

RACF Update

GSE Large Systems Meeting

May 3rd 2007

Agenda

- **z/OS Version 1 Release 7**
 - Quick Review
- **z/OS Version 1 Release 8**
 - Look at what functionality IBM have provided
- **z/OS Version 1 Release 9**
 - Quick Preview

z/OS Security Server (RACF) Update



z/OS V1R7

RACF USER-related Enhancements:
Mixed-Case Passwords

- Allows RACF to distinguish between upper- and lower-case characters in passwords.
- Supported by TSO/E, CICS TS 3.1 (and 2.2 and 2.3 via PTF), Console logon, JOB statements, and z/OS UNIX functions.
- Controlled by SETR PASSWORD(MIXEDCASE | NOMIXEDCASE)
 - ▶ Do not enable mixed-case passwords unless all local systems sharing RACF DB are at z/OS R7
 - ▶ For RRSF, RACF will ensure passwords are in upper-case if sent to an RRSF node at z/OS R6 or earlier.

**RACF USER-related Enhancements:
Mixed-Case Passwords...**

- **Additional SETROPTS password rules:**
 - ▶ **NATIONAL**
 - # (X'7B'), \$ (X'5B'), and @ (X'7C')
 - ▶ **MIXEDCONSONANT**
 - Upper- or lower-case consonants (A-Z, a-z)
 - ▶ **MIXEDVOWEL**
 - Upper- or lower-case vowels (a, e, i, o, u, A, E, I, O, U)
 - ▶ **MIXEDNUM**
 - Upper- or lower-case alphabetic, or numeric, or national
 - At least one upper-case alpha or national, one lower-case alpha, and one numeric
- **Old rules (ALPHA, ALPHANUM, CONSONANT, VOWEL, NOVOWEL) will not match lower-case alphabetic characters.**

RACF USER-related Enhancements: Mixed-Case Passwords...

- Notes:

- ▶ RACF will remember whether a user has ever had a mixed-case password. If not, when comparing a password entered by the user RACF will check both the value as presented to RACF and the upper-case version of that value.
- ▶ When the user is changing his password, RACF will check that the new password and current password, when converted to upper-case, are different. Example:
 - If current password is ABCD
 - Then new password aBcD will be rejected

RACF USER-related Enhancements: Detect or Prevent Password Recycling

- Problem: Users can change passwords repeatedly and recycle their password history, keeping same password.
- Part 1 of Solution: With SETROPTS AUDIT(USER) in effect, RACROUTE REQUEST=VERIFY (logon, etc.) processing will create a type 80 SMF record indicating a password change.

RACF USER-related Enhancements: Detect or Prevent Password Recycling...

- Part 2 of Solution: SETROPTS PASSWORD(MINCHANGE(nnn))
- The MINCHANGE value specifies the minimum lifetime of a user's password, from 0 (not limited) up to the SETR PASSWORD(INTERVAL(mmm)) value.
 - ▶ Before nnn days, a user cannot change his/her own password again.
 - ▶ Helpdesk personnel authorized via IRR.PASSWORD.RESET need CONTROL authority to change a user's password before nnn days.
 - ▶ SPECIAL and group-SPECIAL users can change another user's password during that interval, but not their own password.

RACF USER-related Enhancements: Maintain revoke date when resuming users

- Problem: Administrator specifies
ALTUSER U1 REVOKE(mm/dd/yy)
then U1 forgets password, becomes revoked early, and administrator resumes U1.

RACF removes the REVOKE date.

- Solution: RACF will keep the revoke date.
- ALTUSER has new keywords NOREVOKE, NORESUME which will clear the REVOKE or RESUME dates, if present.
- LISTUSER and LISTGRP will show REVOKE and RESUME dates, even if in the past.

RACF USER-related Enhancements: Improve SETR INACTIVE processing for new users

- Problem: SETR INACTIVE(30) specified. Administrator creates new user U1, who does not logon for 45 days.

When U1 does logon, RACF does not consider him inactive, and allows the logon.

- Solution: RACF will put the user's creation date into the LJDATE field during ADDUSER processing. Then RACROUTE REQUEST=VERIFY (logon, etc.) processing will have a value to use for checking inactivity.
- LJTIME is not set during ADDUSER, so logon processing and LISTUSER and applications can still tell the user has never signed on.

