#SHAREorg

SHARE
Technology · Connections · Results

Hear What's New with CA Mainframe Security

Carla A. Flores

ca technologies

March 15, 2012
Session Number 10207

Visit www.SHARE-SEC.com for more information on the SHARE Security & Compliance Project

legal notice

THIS PRESENTATION IS FOR YOUR INFORMATIONAL PURPOSES ONLY. CA assumes no responsibility for the accuracy or completeness of the information. TO THE EXTENT PERMITTED BY APPLICABLE LAW, CA PROVIDES THIS DOCUMENT “AS IS” WITHOUT WARRANTY OF ANY KIND, INCLUDING, WITHOUT LIMITATION, ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NONINFRINGEMENT. In no event will CA be liable for any loss or damage, direct or indirect, in connection with this presentation, including, without limitation, lost profits, lost investment, business interruption, goodwill, or lost data, even if CA is expressly advised of the possibility of such damages.

Certain information in this presentation may outline CA’s general product direction. This presentation shall not serve to (i) affect the rights and/or obligations of CA or its licensees under any existing or future written license agreement or services agreement relating to any CA software product; or (ii) amend any product documentation or specifications for any CA software product. The development, release and timing of any features or functionality described in this presentation remain at CA’s sole discretion.

Notwithstanding anything in this presentation to the contrary, upon the general availability of any future CA product release referenced in this presentation, CA may make such release available (i) for sale to new licensees of such product; and (ii) in the form of a regularly scheduled major product release. Such releases may be made available to current licensees of such product who are current subscribers to CA maintenance and support on a when and if-available basis.

Agenda

- CA Mainframe Security Release Status
- CA ACF2™ for z/OS & CA Top Secret® for z/OS r15 Overview
- CA Mainframe Security Product Update
- Open Discussion/Questions

Note: Specific examples of some features are in an Appendix section at the end of this presentation

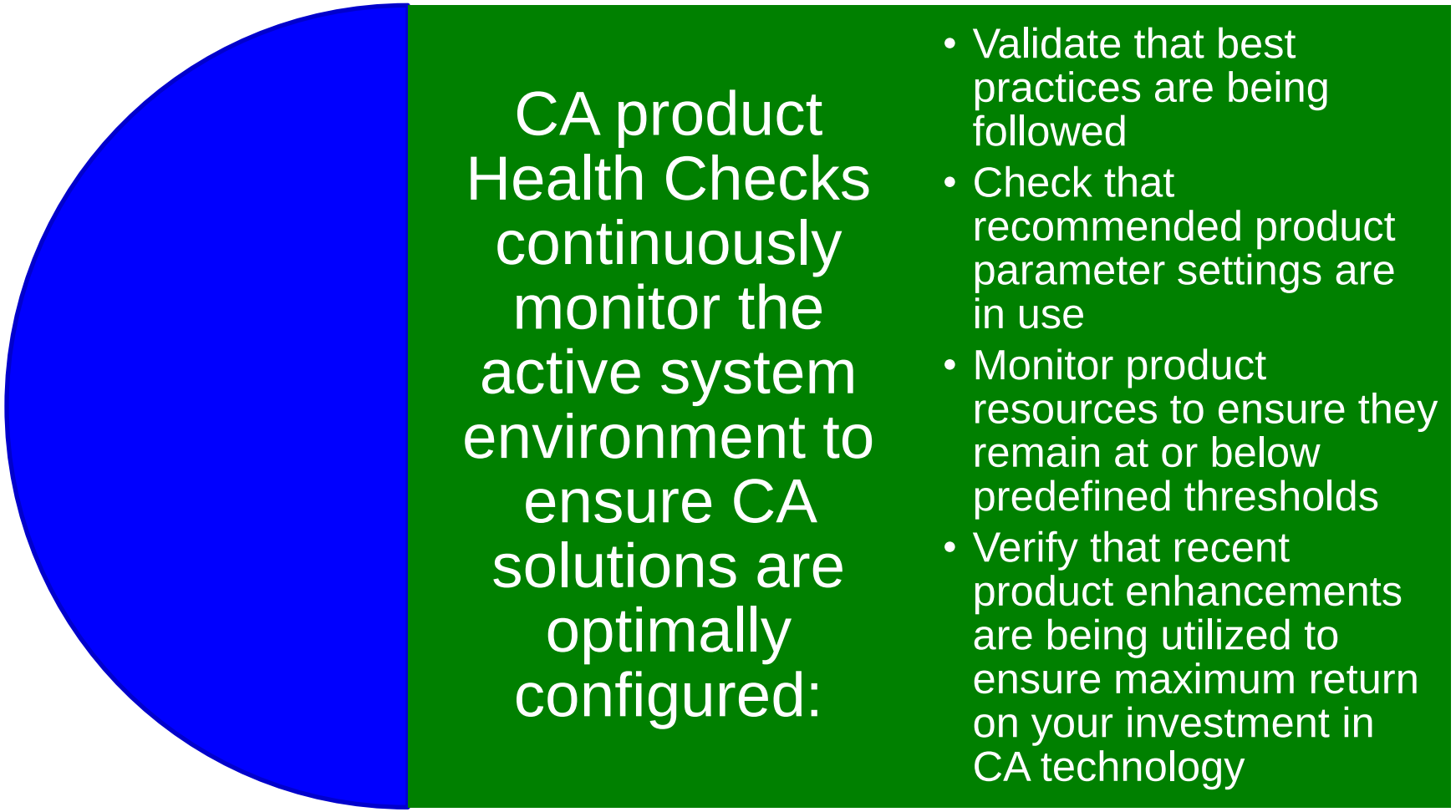
Release status

- CA ACF2 & CA Top Secret r15 – 9/2010
- CA ACF2 & CA Top Secret r14 sp1 – 2/2010
- CA ACF2 / CA Top Secret r12 – End of Service 3/1/2011
- CA ACF2 & CA Top Secret r1.3 for DB2 – 6/2010
- CA ACF2/VM & CA Top Secret/VM r12 sp3 – 02/2012
- CA Cleanup r12 sp1 – 6/2010
- CA Auditor r12.1 – 6/2010
- CA Compliance Manager r2 – 11/2011
- CA Mainframe Chorus for Security and Compliance Management r2 – 12/2011

- EAL4+ Certification (CA ACF2, CA Top Secret, CA Compliance Manager – Complete

- http://www.ca.com/us/Support/mainframe-compatibilites/z196-Compatibility-Matrix.aspx

