

z/OS 2.4 IBM Education Assistant (IEA)

Solution (Epic) Name: zSecure 2.4.0

Element(s)/Component(s): 5655-N16 5655-N17 5655-N20 5655-N21 5665-AD8



Agenda

- Trademarks
- Session Objectives
- Overview
- The Command and Ticket logging feature
- Interactions & Dependencies
- Migration & Coexistence Considerations
- Installation
- Session Summary
- Appendix

Trademarks

- See url <http://www.ibm.com/legal/copytrade.shtml> for a list of trademarks.
- Additional Trademarks:
 - None

Session Objectives

- Explain new zSecure product family features:
 - Command and Ticket logging
 - Command library productivity enhancements
 - Enhancements for ICSF HCR77D0 auditing
 - Support for RACF IDTPARMS segment to authenticate JSON Web Tokens.
 - Support for RACF JES segment
 - Enhancements for File Integrity Monitoring
 - Enhancements for auditing DB2
 - Enhancements for auditing IMS
 - Enhancements for ACF2 general resource protection compliance checking
 - Upgrade compliance checking to recent DISA STIG version

Overview

- Who (Audience)
 - z/OS security administrators, analysts, auditors, and systems programmers
- What (Solution)
 - New security administration command log stream
 - New IMS and DB2 security compliance test points
 - New analysis logic for sensitive ACF2 resource access
- Wow (Benefit / Value, Need Addressed)
 - Link security administration actions to change ticket numbers
 - Deploy commands for a change ticket to the next system
 - Further slash time need for ACF2 STIG compliance checking
 - Help automate IMS and DB2 security compliance checking

Extended zSecure Admin with a new feature

Command and Ticket Logging

Security definition changes are only allowed
with appropriate management approval

What was the change request number?



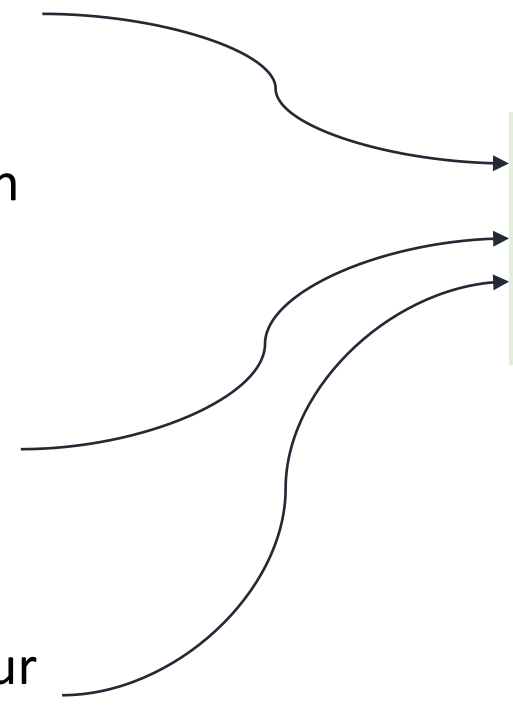
With zSecure, no need for the auditor to bother
the security administrator

Let me show how to find it in zSecure



CKXLOG started task

- Writes to system or sysplex wide CKXLOG log stream.
- Command logging requests are sent to CKXLOG by zSecure Admin and zSecure Command Verifier with an optional ticket id.
- Characteristics are defined once during install for a model logstream.
- Remembering a current ticket in the server is limited here to 1 hour (HHMM is 0100).



```
SETUP LSNAME(&SYSPLEX..CKXLOG)
SETUP LSMODEL(MODEL.CKXLOG)
SETUP TICKETEXPIRE(0100)
```

The diagram consists of four curved arrows originating from the list items on the left and pointing to the code blocks on the right. The first arrow points from the first list item to the first line of code. The second arrow points from the second list item to the second line of code. The third arrow points from the third list item to the third line of code. The fourth arrow points from the fourth list item to the third line of code.

- ```

Menu Options Info Commands Setup

zSecure Admin - Mass update - Copy group

Command ==> _____

From group oldgroup
To id newgroup _____

Ticket identifier
ID UZ180B050
Description _____ More _

- Do not create OMVS segment
- Copy permits only (target id may be a group or a user)
- Generate RACF commands even when the target group exists
- Copy CUSTOMDATA
Specify options for new group
- Copy catalog aliases (only if CKFREEZE is present)
/ Issue ADDSD/RDEF for user resources
/ Copy RACFVARS profiles/members too (if option above selected)

```

# CKXLOG primary command

- Or in the zSecure UI, type CKXLOG and modify the current change ticket number plus any extra description required by the auditors.

```
zSecure Admin - Change ticket ID/Description

Command ==> _____

Ticket ID
UZ180B050 test2 _____

Description

Press ENTER to accept changes.
```

# TSO command streams

- In batch TSO command streams or home grown applications the command CKXLOGID can be used to impart the ticket id.
- When zSecure Admin generates command for different systems or queued execution it also generates CKXLOGID SET commands.
- Example shows a C(opy) action on a user id.

```
File Edit Edit_Settings Menu Utilities Compilers Test Help

EDIT CRMASCH.DATA.C2R126C.CKRCMD Columns 00001 00080
Command ==> _____ Scroll ==> CSR
***** ***** Top of Data *****
==MSG> -Warning- The UNDO command is not available until you change
==MSG> your edit profile using the command RECOVERY ON.
000001 /* CKRCMD file CKR1CMD complex PLEX1 NJE <LOCAL> generated 8 Feb -
000002 2019 19:36 */
000003 /* CKRCMD file CKRT1CMD complex PLEX1 NJE <LOCAL> generated 8 Feb -
000004 2019 19:37 */
000005 CKXLOGID SET ID('UZ1902010') DESC('Make educational presentaion')
000006 /* Commands generated by COPY USER/GROUP */
000007 adduser CRMASCH4 special nopassword nooidcard +
000008 name('HANS SCHOONE') +
000009 data('HANS SCHOONE') +
000010 owner(CRMA) +
000011 tso(acctnum(ACCT#) +
000012 msgclass(A) +
000013 proc(TSOZSEC) +
000014 size(32000) +
000015 maxsize(32000) +
000016) +
000017 operparm(auth(MASTER) +
000018 dom(NORMAL) +
000019 level(ALL) +
000020 logcmdresp(SYSTEM) +
000021 mform(M) +
000022 midid(YES) +
000023 routcode(ALL) +
000024 storage(1) +
```