RACF Availability Enhancement: Automatic RVARY SWITCH to backup for some errors

- **Problem: RVARY SWITCH is needed to recover from device errors on primary RACF DB, but**
 - It can take awhile to issue this command, especially if operator needs to supply the password.
 - RVARY cannot work while requests to use the DB are in process, so even after entering password, operator must VARY the device offline.
- **Improvement:**
 - If major device errors have occurred, affecting RACF and other users of the device, operator can VARY the RACF primary DB device offline (V nnn,OFFLINE,FORCE).
 - z/OS will terminate any outstanding requests with I/O error.
 - RACF will detect this I/O error, see device is offline, and automatically RVARY SWITCH to the backup
 - No password needed
 - SWITCH will happen on all systems in SYSPLEX Communication.

RACF Availability Enhancement: Automatic RVARY SWITCH
to backup for some errors...

▪ Notes:

- ▶ RVARY is still the preferred method for many cases.
 - VARY will affect all applications using data on that volume

- ▶ However, if the device is really broken, the other applications are probably in trouble, anyway.

RACF Support for the IBM Health Checker for z/OS

- What is the IBM Health Checker for z/OS?
 - Originally a tool developed by ITSO to address component configuration and setup errors commonly made by installations
 - Web download
 - Implemented as a batch job
 - 37 checks
 - With z/OS V1R7, the IBM Health Checker for z/OS is integrated into z/OS
 - Implemented as a started task
 - 55 checks
 - Rolled back to z/OS V1R4 as a web download
 - Checks are shipped with components
 - Installations and vendors can write checks
 - Extensive SDSF support

RACF Support for the IBM Health Checker for z/OS...

- RACF Support for the IBM Health Checker for z/OS:
 - ▶ New general resource classes: XFACILIT/GXFACILI
 - The eXtended FACILITY class
 - Resource name of up to 246 characters
 - Shared POSIT value with the FACILITY class
 - Shipped in APAR OA10774, back to z/OS V1R4
 - ▶ Two RACF checks:
 - RACF_GRS_RNL (rolled back to z/OS V1R6 with APAR OA11833)
 - Checks to see if any of the RACF ENQ names are on a GRS resource name exclusion list which changes the scope of the RACF ENQ
 - RACF_SENSITIVE_RESOURCES (rolled back to z/OS V1R4 with APAR OA11833)
 - Looks at the current APF data sets and the RACF database data sets and flags those that are improperly protected
 - Are not found on the indicated volume
 - Are improperly protected

RACF API Enhancement: R_admin extract function for USER, GROUP, and CONNECT info

- Problem: R_admin callable service allows programs to issue RACF commands, including LISTUSER and LISTGROUP, but:
 - ▶ 1. Output of commands is not a programming interface
 - ▶ 2. Output is difficult to parse to extract the needed data
 - ▶ 3. RACF restricts output to 4096 lines
- Solution: New R_admin functions to extract USER, GROUP, or CONNECT info

RACF API Enhancement: R_admin extract function for USER, GROUP, and CONNECT info...

- New USER-related functions:
 - ▶ Extract USER
 - ▶ Extract next USER
 - ▶ Extract CONNECT
- New GROUP-related functions:
 - ▶ Extract GROUP
 - ▶ Extract next GROUP
- Data returned in a structured format
 - ▶ Segment name
 - ▶ Field name
 - ▶ Data

RACF API Enhancement: R_admin extract function for USER, GROUP, and CONNECT info...

- Problem state callers require access to FACILITY resource:
 - ▶ IRR.RADMIN.LISTUSER for USER-related extract functions
 - ▶ IRR.RADMIN.LISTGRP for GROUP-related extract functions
- Normal LISTUSER and LISTGRP security rules also apply

RACF Security Enhancement for Servers: Nested ACEEs

- Scenario: A server authenticates a client, creates ACEE, and then does access checking.
- Problem: Sometimes a check should use the server identity, not the client identity.
 - Example: Server may use SSL or TLS for communication security, but after client authentication occurs, it may be the client (today) who needs authority to use ICSF crypto services or keys.
- This is solved for FTP today, in different ways depending on z/OS release, via PTFs
- Not solved for other servers, though, and a fix like the one in FTP is very complex
 - We need a simpler solution

RACF Security Enhancement for Servers: Nested ACEEs

- **Solution:**

- ▶ The server tells RACF to create a client ACEE, but to also embed a copy of the server ACEE in the client ACEE, as an ENVR object
- ▶ The administrator (only if instructed by server documentation) tells RACF to use the embedded ACEE.
 - Example: `RALTER CSFSERV CSFENC
APPLDATA('RACF-DELEGATED')`
- ▶ Server then uses `RACROUTE REQUEST=FASTAUTH` to do the authorization check
- ▶ `FASTAUTH` first checks client authority to the resource, and if that fails, checks server authority

