z/OS V1R9
RACF Writeable Keyrings
PKI Services Updates

Session 07

Prepared by Patrick Kappeler
IBM Consulting IT Specialist
kappeler@fr.ibm.com

Redbooks
International Technical Support Organization

z Security Update

Trademarks

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

The following are trademarks or registered trademarks of other companies.

Java and all Java-related trademarks and logos are trademarks of Sun Microsystems, Inc., in the United States and other countries.
Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.
Microsoft, Windows and Windows NT are registered trademarks of Microsoft Corporation.
UNIX is a registered trademark of The Open Group in the United States and other countries.
SET and Secure Electronic Transaction are trademarks owned by SET Secure Electronic Transaction LLC.

* All other products may be trademarks or registered trademarks of their respective companies.

Notes:

Performance is in Internal Throughput Rate (ITR) ratio based on measurements and projections using standard IBM benchmarks in a controlled environment. The actual throughput that any user will experience will vary depending upon considerations such as the amount of multiprogramming in the user's job stream, the I/O configuration, the storage configuration, and the workload processed. Therefore, no assurance can be given that an individual user will achieve throughput improvements equivalent to the performance ratios stated here.

IBM hardware products are manufactured from new parts, or new and serviceable used parts. Regardless, our warranty terms apply.

All customer examples cited or described in this presentation are presented as illustrations of the manner in which some customers have used IBM products and the results they may have achieved. Actual environmental costs and performance characteristics will vary depending on individual customer configurations and conditions.

This publication was produced in the United States. IBM may not offer the products, services or features discussed in this document in other countries, and the information may be subject to change without notice. Consult your local IBM business contact for information on the product or services available in your area.

All statements regarding IBM's future direction and intent are subject to change or withdrawal without notice, and represent goals and objectives only.

Information about non-IBM products is obtained from the manufacturers of those products or their published announcements. IBM has not tested those products and cannot confirm the performance, compatibility, or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

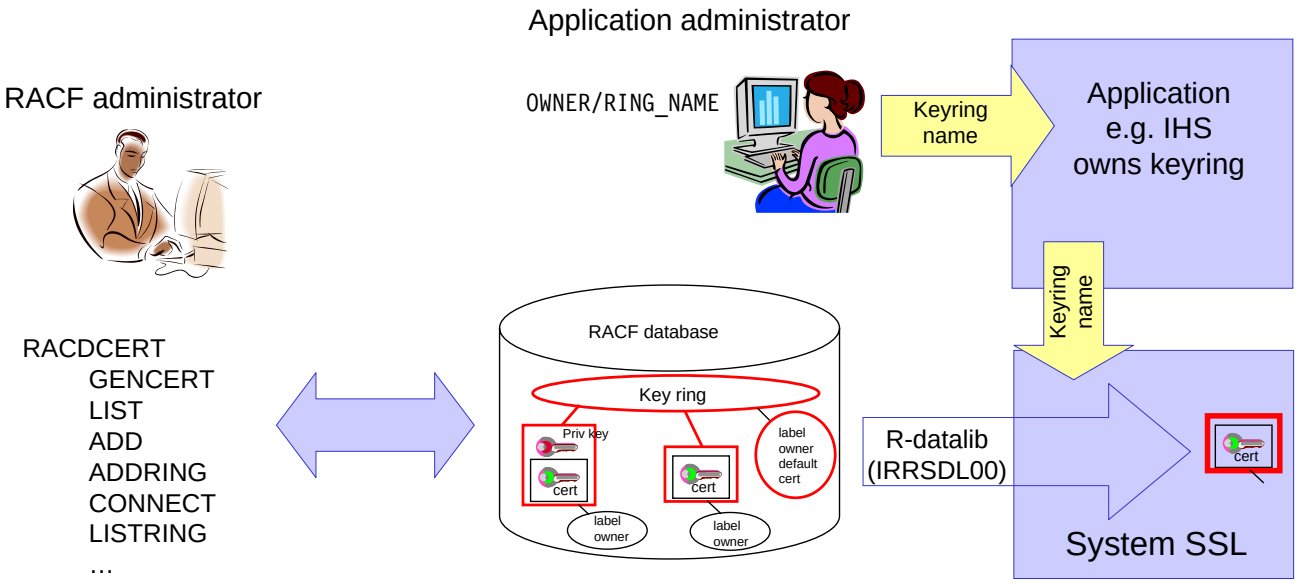
Prices subject to change without notice. Contact your IBM representative or Business Partner for the most current pricing in your geography.