# CKXLOG input

- The SETUP FILES can select the *active* command log stream (last 24 hours), or a *specific* log stream, or an *offloaded* or *unloaded* data set.
- In CARLa, the files are allocated with ALLOC TYPE=CKXLOG.

```
Menu Options Info Commands Setup

zSecure Admin - Setup - Input files Row 1 to 13 of 13
Command ==> _____ Scroll ==> CSR

Select the type of data set or file

Type Description
- ACCESS RACF ACCESS monitor data set
- ACT.BACK The backup RACF database of your active system
- ACT.CKXLOG Live command execution logstream
- ACT.PRIM The primary RACF database of your active system
- ACT.SYSTEM Live settings
- CKFREEZE System resource information data set
- CKRCMD A file for generated RACF commands
- CKX.LOGSTR Command execution logstream
- CKXLOG Command execution log
- COPY.RACF A copy of a single data set RACF database
- COPY.SEC A non-first component of a multiple data set RACF databas
- COPY.TEMP The first component of a multiple data set RACF database
- UNLOAD An unloaded RACF database

***** Bottom of data *****
```

- The Command and Ticket Logging feature

# Command Review option

- A new primary option menu item CR for *Command Review* has been added to zSecure Admin.
- You can easily run members with RACF commands (CR.1).
- You can easily review and run commands in the CKXLOG command log (CR.2).

| zSecure Suite - Main menu |                |                                                      | More: |
|---------------------------|----------------|------------------------------------------------------|-------|
| Option ==>                |                |                                                      |       |
| SE                        | Setup          | Options and input data sets                          |       |
| RA                        | RACF           | RACF Administration                                  |       |
| AA                        | ACF2           | ACF2 Administration                                  |       |
| AU                        | Audit          | Audit security and system resources                  |       |
| RE                        | Resource       | Resource protection reports                          |       |
| AM                        | Access         | RACF Access Monitor                                  |       |
| EV                        | Events         | Event reporting from SMF and other logs              |       |
| CR                        | Command review | Review and run commands                              |       |
| 1                         | Libraries      | Review and run commands from library                 |       |
| 2                         | CKXLOG         | Review and re-run commands in commands execution log |       |
| CU                        | CARLa          | Work with CARLa queries and libraries                |       |
| IN                        | Information    | Information and documentation                        |       |
| LO                        | Local          | Locally defined options                              |       |
| X                         | Exit           | Exit this panel                                      |       |

# Select command log records

- In the CR.2 selection panel, select records and specify how you want to *summarize*
- *Concise report* will show just time / user / command overview under the summary, but will show detail when zooming in.

```
zSecure Suite - Command review

Command ==> _____

Show command execution log records that fit all of the following criteria
Userid/logonid/ACID . . . _____ (ESM id or EGN mask)
Job name _____ (job name or EGN mask)
System _____ (system or EGN mask)
Profile _____ (profile or EGN mask)
Class _____ (class or EGN mask)
Ticket id _____ (search)

Advanced selection criteria
_ Date time _ Other

Output/run options
Summarize by _ 1. Ticket id 3. User 5. Command 7. Class+Profile
 2. System 4. Orig. user 6. Component 8. Complex
Ticket ID width . . . _ (1-32)
/_ Concise report _ Suppress pre-exec ESM cmds
_ Recreate commands Set ticket id
_ Print format Send as e-mail Background run
```

# Overview of Command Log records - summary

- For example: summary by ticket id.

| Command history    |                                               |  | 15 Mar 2019 |
|--------------------|-----------------------------------------------|--|-------------|
| Command ==>        |                                               |  | Count       |
| Ticket             | Description                                   |  |             |
| —                  |                                               |  | 2841        |
| — demo munchen     | long description                              |  | 4           |
| — myticket         | testing of ckxlog                             |  | 11          |
| — newpass \$BASE   |                                               |  | 12          |
| — remote test      | check if this ends up                         |  | 1           |
| — sdfsdg sdfsdg sd | sdfsdg dsffffsd                               |  | 2           |
| — setropts_test    | no details needed                             |  | 1           |
| — test             | <more>                                        |  | 13          |
| — test 1           | test 2                                        |  | 22          |
| — test-ticket-7    | description                                   |  | 2           |
| — test_setr        | Show some keywords                            |  | 4           |
| — test05           | Show some keywords                            |  | 2           |
| — test06           | storage leak test                             |  | 102         |
| — test07           | Debug msg test                                |  | 13          |
| — test12122018     | test for RL>                                  |  | 2239        |
| — toch wat langer  | no desc                                       |  | 1           |
| — tset             |                                               |  | 10          |
| — tset ddd         | dsfsdfsdf                                     |  | 8           |
| — wz180c060        |                                               |  | 2           |
| — Guustest         |                                               |  | 2           |
| — Hans' ticketid   |                                               |  | 4           |
| — Long test 1      | See what happens with very long commands..... |  | 2           |
| —                  |                                               |  | 50          |



# Overview of Command Log records

- For example: summary by ticket id.
- Pre-execution image logged by component CKXI
- Post-execution by component C4RMAIN shows return code

Command history

Command ==>

15 Mar 2019 13:34

Count

5

Count

5

| TimestampHere  | Verb     | User    | Jobname | OrgNode | OrgUser | Comp    | RC | Command                              |
|----------------|----------|---------|---------|---------|---------|---------|----|--------------------------------------|
| 8Feb2019 16:51 | ALTUSER  | CRMASCH | CRMASCH | PLEX1   | CRMASCH | CKXI    |    | ALTUSER CRMASCH NAME('HANS SCHOONE') |
| 8Feb2019 16:51 | ALTUSER  | CRMASCH | CRMASCH |         |         | C4RMAIN | 0  | ALTUSER CRMASCH NAME('HANS SCHOONE') |
| 8Feb2019 16:52 | ALTUSER  | CRMASCH | CRMASCH | PLEX1   | CRMASCH | CKXI    |    | ALTUSER CRMASCH NAME('HANS SCHOONE') |
| 8Feb2019 16:52 | ALTUSER  | CRMASCH | CRMASCH |         |         | C4RMAIN | 0  | ALTUSER CRMASCH NAME('HANS SCHOONE') |
| 8Feb2019 16:52 | LISTUSER | CRMASCH | CRMASCH | PLEX1   | CRMASCH | CKXI    |    | LISTUSER CRMASCH                     |

