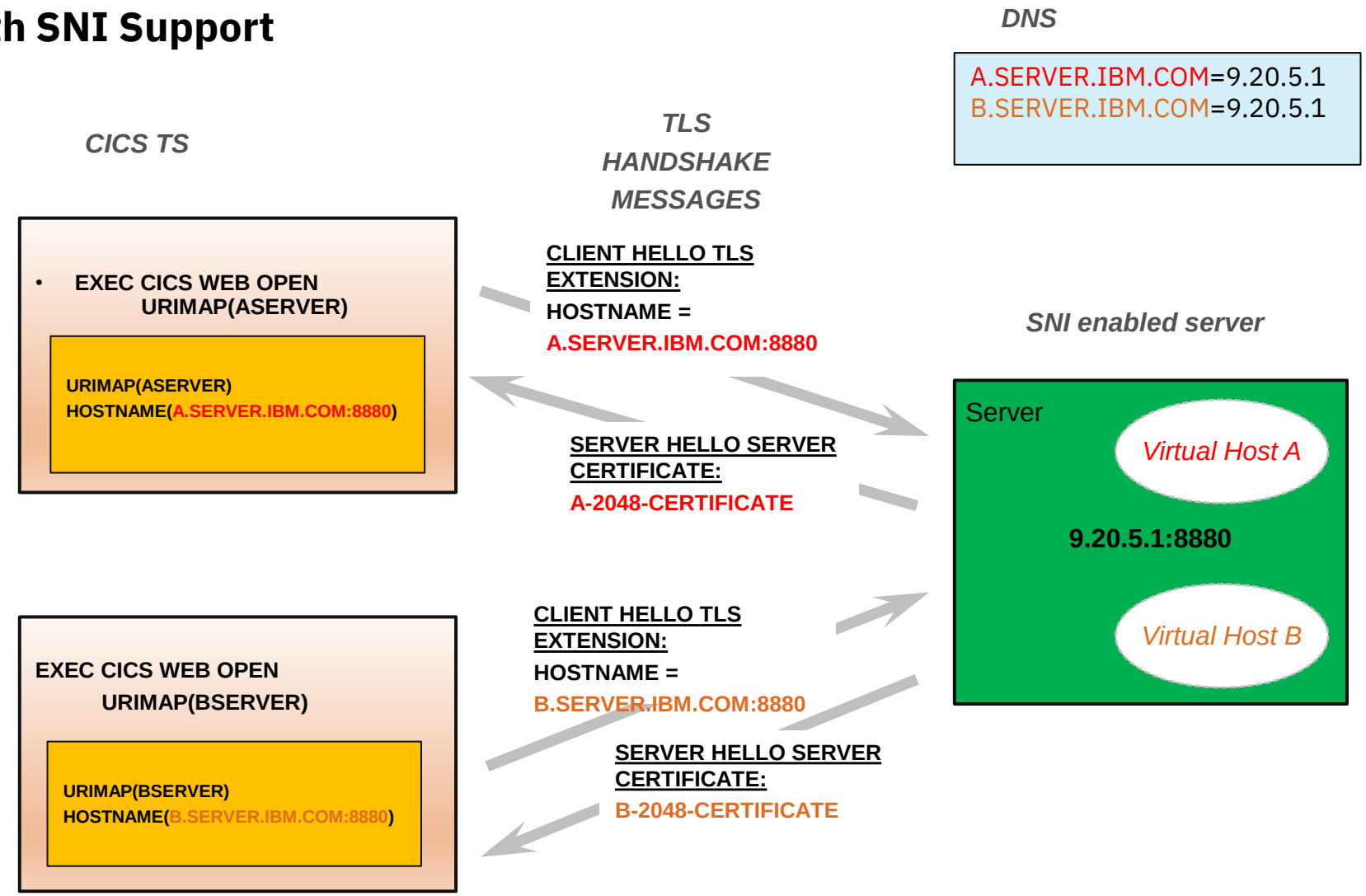
- RFC 6066 is a companion document to RFC 5246 that described TLS 1.2.
- RFC 5346 superseded an earlier description of SNI in RFC 3546.