Agenda

- RACF Writeable Keyrings
- PKI Services Updates
  - Automated Certificate Renewal
  - SDBM Support
  - Email Notification To Administrator
  - Query On Expiring Certificates

z/OS V1R9 RACF Writeable Keyrings

Preamble – RACF Keyrings In z/OS V1R8



keyrings are readable-only by applications (R_datalib RACF callable service)

Access to keyring and certificates is controlled through the IRR.DIGTCERT.LISTRING and IRR.DIGTCERT.LIST profiles in the FACILITY class
(READ: access your own keyring, UPDATE: access somebody else's keyring)

z/OS V1R9 - RACF Writeable Keyrings

- Provide new functions in R_datalib, so that RACF keyrings can be created and populated by applications
  - 5 new functions in R_datalib
    - NewRing
    - DelRing
    - DataPut
    - DataRemove
    - DataRefresh

    See appendix

- Provide more granular access control to keyrings
  - New RDATALIB class to provide granular ring access control
  - Access controlled per ring's owner, ring's name, access (list/update)

Will roll back to z/OS V1R7 and V1R8

RACF Writeable Keyrings – New Access Controls

- Profiles in the RDATALIB class
- Access control to the new update functions
  <ringOwner>.<ringName>.**UPD**
- Access control to the ring related read functions
  Real ring: <ringOwner>.<ringName>.**LST**
  Virtual ring: <virtual ring owner>.**IRR_VIRTUAL_KEYRING.LST**
- Old type global access control profiles read functions if the new profile is absent
  IRR.DIGTCERT.<function>

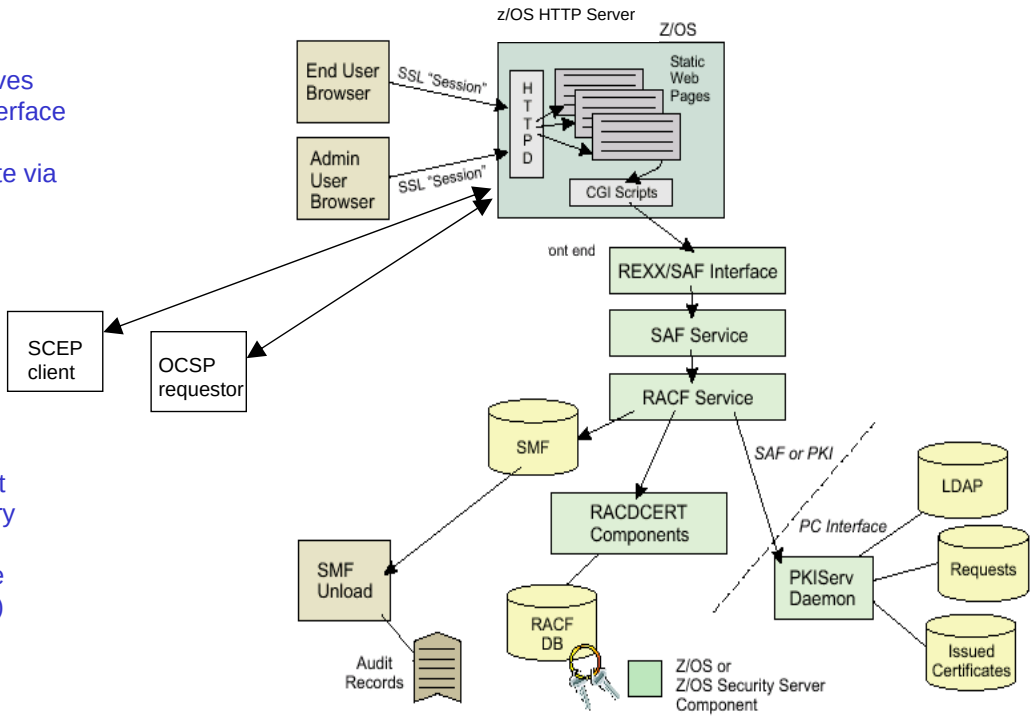
Application XYZ needs to be able to install certificate in all the key rings with a name that starts with ABC and owned by ABCJOB in the RACF database