\*\*\*\*\* Bottom of Data \*\*\*\*\*

# Pre-execution command detail

- Here we see where a command *originated* (e.g. submittor) and what the current ticket number was.
- The commands and parameters have been *normalized* to ease searching.
- Note that this may be done by a different user on a different system, different sysplex, and on a different day than where the command is finally executed!

```
Command history
Command ==>

Ticket
Ticket id UZ180B050
Ticket description

Origin
Originating node PLEX1
Originating user CRMASCH
System name in CVT (SYSNAME) NMPIPL84
System name ZS13
Security complex name PLEX1
Jobname CRMASCH
User id CRMASCH HANS SCHOONE
Component CKXI

When
Local time of last occurrence 8 Feb 2019 16:51:03.06
Time here of last occurrence 8 Feb 2019 16:51:03.06
Command return code if known

Class Profile
USER CRMASCH

Command
ALTUSER CRMASCH NAME('HANS SCHOONE')
***** Botto
```

# Post-execution command detail

- Here we see the *command return code* and what the original ticket number was as best as we can determine.
- Post-execution image and return code is *only* recorded if you have the zSecure Command Verifier product.
- Note that the command may have been modified by Command Verifier policies!
- Note that an *extra* command may have been issued by Command Verifier.

```
Command history
Command ==> _____

Ticket
Ticket id UZ180B050
Ticket description

Origin
Originating node
Originating user
System name in CVT (SYSNAME) NMPIPL84
System name ZS13
_ Security complex name PLEX1
_ Jobname CRMASCH
_ User id CRMASCH HANS SCHOONE
_ Component C4RMAIN

When
Local time of last occurrence 8 Feb 2019 16:51:03.27
Time here of last occurrence 8 Feb 2019 16:51:03.27
Command return code if known 0

Class Profile
_ USER CRMASCH

Command
_ ALTUSER CRMASCH NAME('HANS SCHOONE')

***** Bottom
```

- ```

zSecure Admin - Confirm command
Command ==> _____

Ticket ID . . UZ1902010
Description . _____ More _

Confirm or edit the following command
ALTUSER CRMASCH NAME('HANS SCHOONE')
_____
_____

Command execution . 1
1. EXECUTE RACF command
2. EXECUTE CKGRACF command (allows use of Reason)
3. ASK administrator to execute CKGRACF command
4. REQUEST CKGRACF command for later execution
5. WITHDRAW CKGRACF command

Reason . . . . . _____
Press ENTER to continue or END to cancel the command

```

- The Command and Ticket Logging feature

Recreate commands checkbox

- The CR.2 'Recreate commands' checkbox generates a command file of all selected commands at the same time as display
- The 'Suppress pre-exec ESM cmds' prevents generating commands twice in case you have Command Verifier.
- The Set ticket id checkbox adds a CKXLOGID SET command in front

```

zSecure Admin - Command review

Command ==> _____

Show command execution log records that fit all of the following criteria
Userid . . . . . _____ (userid or EGN mask)
Job name . . . . . _____ (job name or EGN mask)
System . . . . . _____ (system or EGN mask)
Profile . . . . . _____ (profile or EGN mask)
Class . . . . . _____ (class or EGN mask)
Ticket id . . . . . UZ180B050 test2 (search)

Advanced selection criteria
_ Date time _ Other

Output/run options
Summarize by 1 1. Ticket id 3. User 5. Command 7. Class+Profile
              2. System 4. Orig. user 6. Component 8. Complex

Ticket ID width . . . . . (1-32)

/ Concise report / Suppress pre-exec ESM cmds
/ Recreate commands / Set ticket id
_ Print format _ Send as e-mail _ Background run
  
```

Concise command overview

- For example: summary by ticket id with suppressed pre-execution image.

```

0 s elapsed, 0.1 s CPU
Command ==> _____ Scroll==> CSR
Ticket          Description          Count
UZ180B050 test2
Description          Count
                    54
TimestampHere  User      Command
___ 28Nov2018 16:38 CRMASCH ALTUSER  CRMASCH NAME('HANS SCHOONE0')
___ 28Nov2018 17:06 CRMASCH PERMIT   CKG* CLASS(PROGRAM) ID(KANWEG) ACCESS(ALTER)
___ 28Nov2018 17:06 CRMASCH PERMIT   CKR* CLASS(PROGRAM) ID(KANWEG) ACCESS(ALTER)
___ 28Nov2018 17:06 CRMASCH PERMIT   C2R* CLASS(PROGRAM) ID(KANWEG) ACCESS(ALTER)
___ 28Nov2018 17:06 CRMASCH PERMIT   $CNG.CMD.CMD.EX.DEFINE CLASS(FACILITY) ID(KANWEG) ACCESS(UPDATE)
___ 28Nov2018 17:06 CRMASCH PERMIT   $CNG.SCP.ID.CRMQA048.CRMQA.CRMQA CLASS(FACILITY) ID(KANWEG) ACCESS(READ)
___ 28Nov2018 17:06 CRMASCH PERMIT   $C2R.C2RCARLA.APF CLASS(FACILITY) ID(KANWEG) ACCESS(READ)
___ 28Nov2018 17:06 CRMASCH PERMIT   BPX.FILEATTR.APF CLASS(FACILITY) ID(KANWEG) ACCESS(READ)
___ 28Nov2018 17:06 CRMASCH PERMIT   BPX.FILEATTR.PROGCTL CLASS(FACILITY) ID(KANWEG) ACCESS(READ)
___ 28Nov2018 17:06 CRMASCH PERMIT   CKG.CMD.CMD.EX.DEFINE CLASS(FACILITY) ID(KANWEG) ACCESS(UPDATE)
___ 28Nov2018 17:06 CRMASCH PERMIT   CKG.SCP.ID.CRMQA048.CRMQA.CRMQA CLASS(FACILITY) ID(KANWEG) ACCESS(READ)
___ 28Nov2018 17:06 CRMASCH PERMIT   CKR.CKRCARLA.APF CLASS(FACILITY) ID(KANWEG) ACCESS(READ)
___ 28Nov2018 17:06 CRMASCH PERMIT   CKR.C2RCARLA.APF CLASS(FACILITY) ID(KANWEG) ACCESS(READ)
___ 28Nov2018 17:06 CRMASCH PERMIT   STGADMIN.EDG.MASTER CLASS(FACILITY) ID(KANWEG) ACCESS(UPDATE)
___ 28Nov2018 17:06 CRMASCH PERMIT   STGADMIN.EDG.OWNER.CRMASCH CLASS(FACILITY) ID(KANWEG) ACCESS(UPDATE)
___ 28Nov2018 17:06 CRMASCH PERMIT   OPER CLASS(TSOAUTH) ID(KANWEG) ACCESS(READ)
___ 28Nov2018 17:06 CRMASCH PERMIT   CKG.CMD.CMD.EX.ALTUSER CLASS(XFACILIT) ID(KANWEG) ACCESS(UPDATE)
___ 28Nov2018 17:06 CRMASCH PERMIT   CKG.CMD.CMD.EX.DEFINE CLASS(XFACILIT) ID(KANWEG) ACCESS(UPDATE)
___ 28Nov2018 17:06 CRMASCH PERMIT   CKG.SCP.ID.CRMQA048.CRMQA.CRMQA CLASS(XFACILIT) ID(KANWEG) ACCESS(READ)
___ 28Nov2018 17:06 CRMASCH PERMIT   CKR.CKRCARLA.APF CLASS(XFACILIT) ID(KANWEG) ACCESS(READ)
___ 28Nov2018 17:06 CRMASCH PERMIT   'CRMA.T.**' CLASS(DATASET) GENERIC ID(KANWEG) ACCESS(ALTER)
___ 28Nov2018 17:06 CRMASCH PERMIT   $CNG.SCP.G.CR.CRM.CRMQ.** CLASS(FACILITY) ID(KANWEG) ACCESS(NONE)
___ 28Nov2018 17:06 CRMASCH PERMIT   $CNG.SCP.ID.CRMQA0*.CRMQA.CRMQA CLASS(FACILITY) ID(KANWEG) ACCESS(NONE)
___ 28Nov2018 17:06 CRMASCH PERMIT   $CNG.SCP.U.&CRMA1%** CLASS(FACILITY) ID(KANWEG) ACCESS(READ)
___ 28Nov2018 17:06 CRMASCH PERMIT   $CNG SCP II &CRMA1%** ** CLASS(FACILITY) ID(KANWEG) ACCESS(READ)