Backported to CICS TS 5.3 in APAR PH20063

Without SNI support



With SNI Support



TLS 1.3

Major change to TLS

3 new ciphers for 1.3

Ciphers incompatible with TLS 1.2

Performance changes

Single handshake

More secure algorithms

Change to caching

RFC 8446 approved in Aug 2018

1301 TLS_AES_128_GCM_SHA256

1302 TLS_AES_256_GCM_SHA384

1303 TLS_CHACHA20_POLY1305_SHA256

External Changes

SIT Changes

- MINTLSLEVEL={TLS11,TLS12,TLS13}
- MAXTLSLEVEL={TLS11,TLS12,TLS13}

Removed
-ENCRYPTION=
-MINTLSLEVEL=TLS10, TLS10ONLY

CIPHERS option on resources

IPCONN, TCPIPSERVICE and URIMAP

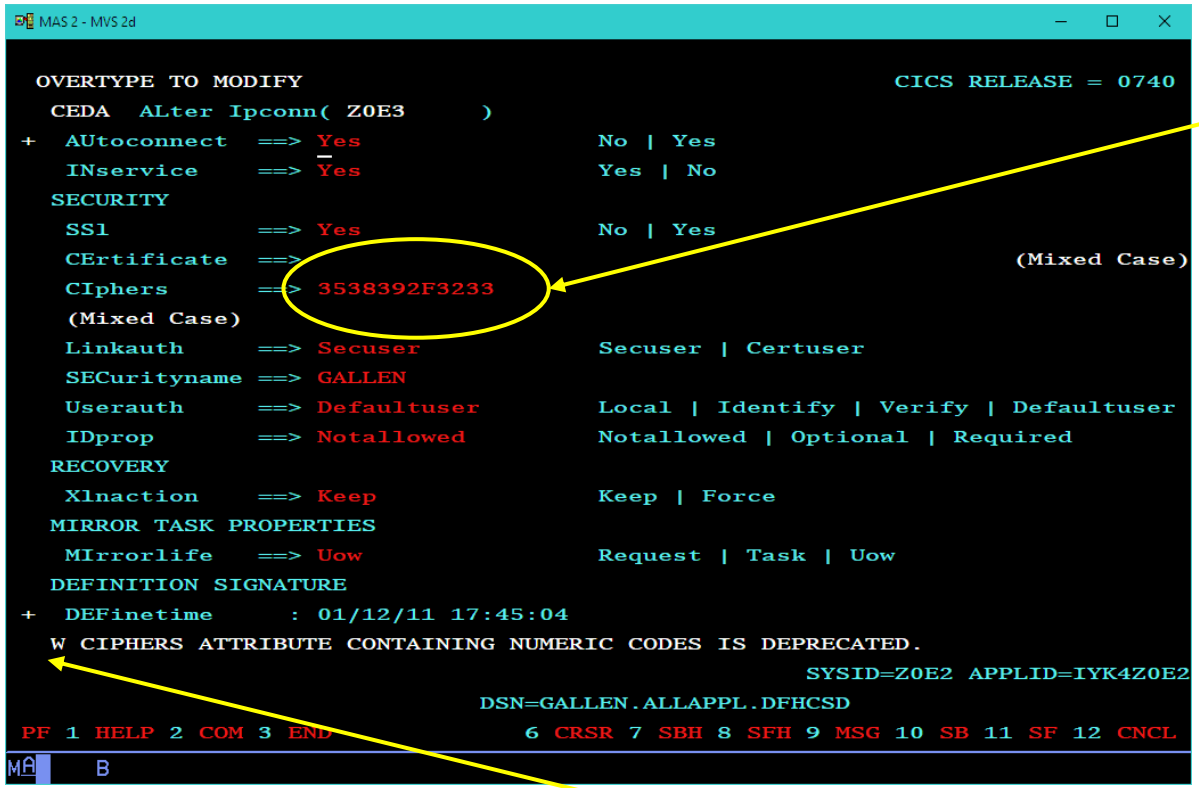
Defaults to **defaultciphers.xml** rather than numeric ciphers

Deprecated / Removed
- Numeric ciphers

USSCONFIG must have the following file

/security/ciphers/**defaultciphers.xml**

MAXTLSLEVEL<=TLS 1.2



Change/Install numeric cipher give warning

Blanking out sets default to defaultciphers.xml

MAXTLSLEVEL=TLS13

Numeric ciphers no longer supported

All definitions must use xml files

Change/Install numeric ciphers will fail

MAXTLSLEVEL<=TLS 1.2

EXEC CICS WEB OPEN CIPHERS(353839)
<URIMAP(urimap)>

Warning messages issued
- Once per program issuing command

Existing requests still honoured

New translate will fail

MAXTLSLEVEL=TLS13

EXEC CICS WEB OPEN ~~CIPHERS(353839)~~
<URIMAP(urimap)>

CIPHERS option ignored

Warning messages issued

Once per program issuing command

CIPHERS from URIMAP (if specified)

Otherwise defaultciphers.xml used

Migration to using TLS 1.3

Upgrade to z/OS 2.4

Upgrade to CICS TS Open Beta
- Copy and customise defaultciphers.xml

Prepare RDO definitions
- All resources must use xml files in CIPHERS
- TLS 1.3 ciphers must be included

Upgrade certificates
- RSA key size at least 2048 bits
- ECC keys size at least 256 bits

Then set MAXTLSLEVEL=TLS13

It is important to upgrade all definitions to use cipher files.

This will make it easier for compliance

All ciphers will be defined in USSCONFIG

If any ciphers are found to have security flaws it can be changed in one place

Replacing outbound default ciphers

Override the system supplied default 2 digit ciphers (a very limited set)

Used on
EXEC CICS WEB OPEN
EXEC CICS INVOKE SERVICE

Replace with defaultciphers.xml

CD Item on CICS TS 5.6
PH38091

Feature toggle to enable

com.ibm.cics.web.defaultcipherfile=true

CICS security documentation restructure with best practices †

Health Checks for conformance to best practice †

† CICS TS Open Beta

Enhancements to TLS

Scenarios and Best Practices

Monitoring and Preventing Threats

Simplification and Improved Diagnostics

CICS security documentation restructure

Objectives

Education on concepts and terminology
- Aimed at new joiners

Advice on security in application architecture scenarios
- Aimed at application architects