An overview of CA Security Health Checks



CA ACF2 Health Checks

ACF2 Health Checks

- ✓ Determine use of SAFDEFs with NOAPFCHK
- ✓ Determine if the CA ACF2 AUTO Start feature is in use (CAISEC00)
- ✓ Determine if volume contention exits with ACF2 Databases
- ✓ Exits

Leveraging the power of the z/OS Health Checker for your Security implementation

CA ACF2 Health Checks

ACF2 Health Checks

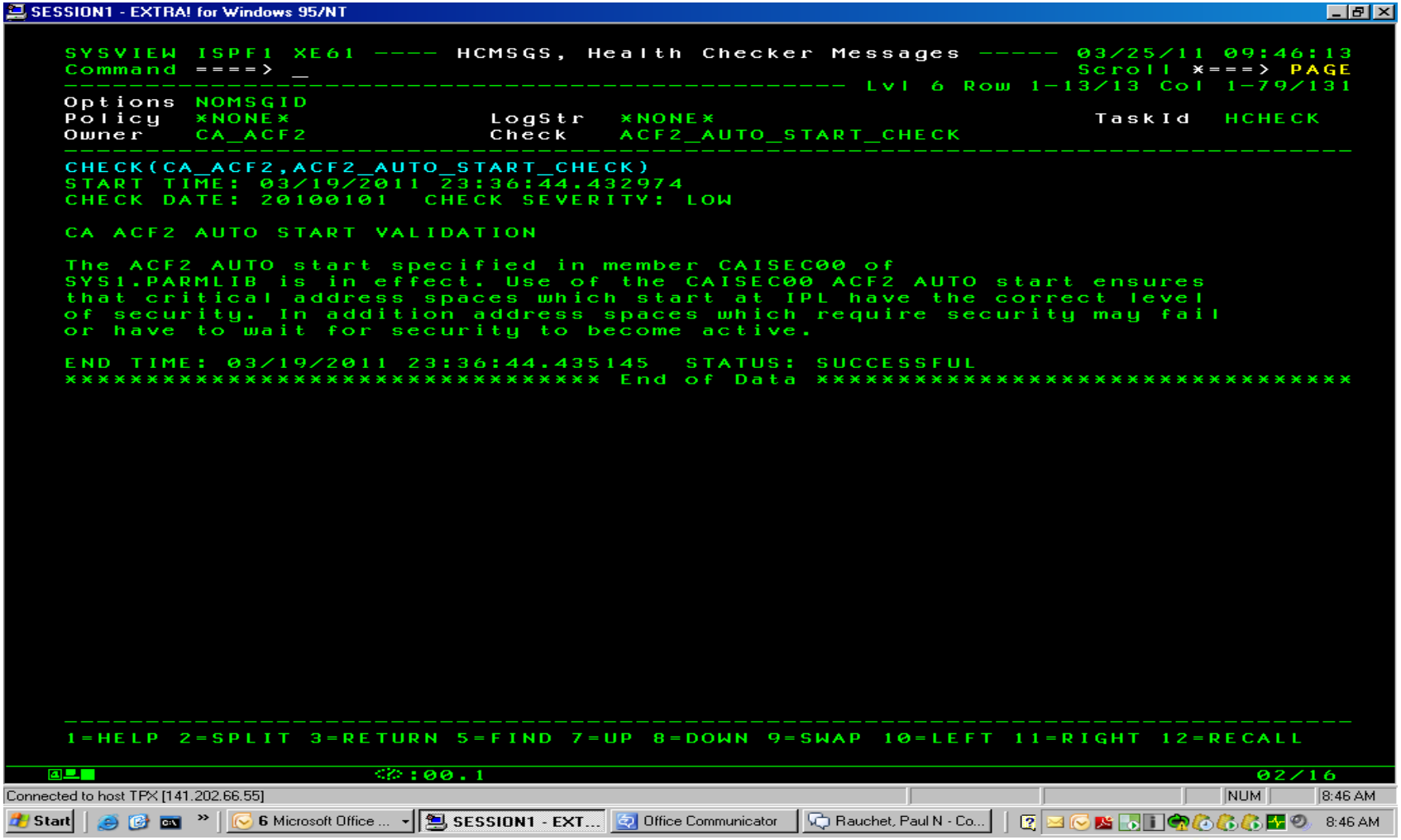
- ✓ Determine use of SAFDEFs with NOAPFCHK
- ✓ Determine if the CA ACF2 AUTO Start feature is in use (CAISEC00)
- ✓ Determine if volume contention exits with ACF2 Databases
- ✓ Exits

Leveraging the power of the z/OS Health Checker for your Security implementation

Benefit

- ✓ Reduces risk of user bypassing APF checking on RACROUTE calls
- ✓ Enables CA ACF2 to start early and ensures other Address Spaces that start during IPL will have correct level of security

CA ACF2 Health Check Sample



Top Secret Health Checks

Top Secret Health Checks

- ✓ Determine if CA Top Secret Audit Tracking file is allocated on same volume as the TSS Security File
- ✓ Determine if CA Top Secret CACHE and SECCACHE features are enabled