```

Recreate command result

- After pressing END on the display we are in command file edit.

```
File Edit Edit_Settings Menu Utilities Compilers Test Help
EDIT          CRMASCH.DATA.C2R226C.CKRCMD          Columns 00001 00080
Command ==>          Scroll ==> CSR
***** ***** Top of Data *****
==MSG> -Warning- The UNDO command is not available until you change
==MSG>          your edit profile using the command RECOVERY ON.
000001 /* CKRCMD file CKR2CMD complex PLEX1 NJE <LOCAL> generated 15 Mar -
000002 2019 14:28 */
000003 /* Pre-execution log not suppressed. Duplicate commands can occur. */
000004
000005 CKXLOGID SET ID('UZ180B050 test2') DESCRIPTION('')
000006
000007 ALTUSER  CRMASCH NAME('HANS SCHOONE0')
000008 PERMIT   CKG* CLASS(PROGRAM) ID(KANWEG) ACCESS(ALTER)
000009 PERMIT   CKR* CLASS(PROGRAM) ID(KANWEG) ACCESS(ALTER)
000010 PERMIT   C2R* CLASS(PROGRAM) ID(KANWEG) ACCESS(ALTER)
000011 PERMIT   $CNG.CMD.CMD.EX.DEFINE CLASS(FACILITY) ID(KANWEG) -
000012 ACCESS(UPDATE)
000013 PERMIT   $CNG.SCP.ID.CRMQA048.CRMQA.CRMQA CLASS(FACILITY) ID(KANWEG) -
000014 ACCESS(READ)
000015 PERMIT   $C2R.C2RCARLA.APF CLASS(FACILITY) ID(KANWEG) ACCESS(READ)
000016 PERMIT   BPX.FILEATTR.APF CLASS(FACILITY) ID(KANWEG) ACCESS(READ)
000017 PERMIT   BPX.FILEATTR.PROGCTL CLASS(FACILITY) ID(KANWEG) ACCESS(READ)
000018 PERMIT   CKG.CMD.CMD.EX.DEFINE CLASS(FACILITY) ID(KANWEG) -
000019 ACCESS(UPDATE)
000020 PERMIT   CKG.SCP.ID.CRMQA048.CRMQA.CRMQA CLASS(FACILITY) ID(KANWEG) -
000021 ACCESS(READ)
000022 PERMIT   CKR.CKRCARLA.APF CLASS(FACILITY) ID(KANWEG) ACCESS(READ)
0
0
0
000026 ACCESS(UPDATE)
```

Press PF3, enter R at the cursor location, press ENTER to run these commands

The Command and Ticket Logging feature

Various administrator groups may have varying needs

I want to stage deployment



Show ticket id fields - none, some, or every time

resource name: CKR.CKXLOG.ID.SHOW

access NONE – do not show fields in user interface to modify ticket id

access READ – allow user to change ticket id and show fields to do it

resource name: CKR.CKXLOG.ID.PROMPT

access NONE – do not force extra prompts

access READ – show ticket id prompts

Logging policy by user and component

resource name: CKX.CKXLOG.LOG.*component*

access NONE – do not log

access READ - log

- CKRCARLA

Commands issued from the CARLa engine (local, immediate)

- CKXI

The CKX command executor (local queued or remote)

- CKGRACF

Multiple authority commands when approved

Timed command execution

- C4RMAIN

Any RACF command (post-execution).