Security **configuration tasks** for these scenarios
- Aimed at new sysprogs

Clear Best Practice advice and Recommendations

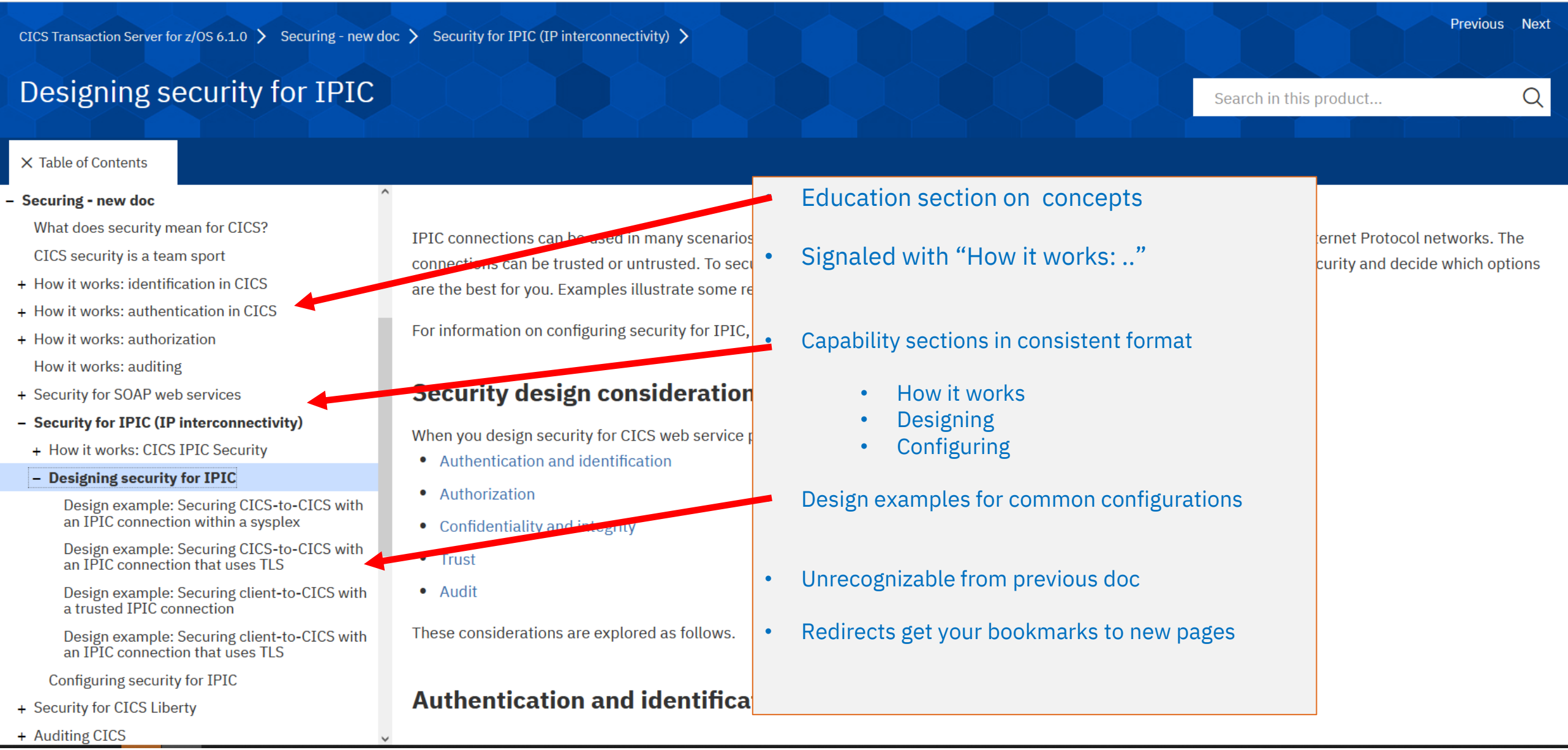
CICS TS Open Beta

IBM Docs has a mixture of old and new

How it works
- Identification
- Authentication
- Authorization
- Confidentiality and Integrity
- Auditing

Initial scenarios
- Web Services
- Liberty
- IPIC

Rewrite and Restructure of CICS Security Documentation

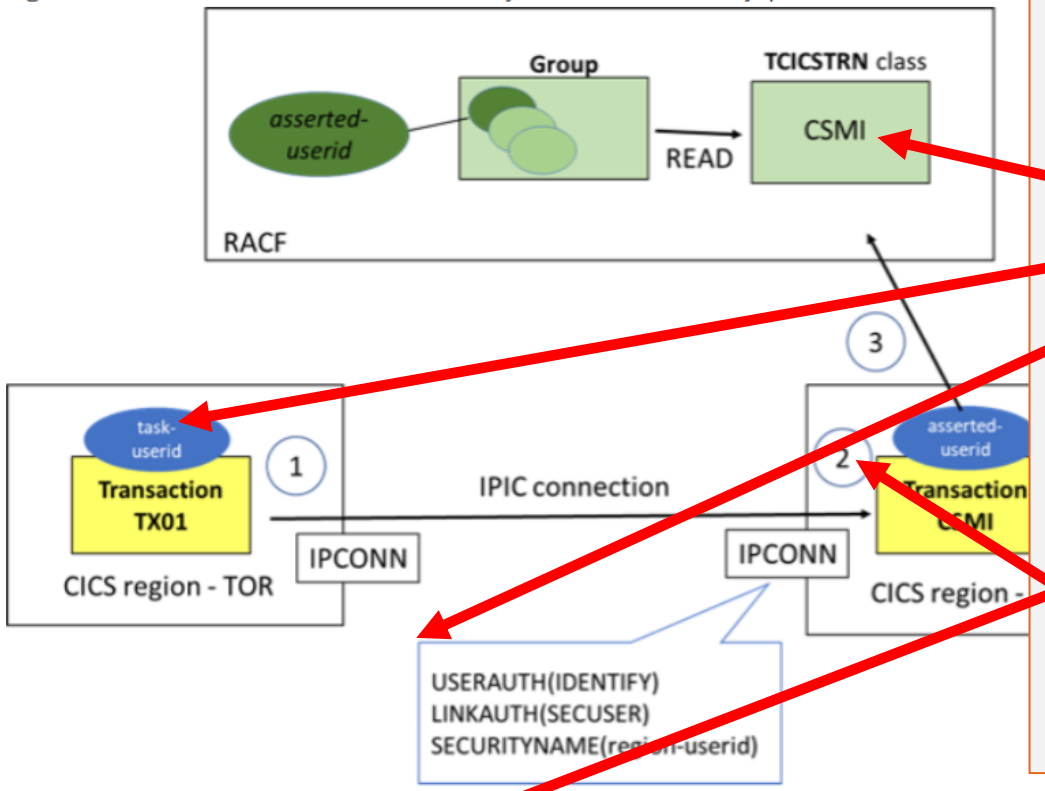


- Education section on concepts
- Signaled with “How it works: ..”
- Capability sections in consistent format
  - How it works
  - Designing
  - Configuring
- Design examples for common configurations
- Unrecognizable from previous doc
- Redirects get your bookmarks to new pages

Design Example Diagrams

Figure 1 shows an overview of the scenario.

