IBM Education Assistance for z/OS V2R2

Item: RACF RACDCERT Granular Certificate Administration
Element/Component: RACF

Material current as of May 2015

Agenda

- Trademarks
- Presentation Objectives
- Overview
- Usage & Invocation
- Presentation Summary
- Appendix

Trademarks

- See url http://www.ibm.com/legal/copytrade.shtml for a list of trademarks.

Presentation Objectives

- Digital certificates usage has been growing
- Continuous enhancements to fulfill customer requirements
- Components on certificate support:
  - RACF: RACDCERT command and the R_datalib callable service
- At the end of this presentation, you should have an understanding of the support from RACDCERT granular administration

Overview

- Problem Statement / Need Addressed
  - Certificate and key ring administration in RACF is handled by the RACDCERT command
  - Currently, RACDCERT functions access is controlled by the FACILITY class, through the profiles IRR.DIGTCERT.<racdcert function>
  - The access needed is based on the ownership of the certificates or key rings
    - READ to act on your own
    - UPDATE to act on other's
    - CONTROL to act on CERTAUTH / SITE
  - This access model is either 'none' or 'all', no granular control, eg.
    - When you have CONTROL access to IRR.DIGTCERT.GENCERT, you can generate any CA certificates

Overview

- Solution
  - Provide RACDCERT granular control based on
    - owner
    - certificate label
    - key ring name
    - function

Overview

- Benefit / Value
  - Enable the customers to segregate RACDCERT authorities among the administrators
  - Enforce a naming convention for naming the certificates and keyrings

Usage & Invocation

- Granular control is turned on by the presence of the profile IRR.RACDCERT.GRANULAR in the RDATALIB class

- If the profile IRR.RACDCERT.GRANULAR does not exist, the original IRR.DIGTCERT.<racdcert function> profile(s) in the FACILITY class will be used.

- Applies to these 13 RACDCERT functions only

Cert

- ADD
- ALTER
- DELETE
- EXPORT
- GENCERT
- GENREQ
- IMPORT
- REKEY
- ROLLOVER

Ring

- ADDRING
- DELRING

Cert and Ring

- CONNECT
- REMOVE

Usage & Invocation

- When granular control is turned on, one or both types of the following profiles in the RDATALIB class will be checked for READ access, depending on whether a certificate, a ring or both is involved
  - from the customers feedback, it is preferred to have one level of access, READ
- For certificates
  - IRR.DIGTCERT.<cert owner>.<cert label>.UPD.<racdcert cert functions>
    - where 'cert owner' is the RACF user ID, or CERTIFAUTH (for certificate owned by CERTAUTH), or SITECERTIF (for certificate owned by SITE)
    - EXPORT may use IRR.DIGTCERT.<cert owner>.<cert label>.LST.EXPORT if no private key is exported
  - If the function involves multiple certificates, eg, exporting a chain of certificates, multiple profiles will be checked

Usage & Invocation

- For key rings
  - <ring owner>.<ring name>.UPD.<ADDRING or DELRING>
  -

- For certificates and key rings
  - IRR.DIGTCERT.<cert owner>.<cert label>.LST.<CONNECT or REMOVE>

  +

  - <ring owner>.<ring name>.UPD.<CONNECT or REMOVE>

Usage & Invocation

- Example 1 – one profile for one function
- Define a profile to control who can delete the certificate with label FTPSERVER1 owned by user ID ftpid
  - RDEFINE RDATALIB IRR.DIGTCERT.FTPID.FTPSERVER1.UPD.DELETE UACC(NONE)
- Allow USERA to delete the certificate
  - PERMIT IRR.DIGTCERT.FTPID.FTPSERVER1.UPD.DELETE CLASS(RDATALIB) ID(USERA) ACCESS(READ)

Usage & Invocation

- Example 2 – one profile for multiple functions
- Define a profile to control who can add, alter the status, delete, generate, create a request and import a certificate with label FTPSERVER1 owned by user ID ftpid
  - RDEFINE RDATALIB IRR.DIGTCERT.FTPID.FTPSERVER1.UPD.* UACC(NONE)
- Allow USERA to add, delete, generate, create a request and import the certificate
  - PERMIT IRR.DIGTCERT.FTPID.FTPSERVER1.UPD.* CLASS(RDATALIB) ID(USERA) ACCESS(READ)

Presentation Summary

- Now you should have an understanding of the support from RACF for RACDCERT granular administration.

Appendix

- Publication references
  - *Security Server RACF Command Language Reference* (SA22-7687)
  - *Security Server RACF Administrator's Guide* (SA22-7683)