CKXLOGID

Any log request directly from a REXX

Extended zSecure Admin with a new feature

Crypto audit enhancements

AU.S – SYSTEM – ICSF enforcement and configuration

```
System settings RACF complex NMPIPL71          unld  7 Feb 2019 23:45:00
Command ==>
System ZS41      NMPIPL71 sysplex PLEX1          CKFREEZE collected  7 Feb 2019 23:45:00

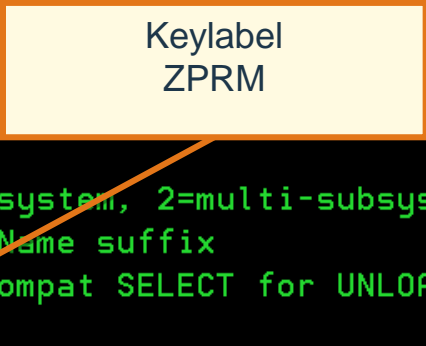
ICSF enforcement options                      ICSF configuration
ICSF is active (not PCF/CUSP) Yes             ICSF crypto domain                1
ICSF PKDS available                      Yes             ICSF installation USERPARM        USERPARM
ICSF TKDS available                      Yes             Sysplex wide CKDS request         Yes
Clear key and PIN enabled                Yes             Sysplex wide CKDS else fail       No
Clear key and PIN enabled SAF            No              Sysplex wide PKDS request         Yes
PKCS#11 FIPS 140-2 compliant             No              Sysplex wide PKDS else fail       No
Use CRYPTO2 FIPSEXEMPT.token             No              Sysplex wide TKDS request         Yes
Abend if not FIPS140-2                   No              Sysplex wide TKDS else fail       No
X9.24 internal token wrapping            No              Message for archived keys         Yes
X9.24 external token wrapping            No              ICSF SAF checks priv caller       Yes
Check conditional ACL CSFKEYS             Yes             Resource name prefix support      Yes
KGUP label security CSFKEYS               Yes             Use SYSNAME prefix in CSFKEYS     Yes
KGUP require CSFSERV CSFKGUP             No              Use SYSNAME prefix in CSFSERV     Yes
```

Db2 Pervasive Encryption

- Db2 use of key labels
 - Encryption is at the data set level. Db2 passes desired keylabel when allocating.
 - System level (ZPRM) – Used for Db2 catalog, directories, and archive logs
 - Tables / Table spaces – The keylabel specified when creating a table
 - Storage groups – The keylabel for table and index spaces in this storage group

```
SYSL          DB2 region display
Command ==>
All DB2 region records

Region security settings
DB2 authorization checking      Yes      Return extended fail reason  Yes
AUTHEXIT check primary        Yes      DBA ca                        No
AUTHEXIT cache refresh all    No
Authorization exit module      DSN3@ATH Access
Signon exit module            DSN3@SGN
Classification Option          2 (1=single-subsystem, 2=multi-subsystem)
_ Class Name Root              DSN      Class Name suffix          1
Separate security tasks        No      Auth compat SELECT for UNLOAD No
Default encryption key label  DBC2LOGK
```



RE.K.S – Symmetric Key Protection – DB2 references

IBM Security zSecure ICSF_SYMKEY summary

Line 276 of 3227

Command ==>

Ver AES MKVP #systems #keys
2058C870E9D3194F 1 3227

Key data set
SYS1.CKDSP1R.DATA

Complex System #keys
UTCPLXJ8 JB0 3227

Volume Man Fa Serial Id #systems #keys
PPRD10 IBM-75-0000000XD261-0D3A 1 3227

HSM migrated data sets with this key

HSM backups of data sets with this key

DB2 ZPRM and Storage Groups with this key

	KeyType	CP	SMjk	SMS	DataSets	Migrated	Backups	DB2Sys	DB2Sto
ACTIVE	DATA	C	0	0	0	0	0	0	0
ARCHIVE	DATA	C	0	0	0	0	0	0	0
EXPIRED	DATA	C	0	0	0	0	0	0	0
NOCP	DATA	C	0	0	0	0	0	0	0
NOEND	DATA	C	0	0	0	0	0	0	0
NOMD	DATA	C	0	0	0	0	0	0	0
NOSTART	DATA	C	0	0	0	0	0	0	0
PREACTIV	DATA	C	0	0	0	0	0	0	0
PROHIBIT	DATA	C	0	0	0	0	0	0	0
RECALL	DATA	C	0	0	0	0	0	0	0
ACTIVE	CV	C	0	0	0	0	0	0	0
ARCHIVE	CV	C	0	0	0	0	0	0	0
EXPIRED	CV	C	0	0	0	0	0	0	0
NOCP	CV	C	0	0	0	0	0	0	0
NOEND	CV	C	0	0	0	0	0	0	0
NOMD	CV	C	0	0	0	0	0	0	0
NOSTART	CV	C	0	0	0	0	0	0	0
PREACTIV	CV	C	0	0	0	0	0	0	0
PROHIBIT	CV	C	0	0	0	0	0	0	0
RECALL	CV	C	0	0	0	0	0	0	0
ACTIVE	DATA	C	0	0	0	0	0	0	0
ARCHIVE	DATA	C	0	0	0	0	0	0	0
EXPIRED	DATA	C	0	0	0	0	0	0	0

RE.K.S – Symmetric Key Protection – reference counts

```
IBM Security zSecure ICSF_SYMKEY summary
Command ==>

Future use references          Current use counts
SAF DFP DATAKEY occurrences  2 DASD data sets under key          4
SAF JES KEYLABEL occurrences  0 Migrated data sets under key       4
SAF SSIGNON SSKEY occurrences  0 Backups encrypted under key       4
Data classes with key         0
DB2 sysparms under key        0
DB2 stogroups under key       0

Class      Resource
CSFKEYS    NMPIPL71.ZSECKEY8
Class      Profile
CSFKEYS    NMPIPL71.ZSECKEY8

UACC      IDSAcc  GlbAcc  Wrn Failure Success
NONE                               No  READ    READ
User      Access  ACL id   When                                     Name      DfltGrp  RI
-group-   READ    SUPERUSR
-group-   READ    CRMA      CRITERIA SMS=DSENCR
-group-   ALTER    CRMB      CRITERIA SMS=DSENCR
```

These counts are not in CKDS but enrichments by zSecure

Note that CSFKEYS prefixing with SYSNAME is active

This is the RACLIST merged Access List of all matching CSFKEYS and GCSFKEY profiles!