Figure 1. IPIC trusted connection between systems in the same sysplex



- Examples with diagrams of security information
- Standard diagrams with
  - RACF profile and permissions
  - UserIDs in flow
  - System Management Resources and security attributes
- Numbered flow of security information

The following security flows occur at the points shown:

1. Transaction TX01 running in the TOR links to a program in the AOR over the IPCONN that connects the two regions and flows its task user ID to the AOR.
2. Identification of the transaction in the AOR is controlled by the USERAUTH(IDENTIFY) setting on the AOR's IPCONN definition which allows the identity to be set to the flowed user ID from the TOR. The flowed user ID from the TOR becomes the *asserted-userid* in the AOR.

Recommendations and Best Practices

- In Liberty JVM server, to control registration with the angel process.

Recommendation

Because the CICS region user ID is a powerful user ID, it must be protected. This user ID must be defined to RACF with the PROTECTED attribute. *Protected user IDs* cannot be used to log on to the system, and are protected from being revoked through incorrect system access attempts. This setting prevents failed password attempts that cause a denial of service attack.

simpler auditing.

Security best practice (validated by IBM Health Checker for z/OS)

In the CICS documentation, configuration best practices that are validated by IBM Health Checker for z/OS are highlighted in boxes, like the one that surrounds this statement.

New Health Checks

What is the health checker?

A tool to help identify potential configuration problems before they impact availability or cause system outages

Programmatically checks the current active z/OS and sysplex settings and definitions for a system

Generates output with detailed messages to inform of any potential problems and suggested actions to take to resolve them.

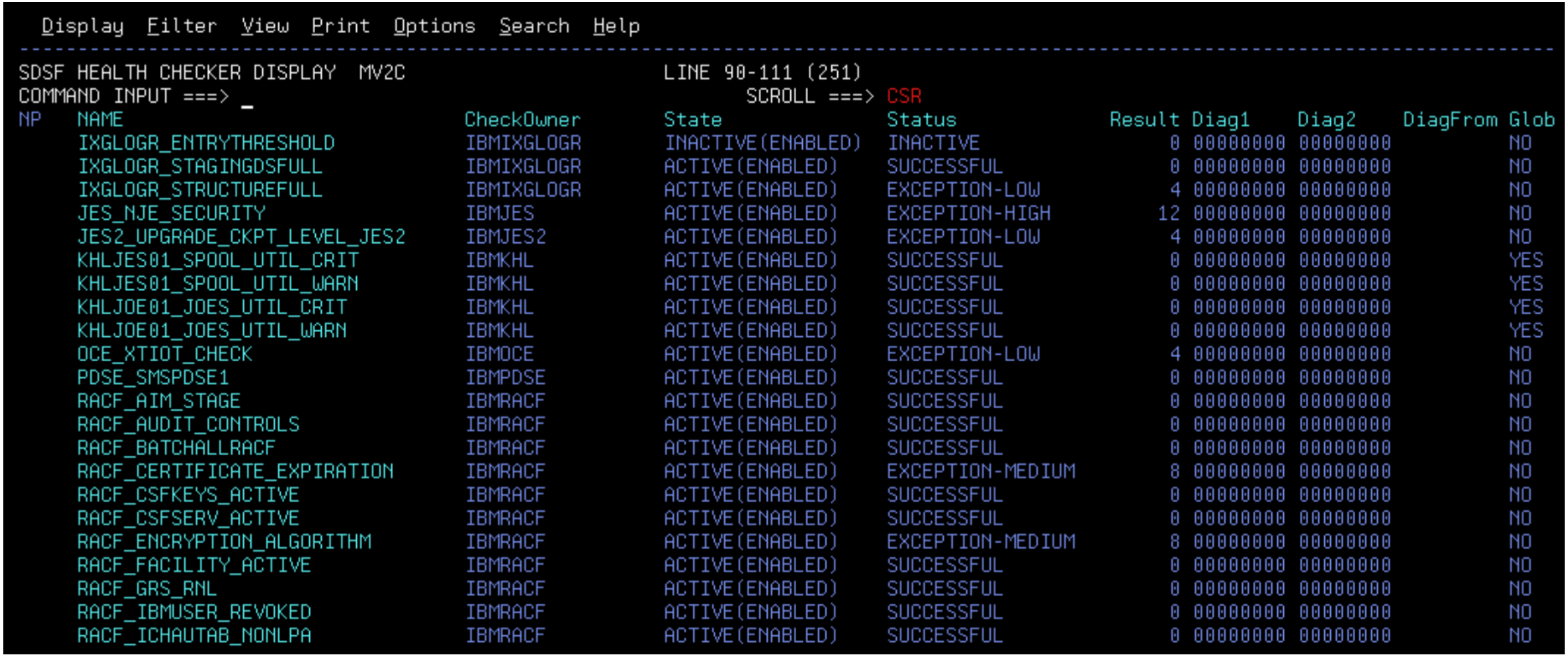
IBM Health Checker for z/OS designed to encourage best practice