- `RDEFINE RDATALIB ABCJOB.ABC*.UPD UACC(NONE)`
- `PERMIT ABCJOB.ABC*.UPD CLASS(RDATALIB) ID(XYZ) ACCESS(UPDATE)`
- Invoke R_Datalib's DataPut function

z/OS V1R9 PKI Services Update

Preamble – z/OS PKI Services In z/OS V1R8

- User requests and receives certificate via browser interface
- Client can get a certificate via SCEP (Simple Certificate Enrolment Protocol)



- Certificate Revocation List published in LDAP directory and HTTP files
- Support for OCSP (Online Certificate Status Protocol)

Identrus compliant

z/OS PKI Services At z/OS V1R9

Automated certificate renewal

Automatically send a renewed certificate to the owner before the old one expires

SDBM support

Allow the PKI Services LDAP userID to be specified as a RACF SDBM distinguished name in the PKI Services configuration file

Email notification to administrator

Notify PKI Services administrator through the email when there are any requests waiting for his approval

Query on expiring certificates

Allow query on certificates based on the number of days they will become expired

z/OS V1R9 PKI Services Automated Certificate Renewal

z/OS PKI Services - Automated Certificate Renewal

- Users request for renewal of a certificate when close to expiration
  - The renewed certificate gets all the information from the original one with a new expiration date and a new serial number
- Automated renewal is implemented in z/OS V1R9 PKI Services
  - Ease certificate renewal management for users and administrators
  - new keywords in
    - The PKI Services configuration file (pkiserv.conf)
      - specification of the time to send
      - specification of a file for the new certificate to be put on
    - The certificates template (pkiserv.templ)
      - an AUTORENEW directive
      - the presence of an autoRenew flag
      - the presence of the notification email address of the receiver
  - The capability of sending the certificate by email with the z/OS sendmail utility

Example

•Prepare the pkiserv.conf file so that an e-mail is sent for certificates automated renewal 30 days before the certificate expiration. The Email message is in /etc/pkiserv/renewcertmsg.form

```
ExpireWarningTime=30d
      RenewCertForm=/etc/pkiserv/renewcertmsg.form
```

•The specific certificate template is updated for automated renewal of this certificate type (here the 1-Year PKI SSL Browser Certificate)

```
<TEMPLATE NAME=1-Year PKI SSL Browser Certificate>
<TEMPLATE NAME=PKI Browser Certificate>
<NICKNAME=1YBSSL>
 <AUTORENEW=Y>
…
%%NotifyEmail%%
```


z/OS V1R9
PKI Services
SDBM Support

z/OS PKI Services - SDBM Credential Support

- The z/OS PKI Services daemon must provide an LDAP user identity (distinguished name) for certificates/certificate revocation lists (CRLs) posting into the LDAP directory

- Prior to z/OS V1R9, The LDAP user DN syntax is constrained by the PKI Services, with no support for the SDBM (RACF) attributes

- At z/OS V1R9, The DN syntax checking is left to the LDAP server
  The following DN is accepted and will work if a valid entry is in the SDBM backend

```
AuthName1=RACFID=ADMIN,PROFILETYPE=USER,O=RACFDB,C=US
   AuthPwd1=secret
```


z/OS V1R9 PKI Services email Notification To Administrator

z/OS PKI Services - email Notification To Administrator

- Prior to z/OS V1R9, the PKI Services administrator does not know of any requests waiting for his approval otherwise than by periodically doing a manual checking

- At z/OS V1R9

  Two new keywords in the PKI Services configuration file to specify the email address(es) of the administrator(s)

  - Immediate notification when a new request is pending
    `AdminNotifyNew=<email_address>`