Leveraging the power of the z/OS Health Checker for your Security implementation

Top Secret Health Checks

Top Secret Health Checks

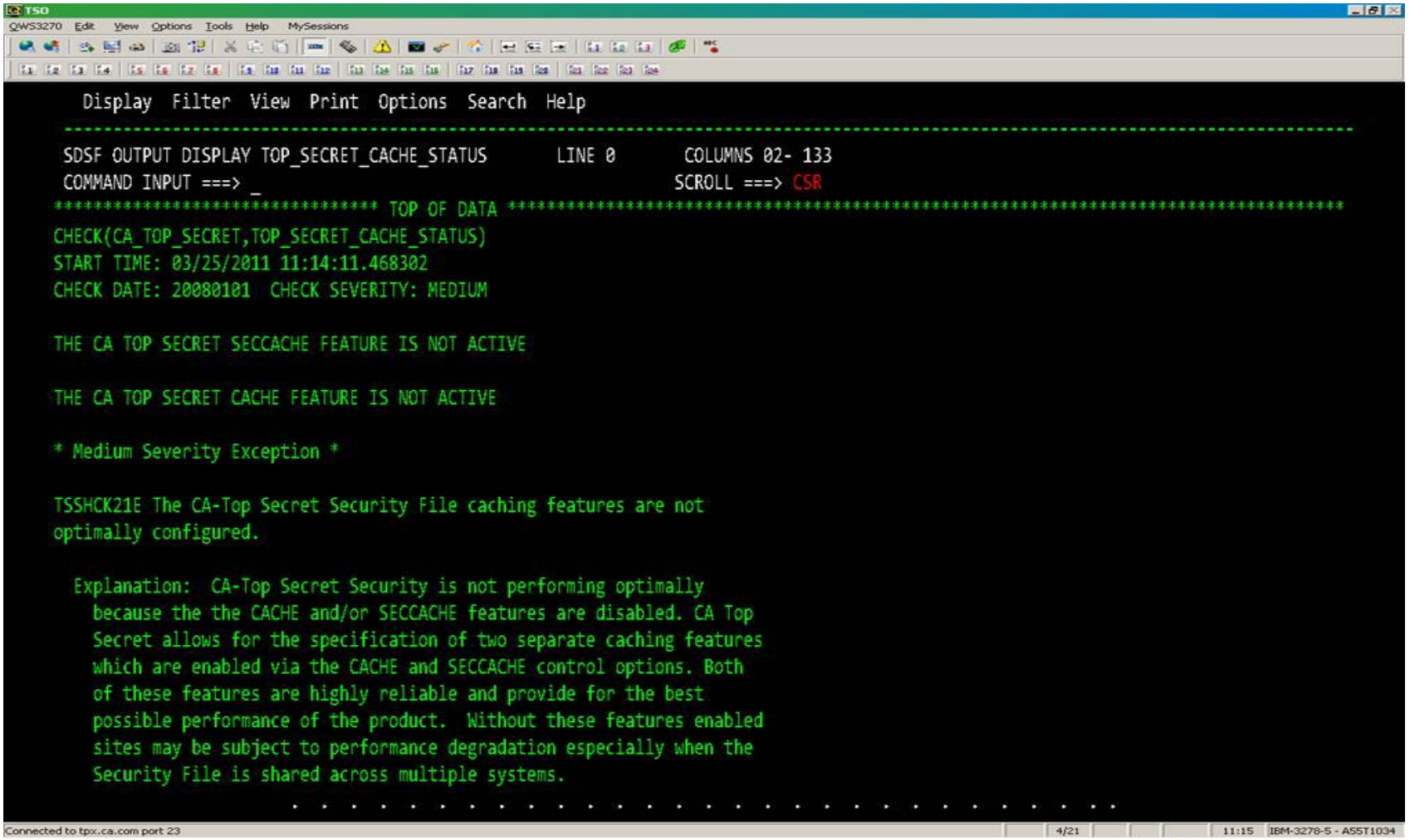
- ✓ Determine if CA Top Secret Audit Tracking file is allocated on same volume as the TSS Security File
- ✓ Determine if CA Top Secret CACHE and SECCACHE features are enabled

Leveraging the power of the z/OS Health Checker for your Security implementation

Benefit

- ✓ Reduces the number of support issues resulting from performance degradation when these two files share a DASD volume
- ✓ Helps prevent performance degradation by not using all of the product-supplied cache features

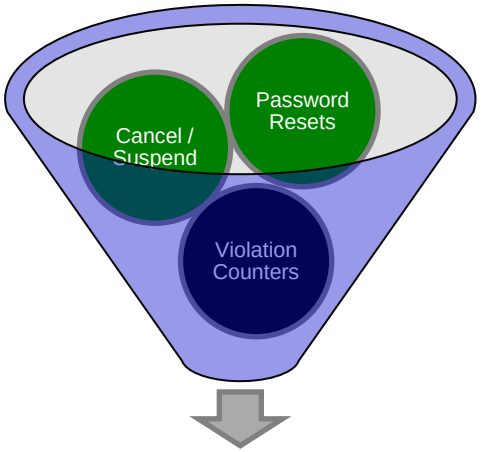
Top Secret Health Check Sample



SHARE
Technology · Connections · Results

CA ACF2 & CA Top Secret r15

Restricted administration controls



You can now control administration capabilities without high-level privileges being given (ie. Security, Account, Audit, MSCA, SCA, etc.)

- Initial target:
  - Passwords and password related fields
  - Administration of certificate commands
- New pre-defined resource class: CASECAUT
  - Internal CLASSMAP record with TYPE=AUT (CA ACF2)
  - NORESCHK not honored for CASECAUT class (CA Top Secret)
- Provide administration access through resource authorization
  - Cannot perform Administration on a higher-level user

Restricted administration controls (CA Top Secret)

- Allows a user other than MSCA to run TSSXTEND and TSSFAR
- Allows a user with no admin authorities to run utilities

New administration commands

- User Comparison
- User Modeling
- User Archival

Automated user comparison (CA ACF2)

- New ACF COMPARE command
  - Single command compares two users and displays differences
    - Compares logonids
    - Compares associated roles
    - Compares user profile segments
      - *CICS, EIM, LANGUAGE, NETVIEW, OPERPARM, SECLABEL, WORKATTR*
    - Syntax: COMPARE userid1 USING(userid2)
- Requirements
  - User must have SECURITY or AUDIT privileges
  - Logonids being compared must be within administrator's scope

Automated user modeling (CA ACF2)

- New ACF MODEL command
  - Copies subset of logonid fields, profiles, and roles from existing user
  - Builds commands to insert new user modeling existing user
  - Syntax: MODEL logonid(newuser) USING(modelid) INTO('pds(member)')
    - If INTO not specified, command output displayed to terminal
    - Administrators can MODEL any logonids within their scope

Automated user archiving (CA ACF2)

- NEW ACF2 ARCHIVE subcommand for LIST and DELETE commands
  - Builds ACF commands that recreate a user (Logonid and User Profiles)
  - Re-adds user to roles they were previously assigned to
  - Syntax: {LIST | DELETE} logonid ARCHIVE INTO('output.work.user(member)')
    - *If INTO not specified, command output displayed to terminal*
    - *Administrators can ARCHIVE any logonid within their scope*

Compare command enhancements (CA Top Secret)

- Description
  - New TSS COMPARE(ACID) USING(ACID) command will compare the two ACIDS and then display the differences to the screen.
- This command is treated like a list command
  - Administrators must have explicit authority via the ADMIN - DATA command
  - The compare command will only display output for the ACIDS within their scope

Administration user modeling (CA Top Secret)

- Description
  - MODEL command
    - Models permissions for datasets/resources from existing user acid to another user acid
    - Generates list of TSS commands
    - First record in output is comment, which contains:
      - *Command*
      - *User acid being modeled*
      - *Date and time of model*
      - *TSS administrator who issued command*
      - *System on which command was executed*
      - *User acid used as a model*

Administration archival (CA Top Secret)