- Report where not conforming with advice
- Part of base product since z/OS 1.7
- On by default from z/OS 2.1 (Sep 2013)

Health Check output

- Visible as option CK in SDSF
- Checks are associated with a product or subsystem
  - IBM provides over 150 health checker checks
- Each check tests configuration or state information
  - Result in SUCCESS, WARNING or EXCEPTION message

ISPF option SDSF;CK



```
  Display  Filter  View  Print  Options  Search  Help
------------------------------------------------------------------------------------------------------------------------
SDSF HEALTH CHECKER DISPLAY  MV2C                    LINE 90-111 (251)
COMMAND INPUT ===> _                                       SCROLL ===> CSR
NP    NAME                          CheckOwner       State              Status              Result Diag1    Diag2    DiagFrom Glob
      IXGLOGR_ENTRYTHRESHOLD        IBMIXGLOGR       INACTIVE(ENABLED)  INACTIVE                 0 00000000 00000000          NO
      IXGLOGR_STAGINGDSFULL         IBMIXGLOGR       ACTIVE(ENABLED)    SUCCESSFUL               0 00000000 00000000          NO
      IXGLOGR_STRUCTUREFULL         IBMIXGLOGR       ACTIVE(ENABLED)    EXCEPTION-LOW            4 00000000 00000000          NO
      JES_NJE_SECURITY              IBMJES           ACTIVE(ENABLED)    EXCEPTION-HIGH          12 00000000 00000000          NO
      JES2_UPGRADE_CKPT_LEVEL_JES2  IBMJES2          ACTIVE(ENABLED)    EXCEPTION-LOW            4 00000000 00000000          NO
      KHLJES01_SPOOL_UTIL_CRIT      IBMKHL           ACTIVE(ENABLED)    SUCCESSFUL               0 00000000 00000000          YES
      KHLJES01_SPOOL_UTIL_WARN      IBMKHL           ACTIVE(ENABLED)    SUCCESSFUL               0 00000000 00000000          YES
      KHLJOE01_JOES_UTIL_CRIT       IBMKHL           ACTIVE(ENABLED)    SUCCESSFUL               0 00000000 00000000          YES
      KHLJOE01_JOES_UTIL_WARN       IBMKHL           ACTIVE(ENABLED)    SUCCESSFUL               0 00000000 00000000          YES
      OCE_XTIOT_CHECK               IBMOCE           ACTIVE(ENABLED)    EXCEPTION-LOW            4 00000000 00000000          NO
      PDSE_SMSPDSE1                 IBMPDSE          ACTIVE(ENABLED)    SUCCESSFUL               0 00000000 00000000          NO
      RACF_AIM_STAGE                IBMRACF          ACTIVE(ENABLED)    SUCCESSFUL               0 00000000 00000000          NO
      RACF_AUDIT_CONTROLS           IBMRACF          ACTIVE(ENABLED)    SUCCESSFUL               0 00000000 00000000          NO
      RACF_BATCHALLRACF             IBMRACF          ACTIVE(ENABLED)    SUCCESSFUL               0 00000000 00000000          NO
      RACF_CERTIFICATE_EXPIRATION   IBMRACF          ACTIVE(ENABLED)    EXCEPTION-MEDIUM         8 00000000 00000000          NO
      RACF_CSFKEYS_ACTIVE           IBMRACF          ACTIVE(ENABLED)    SUCCESSFUL               0 00000000 00000000          NO
      RACF_CSFSERV_ACTIVE           IBMRACF          ACTIVE(ENABLED)    SUCCESSFUL               0 00000000 00000000          NO
      RACF_ENCRYPTION_ALGORITHM     IBMRACF          ACTIVE(ENABLED)    EXCEPTION-MEDIUM         8 00000000 00000000          NO
      RACF_FACILITY_ACTIVE          IBMRACF          ACTIVE(ENABLED)    SUCCESSFUL               0 00000000 00000000          NO
      RACF_GRS_RNL                  IBMRACF          ACTIVE(ENABLED)    SUCCESSFUL               0 00000000 00000000          NO
      RACF_IBMUSER_REVOKED          IBMRACF          ACTIVE(ENABLED)    SUCCESSFUL               0 00000000 00000000          NO
      RACF_ICHAUTAB_NONLPA          IBMRACF          ACTIVE(ENABLED)    SUCCESSFUL               0 00000000 00000000          NO
```

Example of existing health check

```
 Display  Filter  View  Print  Options  Search  Help
------------------------------------------------------------------------------------------------------------------------
SDSF OUTPUT DISPLAY RACF_CERTIFICATE_EXPIRATION   LINE 0       COLUMNS 02- 133
COMMAND INPUT ===> _                                          SCROLL ===> CSR
******************************** TOP OF DATA ***************************************************************************
CHECK(IBMRACF,RACF_CERTIFICATE_EXPIRATION)
SYSPLEX:    PLEX2     SYSTEM: MV2C
START TIME: 02/01/2021 07:00:46.901547
CHECK DATE: 20111010  CHECK SEVERITY: MEDIUM

               Certificates Expiring within 60 Days

 Cert Owner   Certificate Label                End Date   Trust Rings
 ------------ ------------------------------- ---------- ----- -----
  ID(FVRACF1)  Keyring26-Default-Certificate   2013-06-30 No        0
  ID(NICED)    nicedcert                       2018-03-14 Yes       0
  ID(ASCR1)    DefaultWASCert.WCLGW1           2010-12-31 Yes       1
  CERTAUTH     CAJAT238                        2015-11-20 Yes       0
  ID(JATP)     ClientJAT238                    2015-11-20 Yes       0
  ID(PHAVERC)  Havercan OpenSSL Server         2007-03-04 Yes       0
  ID(FVFNT01)  FVFNT01-WUI-SSL                 2015-05-12 Yes       1
  CERTAUTH     LABEL00000008                   2020-10-08 Yes       0
  ID(ASCR1)    DefaultWASCert.WCLRCAZ1         2010-12-31 Yes       1
  ID(FVFNT13)  Keyring26-Web-Server            2013-06-30 Yes       1
  ID(FVFNT13)  Keyring26-EJB-Container         2013-06-30 Yes       1
  ID(FVFNT13)  Keyring26-Default-Certificate   2013-06-30 Yes       1
  ID(FVFNT05)  ABCDEFGHIJKLMNOPQRSTUVWXYZabcdef 2010-01-16 Yes      0
```