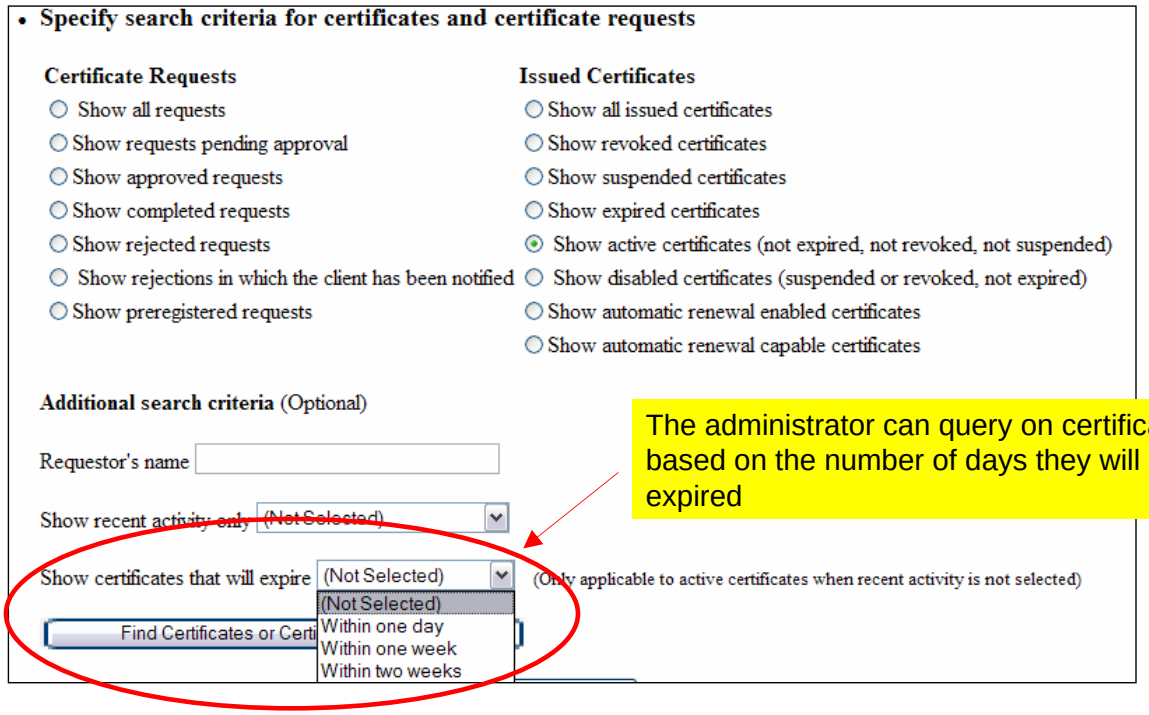
  - Daily notification for accumulated requests
    `AdminNotifyReminder=<email_address>`

  Another keyword specifies where the message is stored waiting to be sent using sendmail
  `AdminNotifyForm=/etc/pkiserv/pendingmsg.form`

z/OS V1R9 PKI Services Query On Expiring Certificates

z/OS PKI Services – Query On Expiring Certificates

z/OS V1R9 – PKI Services Administrator search options



The administrator can query on certificates based on the number of days they will become expired

Thank You

Any Questions ?

Appendix

- z/OS V1R9 Security Server (RACF) Manuals
  - *Callable Services (SA22-7691)*
  - *Command Language Reference (SA22-7687)*
  - *Security Administrator's Guide (SA22-7683)*

- z/OS V1R9 Cryptographic Services Manuals
  - *PKI Services Guide and Reference* (*SA22-7693*)

RACF Writeable Keyrings – R_datalib New Functions

NewRing

- Create a new key ring
- Remove all certificates from an existing ring

DelRing

Delete a key ring

DataPut

- Connect an existing certificate to a key ring
- Add a certificate, then connect
- Re-add a certificate and its associated private key, then connect

DataRemove

- Remove a certificate from the key ring
- Optionally delete it

DataRefresh

- Refresh the in-storage certificates