- Description
  - Archival allows user's permissions and resources to be archived into form of TSS commands
  - Generated TSS commands can be stored in PDS dataset and used to restore a user
  - First record in output is a comment, which contains:
    - Command
    - User acid being modeled
    - Date and time of the archive
    - TSS administrator who issued command
    - System on which command was executed

Administration archival (CA Top Secret)

- Requirements
  - Specify ARCHIVE keyword on LIST or DELETE command
  - Administrator must have DATA(ALL) authority and scope over ACID being archived
  - Specify keyword INTO to have TSS commands written out to PDS
  - During archive processing, most of user's security record information is archived, but some fields are not copied during archive process (e.g., digital certificates)
  - Use EXPORT command
    - If user being archived has digital certificates

Certificate enhancements

- Renew Command
- IDN/SDN Extensions
- Certificate Utility Enhanced

Certificate RENEW command (CA ACF2)

- Renews digital certificate with one command
  - Provide certificate and new ‘expire’ date
  - Eases the administration from up to a six step process to one
  - Syntax: RENEW user.cert EXPIRE(12/31/11) SIGNWITH(my.ca)
- Requirements
  - Certificate & Signer of cert being renewed must have private key in CA ACF2 Info-Storage database or in ICSF (PKDS)

Certificate DN support (CA ACF2)

- Distinguished Name (DN) max sizes increased to accommodate larger CA certificate SDNs/IDNs
- GSO CERTMAP fields SDNFILTR and IDNFILTR increased to allow larger values up to 1024 bytes
- Notes:
  - Do not share INFOSTG database between systems without support
  - Specify SDNSIZE(1024) to activate large DN support only after ALL systems sharing INFOSTG have been upgraded

Certificate enhancements (CA ACF2)

- Expanded Key Ring Support
  - Limitation due to size of INFO-STORAGE Database
  - New User parameter on CONNECT or REMOVE “logically” connects or removes ALL certificates from a user keyring
- Password Prompt
  - Prompt for password if missing from CHKCERT, INSERT, or EXPORT command
- Expiring Certificate Warning
  - New GSO OPTS CERTEXP(days)
  - ACF79468 Certificate xxx.yyy is expiring in xx days

Certificate RENEW command (CA Top Secret)

- Renews digital certificate with one command
  - Provide certificate and new ‘expire’ date
  - Eases the administration from up to a six step process to one
  - Syntax: TSS RENEW(JOE1) DIGICERT(cert1) NADATE(12/31/10)
- Requirements
  - Certificate being renewed must have private key in CA Top Secret database or in ICSF
  - Signer of certificate being renewed must have private key in CA Top Secret database or in ICSF

Large DN support (CA Top Secret)

Requirements

- New maximum DN size is 1024 for Subject DN, 1007 for Issuer DN
- SDNFILTR and IDNFILTR have also been increased
- Large DN feature is incompatible with operating systems that do not have the support
- Sharing a security file between incompatible systems is not supported
- New SDNSIZE(255|1024) parameter will allow migration of all systems to the new support before allowing certificates with large DNs to be inserted or gencerted

Certificate utility enhanced (CA ACF2 & CA Top Secret)

- New fields displayed in Utility output

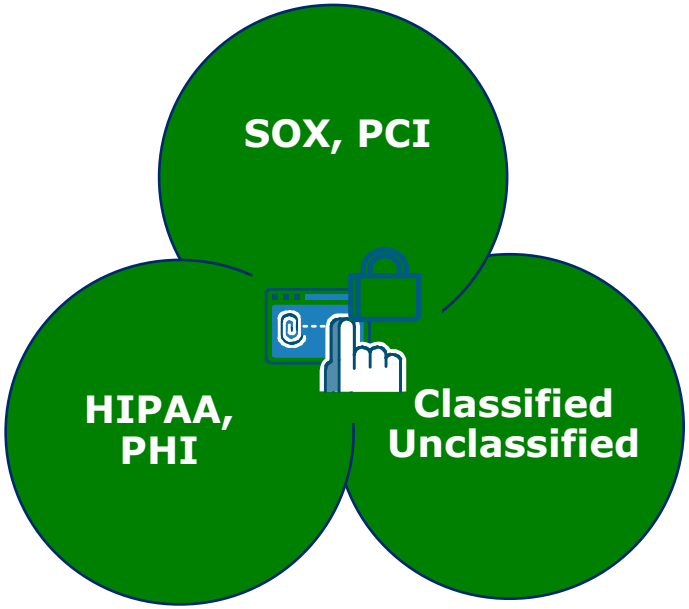
Field	Field Value Description
Algorithm	Signing algorithm
Trusted	Trust status (Yes or No)
Cert Length	Certificate length
Extensions	Contents of certificate extensions (Hex dump, if not common)

- New Totals displayed in Utility output

Totals Field	Totals Field Value Description
Trusted Certificates	Total number of trusted certificates
High Trust Certificates	Total number of high trusted certificates

Data classification enhancement

- Data Classification Enhancement
  - Add Data Classification and Ownerships to CA Compliance Manager Event Records and CA Mainframe Chorus for Security and Compliance Management



CA ACF2™ for z/OS Only

Role based security

- ACFXREF Utility changed to include XROL records
  - Manipulates Cross-reference XROL records and identifies invalid values on INCLUDE and EXCLUDE statements
  - Facilitates removal or restoration of roles and users that no longer exist from role definitions
- New output CMDS and BACKOUT files
  - Valid for all ACFXREF processing types (XROL, XSGP, XRGP)
  - CMDS output file
  - BACKOUT output file

Auto erase enhancements

- Erase-on-Scratch (EOS) support
- “Existing” method (ACF2 intercepts-based)
  - Erase processing done out of ACF2 ERASE intercepts
  - If using existing EOS method, ACF2 does the manual scratching
- “New” method (SAF-based)
  - Controlled by GSO AUTOERAS record – new PROCESS(SAF|ACF2)
  - Better control for user
    - Can control EOS centrally against all data sets via AUTOERAS record - at individual HLQ level & SECLEVEL for data classification records

TSO options

- New BYPPAUSE field
  - Bypasses CA ACF2 message prompt and pause during TSO SIGNON
  - Limits display of CA ACF2 informational messages during TSO logon
  - Incorporation of User Mod UM75289
  - Requirement: Must use CA ACF2 TSO Logon Routine
- New LOGHERE field
  - Allows TSO/E user who has a session on one terminal to log on to another terminal with the RECONNECT option and "steal" the session from the original terminal
  - Requirement: Must be at z/OS 1.11 or above