CICS TS V5 Checks in IBM Health Checker for z/OS

```
SDSF HEALTH CHECKER DISPLAY  MV2C                    LINE 16-37 (245)
COMMAND INPUT ===>                                        SCROLL ===> CSR
NP   NAME                              CheckOwner      State              Status             Result
     CICS_CEDA_ACCESS                  IBMCICS         ACTIVE(ENABLED)    EXCEPTION-LOW           4
     CICS_JOBSUB_SPOOL                 IBMCICS         ACTIVE(ENABLED)    EXCEPTION-LOW           4
     CICS_JOBSUB_TDQINTRDR             IBMCICS         ACTIVE(ENABLED)    EXCEPTION-LOW           4
```

```
 Check Reason:  Jobs can be run with regionid authority by
    unauthenticated users using the SPOOL
Check run (local time)     Jobname  ASID Applid   Regionid Ver  RcRn
12/21/2020 16:22:00.468705 CMAS740  0058 IYK2Z2G2 JTILLI1  0740 0803 18
12/21/2020 16:22:55.256985 CIDRBAF1 0063 IYK2ZAF1 DBEARD1  0740 0803 3
```

These checks were checking correct configuration to prevent attack by the CICSPWN PenTest tool

New CICS Health Checks

Based on best practice reviews of customers

Cover security configuration of

- Regions definitions

- CICS resources

- CICS zFS security

Best practice advice is aimed at production or production-like regions

Examples of checks

SEC=YES

XTRAN=YES|class

XUSER=YES

Default user can access sensitive transactions

Universal USSCONFIG access

Universal JVMPROFILE access

New CICS Checks for IBM Health Checker for z/OS

```
SDSF HEALTH CHECKER DISPLAY  MV2C                    LINE 16-37 (245)
COMMAND INPUT ===>                                        SCROLL ===> CSR
NP   NAME                              CheckOwner      State             Status            Result
     CICS_CEDA_ACCESS                  IBMCICS         ACTIVE(ENABLED)   EXCEPTION-LOW          4
     CICS_JOBSUB_SPOOL                 IBMCICS         ACTIVE(ENABLED)   EXCEPTION-LOW          4
     CICS_JOBSUB_TDQINTRDR             IBMCICS         ACTIVE(ENABLED)   EXCEPTION-LOW          4
     CICS_REGION_CONFIGURATION         IBMCICS         ACTIVE(ENABLED)   EXCEPTION-HIGH        12
     CICS_RESOURCE_CONFIGURATION       IBMCICS         ACTIVE(ENABLED)   EXCEPTION-HIGH        12
     CICS_RESOURCE_SECURITY            IBMCICS         ACTIVE(ENABLED)   EXCEPTION-HIGH        12
     CICS_USS_CONFIGURATION            IBMCICS         ACTIVE(ENABLED)   EXCEPTION-HIGH        12
```

```
09/09/2020 09:16:03.232341 CIDRBAF1 005E IYK2ZAF1 DBEARD1  0740 F200 1
Exception messages:
DFHH0402 XTRAN=NO has been specified.
Warning messages:
DFHH0405 MINTLSLEVEL lower than 1.2 has been specified.

09/09/2020 09:22:26.546624 CICSR740 005A IYK2Z3B1 WHARMBY  0740 A000 1
Exception messages:
DFHH0401 SEC=NO has been specified.
```

System programmer response
Using TLS levels lower than 1.2 does not adequately secure communications. If the affected region is used for anything other than a test environment, consider using TLS 1.2 or higher.

TLS Protocol in monitoring records †

Security Monitoring Capability

Instruction Execution Protection †

† CICS TS Open Beta

Enhancements to TLS

Scenarios and Best Practices

Monitoring and Preventing Threats

Simplification and Improved Diagnostics

TLS Protocol in inbound performance record

```
 Display  Filter  View  Print  Options  Search  Help
-------------------------------------------------------------------------------
SDSF OUTPUT DISPLAY CICSMOND JOB98162  DSID   110 LINE 1,720   COLUMNS 02- 157
COMMAND INPUT ===>                                            SCROLL ===> PAGE
        DFHSOCK  C457     SOTLSLVL          E3D3E2E5 F14BF300                    TLSV1.3
        DFHSOCK  A320     SOCIPHER          00001301                              4865
        DFHTASK  C430     CECMCHTP          F3F9F0F6                             3906
        DFHTASK  C431     CECMDLID          F7F9F940 40404040 40404040 40404040  799
        DFHTASK  C432     LPARNAME          D4E5E2F2 C4404040                    MVS2D
        DFHTASK  A433     MAXTASKS          00000020                               32
        DFHTASK  A434     CURTASKS          00000001                                1
           ...
        DFHCICS  T480     PTSTART           D9885F7FB11B1FA4                2021/04/08 14:04:15.737265
        DFHCICS  P481     PTTRANNO          0000144C                              144
        DFHCICS  C482     PTTRAN            C3E6E7D5                             CWXN
        DFHCICS  A483     PTCOUNT           00000001                                1
           ...
        DFHCICS  C112     RTYPE             404040E3                                T
           ...
        DFHSTOR  A105     SCUGETCT          00000006                                6
           ...
        DFHSTOR  A106     SCUSRHWM          00011F40                            73536
           ...
        DFHSTOR  A107     SCUSRSTG          00000000000021E8                     8680
           ...
```