Clarify blank key label fields

Exploit new format
CHR\$STR('test')

Replaces empty key
label with clarifying text

```

RACF system view of data set encryption
Command ==>
Complex      System      Count  Encrypted  InPolicy  Usable
NM87         ZS14         491    488        437       481
KeyLabel
ZSECKEY8
Policy_datakey
no encryption policy
ZSECKEY8
*****
```

```

RACF system view of data set encryption
Command ==>
Complex      System      Count  Encrypted  InPolicy  Usable
NMPIPL71     ZS41         13     5          1
KeyLabel
unencrypted despite policy
ZSECKEY8
ZSECURE$20180416
*****
```


Extended zSecure Admin with a new feature

z/OS 2.4 support

RACF 2.4 new general resource segments

- Select on presence, absence, display of 3 new general resource segment types:
- CSDATA
- adds custom data fields
- IDTPARMS
- defines how to authenticate identity tokens
- JES
- defines how to encrypt JES spool

zsecure suite - RACF - Resource Segments		
Command ==>		
All profiles		
Only select general resource profiles with a specific segment:		
More:		
Select one segment		
—	CDTINFO	CDT Dynamic Class Descriptor Table data
—	CERTDATA	DIGTCERT Digital certificate data
—	CERTDATA	DIGTRING Digital certificate ring data
—	CFDEF	CFIELD Custom Fields
—	CSDATA	any class Custom defined data
—	DLFDATA	DLFCLASS Data Lookaside Facility data
—	EIM	FACILITY/LDAPBIND Enterprise Identity Manager data
—	ICSF	xCSFKEY Integrated Cryptographic Facility data
—	ICTX	LDAPBIND ICTX Identity caching data
—	IDTPARMS	IDTDATA Identity Token data
—	JES	JESJOBS JES Spool encryption data
—	KERB	REALM Kerberos Realm data
—	MFPOLICY	MFADEF Multi Factor Authentication Policy
—	PROXY	FACILITY/LDAPBIND LDAP proxy server data
—	SESSION	APPCLU Session data
—	SIGVER	PROGRAM Program signature data

RACF 2.4 new segments

General Resource Segment Summary

zSecure Suite Display Selection

Command ==> _____

Name	Summary	Records	Title
_ BASE	52	1824	zSecure Suite General resource overview
_ DIGTCERT	77	77	zSecure Suite DIGTCERT CERTDATA segments
_ DIGTRING	43	43	zSecure Suite DIGTRING CERTDATA segments
_ CDTINFO	1	1	zSecure Suite CDT CDTINFO segments
_ CFDEF	13	13	zSecure Suite CFIELD CFDEF segments
_ CSDATA	8	8	zSecure Suite CSDATA segments
_ IDTPARMS	12	12	zSecure Suite IDTDATA IDTPARMS segments
_ JES	6	6	zSecure Suite JESJOBS JES segments
_ PROXY	1	1	zSecure Suite FACILITY/LDAPBIND PROXY segments
_ SSIGNON	5	5	zSecure Suite PTKDATA SSIGNON segments
_ SESSION	10	10	zSecure Suite APPCLU SESSION segments
_ STDATA	417	417	zSecure Suite STARTED STDATA segments

***** Bottom of Data **

RACF IDTPARMS segment for identity token verification

Selection panel

```
IDTDATA selection
PKCS#11 token name      . . . _____
Token sequence number .  __  _____ (operator+value)
Signing token category  _____
Signature algorithm(s)  _  HS256      _  HS384      _  HS512
Any application . . . .  __  (Yes/No)
Timeout in minutes . .  __  _____ (operator+value 1..1440)
```

Overview panel

zSecure Suite IDTDATA IDTPARMS segments								
Command ==> _____								
All profiles with segment IDTPARMS								
	Profile key	SigToken	Seqnum	Cat	SigAlg	Any	Time	Complex
__	JWT.ZSECURE.CRMBRL1.SAF	RVDL.IDENTITY.TOKEN	00000001	__	__	YES	5	DCEIMGJB
__	JWT.ZSECURE.UNKNOWN.SAF	AHJB.TEST.\$TOKEN	00000006	__	__	YES	5	DCEIMGJB

RACF IDTPARMS segment for identity token verification

Detail panel with modifiable fields to define how an identity token of type 'JSON Web Token' must be verified by SAF for user id CRMBRL1 for application ZSECURE.

```
zSecure Suite IDTDATA IDTPARMS segments
Command ==> _____
All profiles

- Identification DCEIMGJB
  Profile name    JWT.ZSECURE.CRMBRL1.SAF
  Class          IDTDATA

  IDTPARMS segment
  Signing token name      RVDL.IDENTITY.TOKEN
  Signing token sequence number 00000001
  Signing token category  _____
  Id token signing algorithm  _____
  Id token for any application YES
  Id token timeout minutes  5
```

RACF JES segment - JES spool encryption keys

Selection panel

```
JES selection
Key label _____
```

Overview panel

```
zSecure Suite JESJOBS JES segments
Command ==> _____
All profiles with segment JES                                     14 Mar 2019
  Profile key                                     KeyLabel                                     Complex
_ ENCRYPT.DCEIMGJB.SUIMGJB.FTP$DCE2 ZSECURE.SPOOL.D2019Q1 DCEIMGJB
_ ENCRYPT.DCEIMGJB.UNKNOWN.FTP$DCE2 ZSECURE.SPOOL.D2019Q1 DCEIMGJB
```

Detail panel

```
zSecure Suite JESJOBS JES segments
Command ==> _____
All profiles with segment JES

_ Identification                                     DCEIMGJB
  Profile name                                     ENCRYPT.DCEIMGJB.SUIMGJB.FTP$DCE2.*
  Class                                             JESJOBS

  JES segment
  Data key label in ICSF                             ZSECURE.SPOOL.D2019Q1
***** Bottom of Data *****
```

Secured signon / passticket enhancements SSKEY KEYLABEL

- Now allow ICSF key label in SSIGNON SSKEY
- New fields
SSKEY_KEYLABEL
- SSKEY_CMDPARM