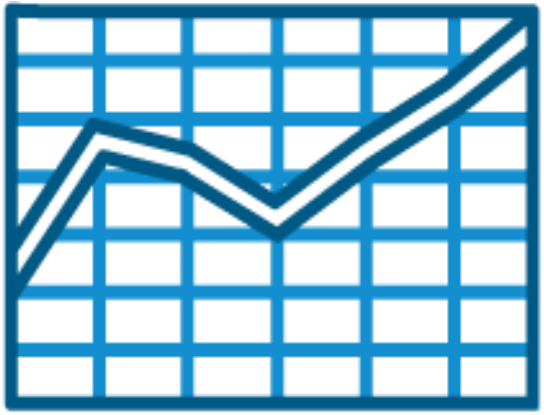
Misc enhancements

- DSERV Exit Support
  - PDSE support for PDS Member Level Protection and Program Pathing
- SHOW RSRCTYPE
  - Incorporated in Show All output

CA Top Secret® for z/OS Only

Virtual storage constraint relief (VSCR)

- Use of 64-bit storage above the bar



Auto Start

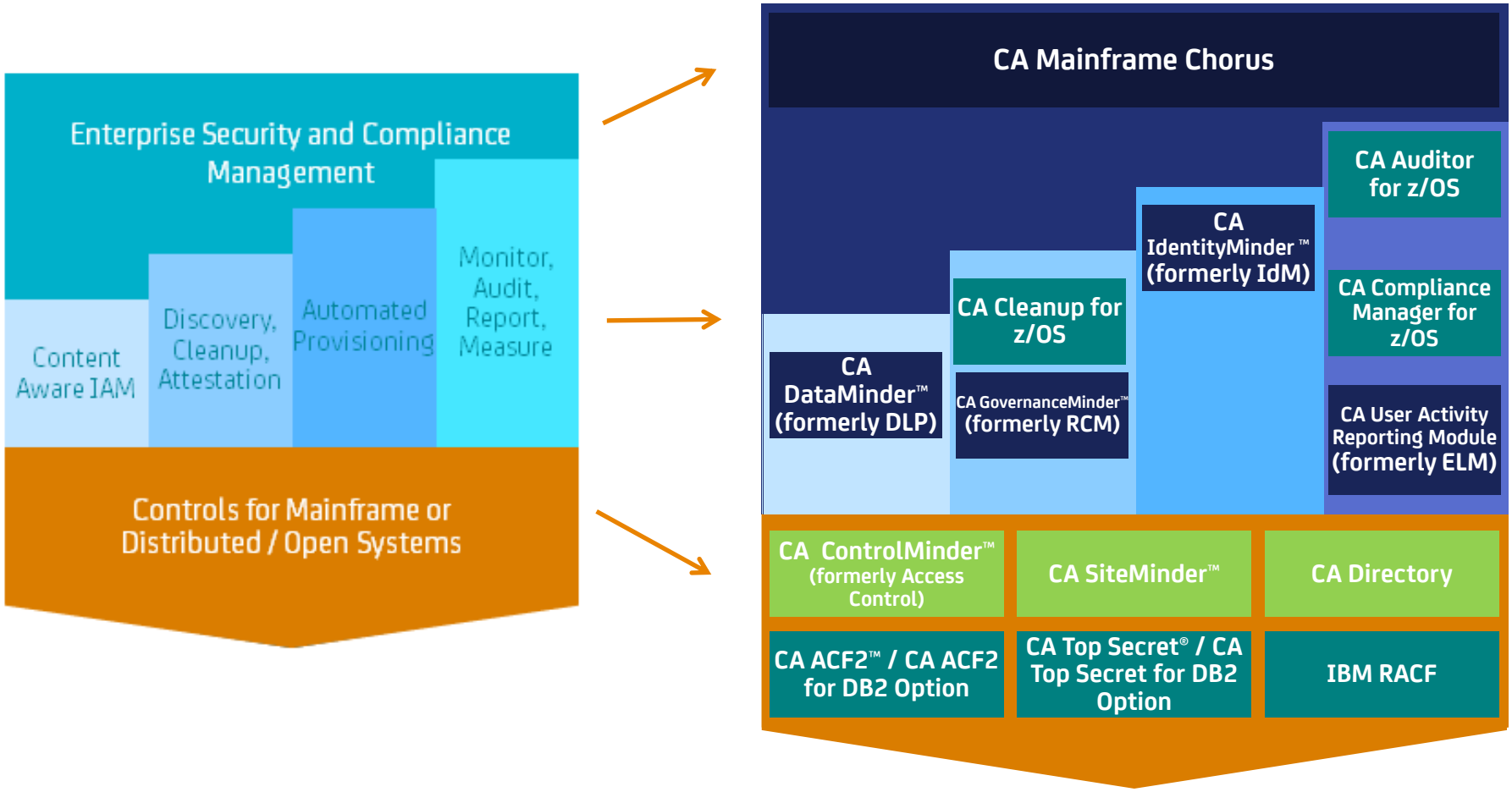
  - Support auto starting TSS as Subsystem
- Requirements
  - Support START/NOSTART in CAISECxx parmlib member
  - Allow control options overrides via CAITSSxx
  - Set subsystem name via SUBSYS= keyword
  - VERIFY issued by AXR is suspended by TSSSFR00
-

#SHAREorg

SHARE
Technology · Connections · Results

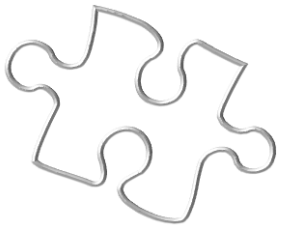
CA Mainframe Security Products

CA Mainframe Security Suite



CA Cleanup for (ACF2, Top Secret, RACF)

- Reports inactive users
- Reports unused security entitlements
- Provides capability to automatically enforce security policy by removing:
  - Inactive user definitions
  - Unused security entitlements
  - Obsolete security entitlements