TLS Protocol in outbound resource record

```
  Display  Filter  View  Print  Options  Search  Help
-------------------------------------------------------------------------------------------------------------------
SDSF OUTPUT DISPLAY CICSMOND JOB98162  DSID   110 LINE 4,894   COLUMNS 02- 157
COMMAND INPUT ===>                                            SCROLL ===> PAGE
         URIMAP                          E3C5E2E3 E4D9C9F1                                  TESTURI1
         CIPHER                          00000035
         TLSLVL                          E3D3E2E5 F14BF200                                  TLSV1.2
         WBURIOPN                        0000002000000001                    00:00:00.000512          1
         WBURISND                        0000000100000001                    00:00:00.000016          1

         URIMAP                          E3C5E2E3 E4D9C9F2                                  TESTURI2
         CIPHER                          00001301
         TLSLVL                          E3D3E2E5 F14BF300                                  TLSV1.3
         WBURIOPN                        0000000500000001                    00:00:00.000080          1
         WBURISND                        0000000100000001                    00:00:00.000016          1

NO WEBSERVICE RESOURCE ENTRIES

----------FIELD-NAME-------------------------UNINTERPRETED--------------------------------INTERPRETED-------------

         TRAN                            C3E2C8D8                                           CSHQ
         USERID                          C7C2F1F2 F2F04040                                  GB1220
         TTYPE                           E4400000                                           U
         START                           D9871BEBD26E696A                    2021/04/07 13:56:36.032230
         STOP                            D9885FF21EFB0E02                    2021/04/08 14:06:15.724976
         TRANNUM                         0000030C                                                  30
```

Security Monitoring Capability

XS security domain had no stats monitoring fields

When introduced in 1992

- Most requests were 3270 signon
- Only password/passtickets
- Request on RO TCB
- Used DES encryption

Security advances mean XS handles more authentication types

- Password/Passphrases with KFDAES, MFA , Kerberos, certificates, …
- CPU and elapsed time authenticating has increased greatly.

To avoid bottlenecks requests cannot now all go through the RO TCB

- Open TCBs are used or attached, increasing usage of TCBs
- TCBs (and probably ESM requests) consume 24-bit storage.

New Security Statistics

```
User

____
  Average timeout reuse time. . . . . :  00:00:00.00000
  Time out reuse count. . . . . . . . :       4,652          Current instances in directory. . . :         102
  Time out expiry count . . . . . . . :         218          Peak instances in directory . . . . :         313
  Directory reuse count . . . . . . . :      16,118          Current instances in timeout. . . . :          50
  Directory not found count . . . . . :           0          Peak instances in timeout . . . . . :         102
  Delete count due to sign off. . . . :         210          ENF events matched. . . . . . . . . :           5
  Delete count due to ENF . . . . . . :           5          ENF events not matched. . . . . . . :           0

Security

________
  New ACEEs with ICRX . . . . . . . . :           0          New ACEEs without ICRX. . . . . . . :         102
  Current ACEEs with ICRX . . . . . . :           0          Current ACEEs without ICRX. . . . . :         102
  Peak ACEEs with ICRX. . . . . . . . :           0          Peak ACEEs without ICRX . . . . . . :         313

  Successful fastpath authentications :       6,012
  Successful fullpath authentications :         303          Failed fullpath authentications . . :          27
  Successful kerberos authentications :           0          Failed kerberos authentications . . :           0
  Successful JWT creations  . . . . . :           0          Failed JWT creations  . . . . . . . :           0
  Successful JWT authentications  . . :           0          Failed JWT authentications  . . . . :           0
s
  Successful resource authorizations  :       8,065          Failed resource authorizations  . . :           2
  Successful command authorizations . :         234          Failed command authorizations . . . :           1
  Successful surrogate authorizations :       1,040          Failed surrogate authorizations . . :           1
  Successful non-CICS authorizations  :           0          Failed non-CICS authorizations  . . :           0

  Max parallel ESM requests . . . . . :          16          Max waiting ESM requests  . . . . . :       9,999
  Current parallel ESM requests . . . :           0          Current waiting ESM requests  . . . :           0
  Peak parallel ESM requests  . . . . :          16          Peak waiting ESM requests . . . . . :          24
```

New Monitoring for Security

435	XSVFYPWD	The total elapsed time that the user task spent verifying passwords, password phrases, PassTickets, and MFA tokens
438	XSVFYBAS	The total elapsed time that the user task spent verifying basic authentication tokens
439	XSVFYKER	The total elapsed time that the user task spent verifying Kerberos tokens
440	XSVFYJWT	The total elapsed time that the user task spent verifying JSON web tokens

435 refers to EXEC CICS VERIFY PASSWORD/PHRASE and EXEC CICS SIGNON
438-40 refer to EXEC CICS VERIFY TOKEN

Instruction Execution Protection

Executable storage

```
58B0 4104 5820 B000
58B0 2004 50B0 41FC
58E0 4110 50E0 4244
58F0 3EF0 4110 41F0
```