zSecure Suite KEYSMSTR/PTKTDATA SSIGNON segments			
Command ==>			
All profiles with segment SSIGNON			
Class	Profile	key	Key label for secured signon
KEYSMSTR	CRMBMB1.SSIGNON.TEST1		*MASKED*
KEYSMSTR	DCE.PASSWORD.KEY		*MASKED*
KEYSMSTR	DCE.PASSWORD.KEY		ZSECKEY8
KEYSMSTR	LDAP.BINDPW.KEY		*MASKED*
KEYSMSTR	LDAP.BINDPW.KEY		*MASKED*
KEYSMSTR	RONALD.TEST		*MASKED*
PTKTDATA	AHJBTEST.ENCR		*KEYTOKEN*
PTKTDATA	AHJBTEST.ENCR.2		*KEYTOKEN*
PTKTDATA	CFZAPPL		*MASKED*
PTKTDATA	CRMBMB1.SSIGNON.KEYMASKED		*MASKED*
PTKTDATA	CRMBMB1.SSIGNON.TEST1		*MASKED*
PTKTDATA	CRMBMB1.SSIGNON.TEST1		KEY
PTKTDATA	CRMBMB1.SSIGNON.TEST2		TEST223
PTKTDATA	FEKAPPL		*MASKED*
PTKTDATA	GPMSEVERE		*MASKED*
PTKTDATA	MVSKERB		*MASKED*
PTKTDATA	MVSKERB		*MASKED*
PTKTDATA	NEW		
PTKTDATA	OMVSAPPL		*MASKED*
PTKTDATA	RONALD.ENCRYPTED		*KEYTOKEN*
PTKTDATA	RONALD.MASKED		*MASKED*
PTKTDATA	RONALD.NOKEY		
PTKTDATA	RONALD.TESTKEY		*MASKED*
PTKTDATA	SAHEEM1		*MASKED*
PTKTDATA	SKRBKDC		*MASKED*
PTKTDATA	SKRBKDC		*MASKED*
PTKTDATA	TEST.SSIGNON.KEYENCRYPTED		*KEYTOKEN*
PTKTDATA	TEST.SSIGNON.KEYLABEL		ZSECKEY8
PTKTDATA	TEST.SSIGNON.KEYLABEL01		@
PTKTDATA	TEST.SSIGNON.KEYLABEL06		@23456
PTKTDATA	TEST.SSIGNON.KEYLABEL64		@234567890123456789012345678901
PTKTDATA	TEST.SSIGNON.KEYMASKED		*MASKED*
PTKTDATA	TEST.SSIGNON.KEYUNKNOWN		*HIDDEN*
PTKTDATA	TEST.SSIGNON.NOSSKEY		
PTKTDATA	ZSECURE.KEYLABEL		THISISATESTOFCRMBVK1
PTKTDATA	ZSECURE.KEYMASKED		*MASKED*

Secured signon / passticket enhancements SSKEY KEYLABEL

- Action command K extended

```
zSecure Suite - PTKTDATA key value

Command ==> _____

Class . . . : PTKTDATA
Profile key : CRMBMB1.SSIGNON.TEST1

Select the method you want to use to protect the key value
1 1. Mask the key value using the masking algorithm
   2. Encrypt the key using ICSF
   3. Set an existing CKDS key label
   4. Convert masked key to encrypted using ICSF

Key value . . : _____ (16 hexadecimal characters)
Key label . . : _____
```


Resource Custom Data

Selection panel

```
GENERAL RESOURCE CSDATA segment selection
  Field name  Field value
-  _____  _____
-  _____  _____
-  _____  _____
-  _____  _____
-  _____  _____
-  _____  _____
-  _____  _____
-  _____  _____
```

Detail panel

```
zSecure Suite CSDATA segments
Command ==> _____
All profiles with segment CSDATA

_ Identification DCEIMGJB
  Profile name    UI.TESTDATA.TEST2
  Class          XFACILIT

  Custom data
_ COMMENTS = Just some text in the XFACILIT class to test with
_ PRODUCT = Test product value 2
_ VESFLDT= asdf
```

RACF 2.4 new DATASET profile segments

Select on presence,
absence, and display of
new segment:

CSDATA
adds custom data fields

```
zSecure Suite - RACF - Data set Segments

Command ==> _____
All profiles
Only select dataset profiles with a specific segment:

Select one segment
_ CSDATA Custom defined data
_ DFP Data set encryption and allocation policies
_ TME Tivoli role data
```

DATASET Custom Data

Selection panel

```
zSecure Suite - Data set - Segment selection

Command ==> _____

DATASET CSDATA segment selection
  Field name  Field value
-  _____  _____
-  _____  _____
-  _____  _____
-  _____  _____
-  _____  _____
-  _____  _____
```

Detail panel

```
zSecure Suite DATASET CSDATA segments

Command ==> _____
All profiles with segment CSDATA

_ Identification                                     DCEIMGJB
  Data set profile                                CRMBRL1.**

  Custom Data
_ COMMENTS = Just some text in the DATASET class to test with
_ PRODUCT = zSecure Suite
***** Bottom of Data *****
```

SMF

- Success logging now includes conditional ACL CRITERIA if used
 - Field RECORDDESC:
RACF ACCESS success for CRMBJU1: (READ,READ) with criteria SMS=DSENCRYPTION on CSFKEYS ZSECKEY8
 - New field CRITERIA shown with default prefix header:
Criteria condition satisfied SMS=DSENCRYPTION
- Identity token status and service return code
- More ICSF record detail
- More DB2 SMF record detail
- More SMF 90 suport
- Watch this space

Extended zSecure Audit with a new feature

File Integrity Monitoring

With zSecure, you can find changes in the trusted computing base

How do I find backdoors?



Upgrade data set modification detection

Added NIST approved modification detection algorithms to CKFCOLL checksum feature.

Exploit CPACF feature on z12, z13, z14.

Using CPACF is much quicker than OLD!

```
CHECK_ALGORITHM=  
[OLD  
| SHA-1  
| SHA2-224 | SHA2-384 | SHA2-512  
| SHA3-224 | SHA3-256 | SHA3-384 | SHA3-512]
```

Not in base ESP level, wait for ESP PTF

File Integrity Monitoring

Two types of fingerprint:

<sample display coming>

- same across customers:

FINGERPRINT

-different across customers:

ANTI_TAMPER_DIGEST

Typical use:

Compare fingerprint against 'golden' version

Compare anti tamper digest with yesterday

Extended zSecure Audit with a new feature

Parallel UNIX File System collection

With zSecure, you can review UNIX security

**I want to
audit UNIX
but it takes
hours**



Parallel UNIX file system collection

It can take hours to review the security of all UNIX file systems.

File systems are read sequentially by CKFCOLL.