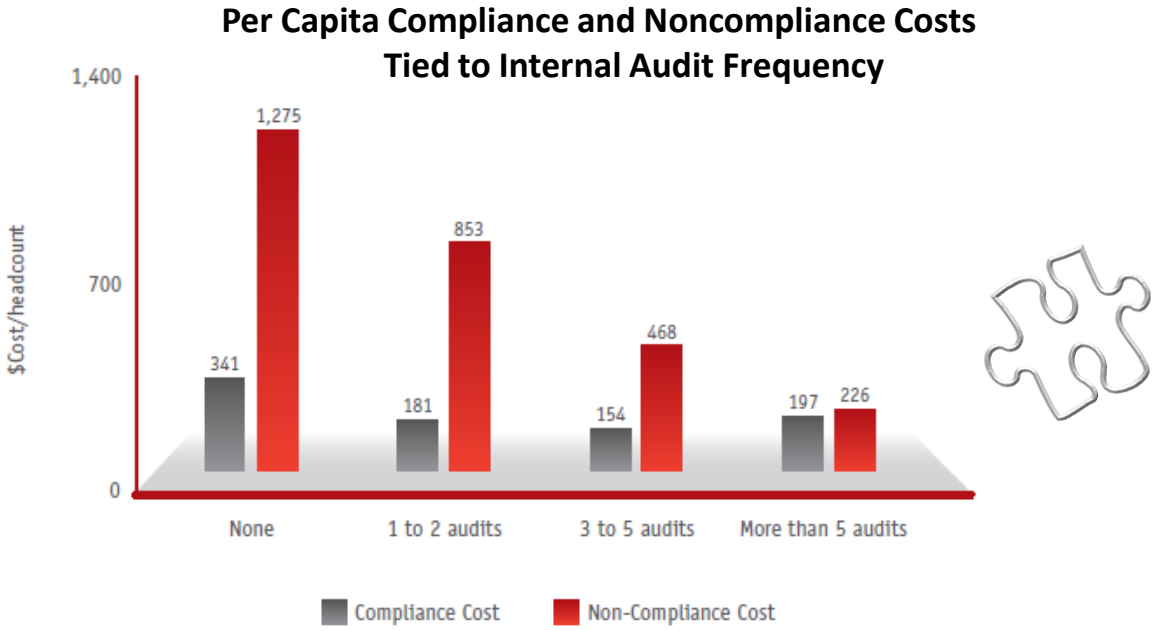
PCI Security Standards Council

PCI DSS Requirements	
8.3	Incorporate two-factor authentication for remote access (network-level access originating from outside the network) to the network by employees, administrators, and third parties. Use technologies such as remote authentication and dial-in service (RADIUS); terminal access controller access control system (TACACS) with tokens; or VPN (based on SSL/TLS or IPSEC) with individual certificates.
8.4	Render all passwords unreadable during transmission and storage on all system components using strong cryptography based on approved standards (defined in *PCI DSS Glossary, Abbreviations, and Acronyms*).
8.5	Ensure proper user authentication and password management for non-consumer users and administrators on all system components as follows:
8.5.1	Control addition, deletion, and modification of user IDs, credentials, and other identifier objects
8.5.2	Verify user identity before performing password resets.
8.5.3	Set first-time passwords to a unique value for each user and change immediately after the first use.
8.5.4	Immediately revoke access for any terminated users.
8.5.5	Remove/disable inactive user accounts at least every 90 days.
8.5.6	Enable accounts used by vendors for remote maintenance only during the time period needed.

CA Auditor for z/OS

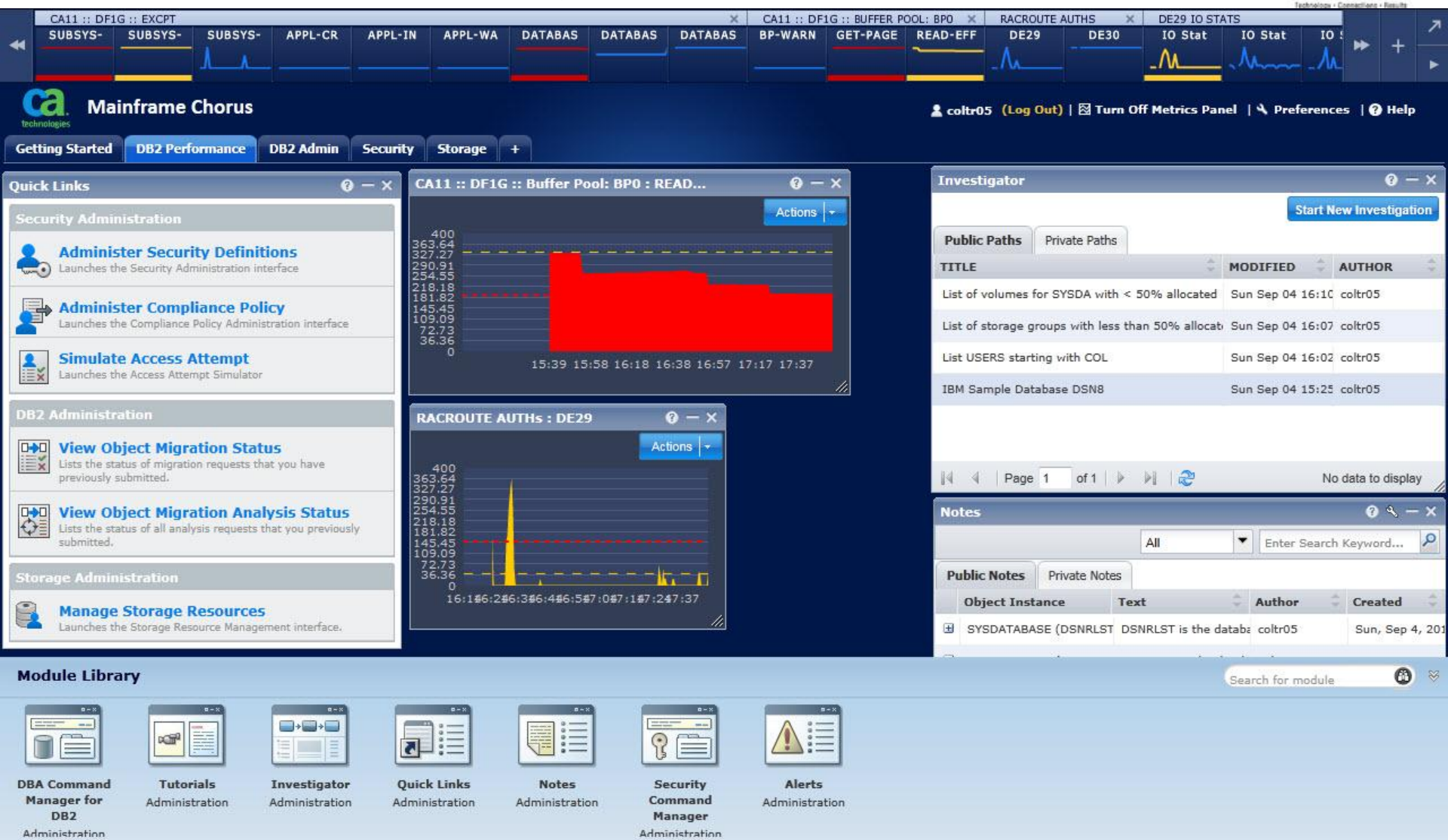
- Facilitates the review of OS resources and validates integrity without in-depth knowledge
- Helps provide that the integrity of your OS meets your corporate standards
- R12 now establishes audit baselines for *internal and external audits*