Protected storage

```
E685 9393 4084 9695
855A 4040 E896 A440
8381 9540 9985 8184
40C5 C2C3 C4C9 C34B
```

Objectives

Separates data storage from program storage

Prevents code from being executed on data storage

Prevents buffer overflow exploits

Hidden code in data

```
C889 8484 8595 4083
9684 857A 50B0 41FC
58E0 4110 50E0 4244
58F0 3EF0 4110 41F0
```

Software and Hardware Prereqs

z/OS 2.4 or z/OS 2.3 + APARs

z14 or higher

z/OS Externals

STORAGE OBTAIN and RELEASE

EXECUTABLE={YES|NO}

IARV64 GETSTOR

EXECUTABLE={SYSTEM_RULES|YES|NO}

EXECUTABLE ignored if hardware or software does not support IEP

DSA	Usage
RDSA/ERDSA	Reentrant programs
SDSA/ESDSA	Shared USER key storage and USER key programs
CDSA/ECDSA	CICS key storage and CICS key programs
UDSA/EUDSA	User key storage

DSA Usage in CICS TS Open Beta

DSA	Usage
RDSA/ERDSA	Reentrant programs
PUDSA/EPUDSA	USER key programs
PCDSA/EPCDSA	CICS key programs
SDSA/ESDSA	Shared USER key storage
CDSA/ECDSA	CICS key storage
UDSA/EUDSA	USER key storage

Storage is either **executable** or **data** (non executable)

Try to execute code in EUDSA
(normal getmained storage)

```
C889 8484 8595 4083
9684 857A 50B0 41FC
58E0 4110 50E0 4244
58F0 3EF0 4110 41F0
```

New IEP Program Check

Protection exception (0c4)

- Kernel ESTAE will identify 0c4 as IEP program check
  - Error code 0c4/akes
  - PSW will be pointing to next instruction
  - BEAR will contain last branch address

- Exception trace call for this program check
- New message (IEP 0c4)

API option

EXEC CICS GETMAIN EXECUTABLE

XPI option

SMMC GETMAIN EXECUTEABLE(YES)

GLUE and TRUE work areas

ENABLE PROGRAM GAEXECUTABLE
ENABLE PROGRAM TAEXECUTABLE

Native assembler dynamic storage

Specify DFHEIENT DATA_EXECUTEABLE=YES

If you really need to make data areas executable

API , XPI and definitions

Primarily intended for ISVs

Require SYSEIB

Enabling IEP

Opt in

feature toggles:

com.ibm.cics.sm.iep=true
com.ibm.cics.ap.syseib.unprotected=true

Allows ISVs and Customers

to check if they execute code in data storage

Improved information for security failures †

Removal of security definitions for CAT 1 transactions †

† CICS TS Open Beta

Enhancements to TLS

Scenarios and Best Practices

Monitoring and Preventing Threats

Simplification and Improved Diagnostics

Improved information for security failures

Currently the following messages show when there is a security violation

Problems can often occur if for example

- The userid is a functional userid
- The transaction is started on another region

How can you identify the end user

```
DFHXS1111 02/24/2021 15:21:29 IYK2ZOX3 CSMI Security violation by user LEW for resource
JAT251.DFHQUERY in class SURROGAT. SAF codes
        are (X'00000008',X'00000000'). ESM codes are (X'00000008',X'00000000'). RACF request made was
FASTAUTH.
```

```
11.27.16 JOB78114  ICH408I USER(LEW     ) GROUP(TSOUSER ) NAME(LEWIS H JAMES       )  153
  153              JAT251.DFHQUERY CL(SURROGAT)
  153              INSUFFICIENT ACCESS AUTHORITY
  153              FROM JAT* (G)
  153              ACCESS INTENT(READ   )  ACCESS ALLOWED(NONE   )
```

A new DFHXS1117 message will accompany DFHXS1111 messages

Available origin data information will be output

- Information will vary depending on entry point
- Distributed Identity will be reported if available

Example message from a web request

```
DFHXS1117 03/11/2021 09:43:27 IYK2ZOX3 CSMI Security violation originated from applid IYK2ZOX1 client
IP address 9.145.169.58 port 53619 facility LEWURI TCPIPSERVICE LEWTCP transaction CWBA user
LEWISJA link user LEW.
```

Example message from a terminal transaction originating in a TOR

```
DFHXS1117 03/11/2021 09:43:27 IYK2ZOX3 CSMI Security violation originated from applid IYK2ZOX1 client
IP address 9.145.169.58 port 53649 facility T135 transaction CECI user LEWISJA link user LEW.
```

Removal of security definitions for CAT 1 transactions

Problem

Creating CAT 1 security definitions problematic and time consuming

Required for all region userids

New transactions missed

Complications of SECPRFX

New CAT 1 transaction in service always cause problems

Requirement

Only the region userid is allowed to run CAT 1 transactions

CICS knows

- The region userid
- The CAT 1 transactions
- How a transaction is started

… so why ask the ESM ?

Removing the ESM check makes it more secure

Not possible to misconfigure

ESM no longer called for CAT 1 transactions

Internal security checking to check

Abend AXS1 if check fails

DFH£CAT1 CLIST removed

Mentioned in Auditor section of CICS’s Doc to ensure auditors are aware

Links

IBM Documentation for CICS TS 5.6 and CICS TS Open Beta
https://www.ibm.com/docs/en/cics-ts

CICS TS Open Beta Announce (9th July 2021)
https://www.ibm.com/support/pages/node/6360807

CICS TS Community feedback on open beta
https://ibm.biz/cicstsopenbeta

RFE (Request for Enhancement)
https://www.ibm.com/developerworks/rfe/

620 separate RFEs already delivered against CICS TS V5.