Solution:

1. apply the

PARALLEL= [NONE | PATHGROUP | PATH]

keyword also to UNIX file systems

2. Introduce multi-tasking in CKFCOLL

Not in base ESP level, wait for ESP PTF

Enhance zSecure Audit productivity

- **Compliance
framework
enhancements**

Merge DB2 zparm configured authid privileges

Add to DB2_ACCESS for compliance checks

Add to DB2_ACL displays

Add to RACF_DB2_ACL for modifiers:

EXPLODE RESOLVE EFFECTIVE

Columns H and L set to Z
Grantor is fixed field name
LastGranted is empty

DB2 region display													
Command ==>													
All DB2 region records													
Userid	ACOSD	AC	DPQ	SACSLT	ARB	BA	TMN	DES	Grantee>>	LastGranted	H	L	Grantor
-group-	..O..	..	DP.R.	..	T..	...	SYSOPR	1Apr85 00:00:00			SYSIBM
CRMBJK1	a....	..	DP.R.	..	T..	...	CRMBJK1	80Oct15 16:02:41	S		SYSADM
IBMUSER	a....	..	DP.R.	..	T..	...	IBMUSER	22Jul14 07:34:33	S		SYSADM
IBMUSER	...S.	..	DP.R.	..	T..	...	IBMUSER		Z	Z	ZPRM_SECADM1
LOUIS	a....	..	DP.R.	..	T..	...	LOUIS	22Jul14 07:34:33	S		SYSADM
ROOT	A..S.	..	DP.R.	..	T..	...	ROOT		Z	Z	ZPRM_SYSADM2
SYSADM	A..S.	..	DP.R.	..	T..	...	SYSADM		Z	Z	ZPRM_SYSADM
SYSADM	...S.	..	DP.R.	..	T..	...	SYSADM		Z	Z	ZPRM_SECADM2
USER1	..O..	..	DP.R.	..	T..	...	USER1		Z	Z	ZPRM_SYSOPR1
USER2	..O..	..	DP.R.	..	T..	...	USER2		Z	Z	ZPRM_SYSOPR2

DB2 region display													
Command ==>													
All DB2 region records													
Userid	ACOSD	AC	DPQ	SACSLT	ARB	BA	TMN	DES	Grantee>>	LastGranted	H	L	Granto
CRMBVK1	..O..	..	DP.R.	..	T..	...	SYSOPR	1Apr85 00:00:00			SYSIBM
CRMBVK2	..O..	..	DP.R.	..	T..	...	SYSOPR	1Apr85 00:00:00			SYSIBM
CRMBWP1	..O..	..	DP.R.	..	T..	...	SYSOPR	1Apr85 00:00:00			SYSIBM
CRMBWP2	..O..	..	DP.R.	..	T..	...	SYSOPR	1Apr85 00:00:00			SYSIBM
IBMUSER	a..S.	IBMUSER	22Jul14 07:34:33	S		SYSADM
LOUIS	a....	LOUIS	22Jul14 07:34:33	S		SYSADM
M80FCHIN	..O..	..	DP.R.	..	T..	...	SYSOPR	1Apr85 00:00:00			SYSIBM
M80FMSTR	..O..	..	DP.R.	..	T..	...	SYSOPR	1Apr85 00:00:00			SYSIBM
RCCSLIN	..O..	..	DP.R.	..	T..	...	SYSOPR	1Apr85 00:00:00			SYSIBM
ROOT	A..S.	ROOT		Z	Z	ZPRM_SYSADM2
STRCHIN	..O..	..	DP.R.	..	T..	...	SYSOPR	1Apr85 00:00:00			SYSIBM
STRTASK	..O..	..	DP.R.	..	T..	...	SYSOPR	1Apr85 00:00:00			SYSIBM
SYSADM	A..S.	SYSADM		Z	Z	ZPRM_SYSADM
USER1	..O..	USER1		Z	Z	ZPRM_SYSOPR1
USER2	..O..	USER2		Z	Z	ZPRM_SYSOPR2

UNIX file protection check symlink support

Selection of a file name now can
resolve symlink and variables

More automation for ZUSS category of
STIG controls

ACF2 STIG coverage

>66%

Interactions & Dependencies

- To exploit this item, all systems in the Plex must be at the new z/OS level: No
- Software Dependencies
 - Basic ISPF available
- Hardware Dependencies
 - Minimum level z196 for 31 bit operation, z12 for 64 bit operation
- Exploiters
 - Not specific to release

Migration & Coexistence Considerations

- AU.C ('Change Track') has been removed - use compliance assertion framework instead (AU.R) or other displays with 'Show differences'.
- Possible migration action: CKRCARLA internally called CKR4Z or CKR8Z196, now it calls CKR4Z196 and CKR8Z12. It has always been the advice to use CKRCARLA, which dynamically selects the module.
- Migration checksum boundary:
 - First use OLD to compare for changes with previous release
 - Change of checksum algorithm will cause all members / data sets to be seen as changed
- Toleration/coexistence APARs/PTFs: none expected.
- Coexistence: compiled for z/OS V2R1 and up. CKNSERVE can communicate with older versions on different nodes, but new functionality will be ignored on these nodes.

Installation

- Normal SMP/E installation, see installation & configuration manual.
- PTFs with new function will follow

Deliverables for zSecure V2R4 ESP

- PDF files of most zSecure publications for V2R4 are delivered much the same way as z/OS V2R4 publications.
- If you are a registered ESP participant and signed in, you will also have access to the zSecure licensed publications:
 - zSecure Admin and Audit for RACF User Reference Manual
 - zSecure Audit for ACF2 User Reference Manual
 - zSecure Audit for Top Secret User Reference Manual
 - zSecure CARLa Command Reference
- Excluded from ESP: Getting Started guides (RACF and ACF2) and the flyer (line and primary commands, RACF only).
- zSecure PDF files can be downloaded individually or in groups (“bulk download”).
- zSecure PDF files are updated at any time, whenever technical updates are completed and documented.
You can subscribe to a deliverable to receive a daily email with updates; if there are no updates, no email is sent.

Note: The zSecure deliverables will also be available through the IBM Knowledge Center after 30 September 2019.

<https://www.ibm.com/servers/resourcelink/svc00100.nsf/pages/zSecureV240Library?OpenDocument>

Session Summary

- zSecure Admin
 - New Command and Ticket logging feature
 - RACF 2.4 support 1 new DATASET segment, 3 new GENERAL segments
- zSecure Audit
 - Crypto audit enhancements (ICSF, DB2, clarifications)
 - File Integrity Monitoring feature
 - Improve UNIX file system data collection performance
 - Compliance framework enhancements (replace AU.C, ACF2 STIG, USS)
- zSecure Command Verifier
 - Invoke zSecure Admin Command and Ticket logging

Appendix

Contact:

Hans Schoone, STSM, Chief Architect zSecure and Manager Netherlands Lab

Hans.Schoone@nl.ibm.com

www.ibm.com/software/security/products/zsecure