Data suggests organizations that perform internal audits on a frequent basis can reduce costs



Source: Ponemon Institute LLC, *The True Cost of Compliance*, Research Study, January 2011

CA Mainframe Chorus for Security and Compliance Management



Review

- Release Status
- CA ACF2 & CA Top Secret Enhancements
  - Compliancy Considerations
  - Administration Capabilities
  - Performance Enhancements
  - Incorporated DARs
- CA Mainframe Security Products
  - CA Cleanup
  - CA Auditor
  - CA Mainframe Chorus for Security and Compliance Management

#SHAREorg

SHARE
Technology · Connections · Results

Open Discussion – Q&A

Visit www.SHARE-SEC.com for more information on the SHARE Security & Compliance Project

Thank you!

Session #10207

Appendix

Sample output

CA ACF2 sample health check – expiring certificates

```
CHECK(CA_ACF2,ACF2_CHECK_EXPIRING_CERTS)
START TIME: 03/15/2010 12:19:07.557056
CHECK DATE: 20100101  CHECK SEVERITY: MEDIUM

CA ACF2 CHECK FOR EXPIRING DIGITAL CERTIFICATES

LIST OF DIGITAL CERTIFICATES EXPIRING WITHIN 30 DAYS

 CERTNAME=CERTAUTH.P11BND
 CERTNAME=CERTAUTH.P11DEL

   * Medium Severity Exception *

ACFHC051E At least one ACF2 Digital Certificate will expire in the next  30 days.

  Explanation:  There is one or more ACF2 Digital Certificate which will  expire in the next 30 days.

  System Action:  ACF2 continues processing.

  Operator Response:  Report this problem to the Security Administrator.

  System Programmer Response:  Have the security administrator review the ACF2 Digital Certificates.

  Problem Determination:  N/A

  Source:  ACF2

  Reference Documentation:  Please refer to chapter Digital Certificate  Support in the ACF2 Administrator Guide
  on the use of Certificates.
```

CA ACF2 sample – restricted administration controls

- Example: help desk admin

```
ACF75052 RESOURCE RULE ACFCMD STORED BY SECADM01 ON 03/22/10-09:00
 $KEY(ACFCMD) TYPE(AUT) ROLESET
  - USER.PASSWORD ROL(HLPDSK1) ALLOW
  - USER.PASSPHRASE ROL(HLPDSK1) ALLOW
  - USER.- ROL(HLPDSK2) ALLOW
 ACF75051 TOTAL RECORD LENGTH= 236 BYTES, 5 PERCENT UTILIZED


change user01 password(user01) passphrase(new passphrase)
ACF6C004 LOGONID  USER01  CHANGED
ACF6D070 PWPHRASE / USER01 RECORD CHANGED

change secadm password(secadm)
ACF00103 NOT AUTHORIZED TO CHANGE FIELD PASSWORD
```

CA ACF2 sample - restricted administration controls

- Example: certificate administration
  - Note: User DCADM1 is “unscoped” and can administer all certificate-related objects for any user

```
set r(aut)
 RESOURCE
comp * store
 ACF70010 ACF COMPILER ENTERED

 .  $KEY(ACFCMD) TYPE(AUT)
 .   DIGTCERT.- UID(DCADM1) SERVICE(READ,UPDATE,DELETE) LOG
 .
 ACF70051 TOTAL RECORD LENGTH= 158 BYTES, 3 PERCENT UTILIZED
 ACF60029 RESOURCE  ACFCMD STORED
 RESOURCE

f acf2,rebuild(aut),c(r)
 ACF8A037 DIRECTORY RAUT ADDED TO RESIDENT CHAIN
```

CA ACF2 sample – compare

```
ACF
Compare  JPETERS USING(JSMITH)

                  LID SECTION
 ------------------------------------------------------------------
  LID           JPETERS              JSMITH
  NAME          JAMES PETERS         JOHN SMITH
                TSO SECTION
 ------------------------------------------------------------------
  TSOPROC    CATSO             XXTSO
  DFT-PFX    PETERS              SMITH
                RESTRICTIONS SECTION
 ------------------------------------------------------------------
  PREFIX     PETERS              SMITH
  GROUP      DEFGRPA             DEFAULTG
               ROLES SECTION
 ------------------------------------------------------------------
            GROUPE              GROUPA
            GROUPH              GROUPC
                 CICS PROFILES
-------------------------------------------------------------------
 OPCLASS                        Y
 OPPRTY              0          255
 TIMEOUT VALUE       0           15
```

CA ACF2 sample – archive

```
ACF
model logonid(newuser) using(ACFUSER) into('MYPDS.FILE(OUTPUT)')

SET LID
INSERT NEWUSER  -
 PASSWORD(NEWUSER) -
 ACCOUNT  -
 ACCTPRIV -
 ALLCMDS  -
 TSOFSCRN -
 GROUP(DEFAULTG)-

SET PROFILE(USER) DIV(CICS)
INSERT NEWUSER -
 OPIDENT(CHI)-
 OPPRTY(255)-
 TIMEOUT(60)-

F ACF2,REBUILD(USR),CLASS(PROFILE)

SET X(ROL)
CHANGE GROUPA  -
INCLUDE(NEWUSER)

F ACF2,NEWXREF,TYPE(ROL)
END
```

CA ACF2 sample - archive

```
ACF
delete newuser archive into('mypds.out(listarch)')

ACF
SET LID
INSERT NEWUSER  -
 PASSWORD(NEWUSER) -
 ACCOUNT  -
 ACCTPRIV -
 ALLCMDS  -
 AUDIT    -
 CICS     -
 GROUP(DEFAULTG)-

SET PROFILE(USER) DIV(CICS)
INSERT NEWUSER -
 OPIDENT(CHI)-
 OPPRTY(255)-
 TIMEOUT(60)-

F ACF2,REBUILD(USR),CLASS(PROFILE)

SET X(ROL)
CHANGE GROUPA  -
INCLUDE(NEWUSER)
CHANGE GROUPC  -
INCLUDE(NEWUSER)
F ACF2,NEWXREF,TYPE(ROL)
END
```

CA ACF2 sample - role based security

```
CA ACF2                - XREF CLEANUP REPORT
DATE 02/24/10 (  10.055 ) TIME   18.32                    PAGE     1


RESOURCE(XROL)     GROUP       SYSID(LONG)       RECID - USERGRP
DESCRIPT(USER GROUP ROLE)
LIST OF INCLUDE VALUES:
USER-
LIST OF EXCLUDE VALUES:
PGMR04
PGMR03
PGMRJ02              -- VALUE NOT FOUND
LIST OF VALUES THAT MATCHED MASK:   USER-
USER4              USER1
USER3              USERSC
USER2              USERGRP
```

CA Top Secret sample - restricted administrative authorities

- User DCA01 is allowed to change passwords

```
tss add(sysdept) casecaut(tsscmd.user)
 TSS0300I  ADD      FUNCTION SUCCESSFUL
tss per(DCA01) casecaut(tsscmd.user.replace.password) access(update)
 TSS0300I  PERMIT   FUNCTION SUCCESSFUL
tss list(DCA01) data(admin)
 ACCESSORID = DCA01     NAME       = DCA
 ----------  ADMINISTRATION AUTHORITIES
LIST DATA  = BASIC,NAMES
----------  RESTRICTED ADMINISTRATION AUTHORITIES
 XA CASECAUT= TSSCMD.USER.REPLACE.PASSWORD              OWNER(SYSDEPT )
   ACCESS  = UPDATE
```

CA Top Secret sample - restricted administrative authorities

- User DCA01 is allowed to run TSSUTIL

```
tss add(sysdept) casecaut(tssutility)
 TSS0300I  ADD      FUNCTION SUCCESSFUL
tss per(DCA01) casecaut(tssutility.tssutil) access(use)
 TSS0300I  PERMIT   FUNCTION SUCCESSFUL
tss list(DCA01) data(xauth)
 ACCESSORID = DCA01     NAME       = DCA
 XA CASECAUT= TSSUTILITY.TSSUTIL                    OWNER(SYSDEPT )
   ACCESS  = USE
   ADMIN BY= BY(MASTER  )    SMFID(XE05)   ON(02/18/2010)  AT(11:03:38)
```

CA Top Secret sample – compare

```
TSS COMPARE(CMPACD2) USING(CMPACDB)
ACID      CMPACD2                    | CMPACDB
DEPTMENT  COMPDEP2                   | COMPDEPT
DIVISION                             | COMPDIVI
ZONE                                 | COMPZONE
---------- Profiles are different or in a different order starting with.
          KRACPROF                   |
LANGUAGE                             | F
---------- SOURCE
          ANOTHER8                   |
          CHAR5                      |
          C2                         |
          FOUR                       |
---------- OPERCLAS                  |
          02                         |
          05                         |
          06                         |
PHYSKEY                              | ADDINGTOACHARACTER
---------- DEFNODES
          LA                         |
          PHI                        |
-----------   SEGMENT OMVS   -----------
ASIZE                                | 2147483647
```

CA Top Secret sample – compare

- Example (TSS COMPARE COMMAND)

```
---------- Facility differences for Acid CMPACDB
FACILITY  = MQM
DAYS =      TUE   THU   SATSUN TIME =ANY
 ACTIONS = FAIL

---------- Permit Differences for ACID  CMPACD2
 XA DATASET   CMPACD1.WORK
EXPIRE(04/12/10  )
 ACCESS=UPDATE
XA DATASET = KAUGE01.BOZO
ACCESS=READ
```

CA Top Secret sample – archive

- Example (implementation)

```
TSS LIST(Rachael) ARCHIVE

TSS LIST(Cassie) ARCHIVE INTO(KOTPA01.ARCHIVE.CASSIE)

TSS LIST(Jonathan) ARCHIVE INTO(KOTPA01.ARCHIVE.DATASET(JONATHAN))
```

CA Top Secret example - archive

- Example (results/output)

```
/*ARCHIVE RACHAEL  STORED 03/08/10-15.25.37 BY MASTER1  ON XE15
/*Please edit any CREATE commands by adding a PASSWORD keyword to the command
TSS CREATE(RACHAEL) NAME('RACHAEL E. KOT') TYPE(USER) DEPT(DEPTLORD)
TSS ADD(RACHAEL) GROUP(OMVSGRP)
TSS ADMIN(RACHAEL) MISC4(CERTAUTH CERTUSER CERTGEN  CERTEXPO CERTCHEK)
TSS ADD(RACHAEL) FAC(BATCH)
TSS ADD(RACHAEL) FAC(CICSPROD)
TSS ADD(RACHAEL) FAC(TSO)
TSS ADD(RACHAEL) UID(0000000004)
TSS ADD(RACHAEL) HOME(/U)
TSS ADD(RACHAEL) DFLTGRP(OMVSGRP)
TSS PER(RACHAEL) DSN(SYS1.) ACCESS(READ)
TSS1594I ARCHIVE   FUNCTION SUCCESSFUL
TSS0300I  LIST     FUNCTION SUCCESSFUL
```

CA Top Secret example - model

- Example (implementation)

```
TSS MODEL USING(Rachael) ACID(Cassie)

TSS MODEL USING(Jonathan) ACID(Ronald) INTO(KOTPA01.MODEL.RONALD)

TSS MODEL(Jonathan) ACID(Jason) INTO(KOTPA01.MODEL.DATASET(JASON))
```

CA Top Secret - model

- Example (results/output)

```
/*MODEL   CASSIE   STORED 03/08/10-16.29.03 BY MASTER1  ON XE15 USING RACHAEL
/*Please edit any CREATE commands by adding a PASSWORD keyword to the command
TSS CREATE(CASSIE) NAME('RACHAEL E. KOT') TYPE(USER) DEPT(DEPTLORD)
TSS ADD(CASSIE) GROUP(OMVSGRP)
TSS ADMIN(CASSIE) MISC4(CERTAUTH CERTUSER CERTGEN  CERTEXPO CERTCHEK)
TSS ADD(CASSIE) FAC(BATCH)
TSS ADD(CASSIE) FAC(CICSPROD)
TSS ADD(CASSIE) FAC(TSO)
TSS ADD(CASSIE) HOME(/U)
TSS ADD(CASSIE) DFLTGRP(OMVSGRP)
TSS PER(CASSIE) DSN(SYS1.) ACCESS(READ)
TSS0300I  MODEL    FUNCTION SUCCESSFUL
```