XML Output for the RACF SMF Unload Utility

- XML: The eXtensible Markup Language
 - An industry standard way of tagging data
 - Simplifies data and document exchange

- The RACF SMF Unload Utility (IRRADU00) now optionally produces XML-tagged output!
 - XML output is created if the new DD names are allocated:
 - XMLOUT: Unformatted (long stream)
 - XMLFORM: Formatter (one tag/pair or field per record)
 - Type 30, 80, 81, and 83 events supported (including EIM)

PKI Services Enhancements

- Support for DSA (Digital Signature Algorithm) in key generation and signing
 - Today only RSA supported
- Enhancement to CRL Distribution Point information: Support URI to indicate location of Certificate Revocation List
 - Today only the DN (distinguished name) format supported
- Create ARL (certificate revocation list) for CA certificates generated by PKI services
 - Today PKI Services creates CRL only for user certificates
- Provide basic OCSP (Online Certificate Status Protocol) responder support
 - Today OCSP support, if desired, requires 3rd party provider

Common Criteria

- **Common Criteria certification for z/OS R7 completed**
 - Labeled Security Protection Profile (LSPP) at Evaluation Assurance Level 4 (EAL4)
 - Controlled Access Protection Profile (CAPP) at EAL4

z/OS Security Server (RACF) Update



z/OS V1R8

Overview

- Password phrase support
- New RACF health checks
- Enhancements with IRRUT200 and IRRUT400
- LDAP change log
- PKI enhancements
- SAF identity token
- z/OS DB2 version 9 support
- Remote authorisation and auditing
- IRRSDA00 enhancements

Support for Password Phrases from 14 to 100 characters in length

- This is in addition to current support for lower case passwords
- Password Phrases allow for an exponentially greater number of possible combinations of characters and numbers than do passwords
- Currently, no exploitation of Password Phrase; RACF supports future exploitation
 - ▶ IE CICS, TSO, JES, etc
- Aimed at new applications probably web based

Support for Password Phrases from 14 to 100 characters in length

- Rules are:
 - ▶ Must not contain the user ID
 - ▶ Must contain at least 2 alphabetic characters
 - ▶ Must contain at least 2 non-alphabetic characters
 - ▶ Must not contain more than 2 consecutive characters that are identical
- New RACF Exit ICHPWX11
- ADDUSER, ALTUSER, LISTUSER & PASSWORD commands updated to support
- SETROPTS Interval rules apply to Password & Passphrase
- Support for RRSF

New Health Checks

- z/OS 1.8 RACF introduces seven new checks
- Six of them check whether a specific general resource class is activated and one checks if the IBMUSER is revoked
- The checks are called:
 - ▶ RACF_OPERCMDS_ACTIVE
 - ▶ RACF_TAPEVOL_ACTIVE
 - ▶ RACF_TEMPDSN_ACTIVE
 - ▶ RACF_TSOAUTH_ACTIVE
 - ▶ RACF_UNIXPRIV_ACTIVE
 - ▶ RACF_IBMUSER_REVOKED

IRRUT200 & IRRUT400 Enhancements

- The significant improvements that have been made to the two utilities are:
 - Synchronised copy of RACF data base with IRRUT200
 - Safety features for IRRUT200 and IRRUT400
 - Dependencies and migration considerations

Synchronised copy of RACF data base with IRRUT200

- Prior to z/OS V1R8, the following steps could be used:
 1. Run the IRRUT200 utility to copy the active primary to a data set with the same name as the active backup
 2. RVAR Y INACT to inactivate the backup data set
 3. Uncatalog the old backup data set & Catalog the new copy
 4. Use the RVAR Y ACTIVE command to activate the new copy as the RACF backup database
- However, during this time any changes made during steps 2 -4 would be missing from the Backup dataset

Synchronised copy of RACF data base with IRRUT200

- The IRRUT200 utility has been modified and introduces an additional Parameter `PARM=ACTIVATE`
- The `ACTIVATE` parameter can ensure that no updates are made to the input data set between the time that it is copied and the time that the copy is activated
- However, it can only ensure a synchronised copy if the system on which the utility is running is in RACF sysplex communications mode, or the RACF data set is not shared with another system
- If other systems share the backup data set and are not in sysplex communications mode, IRRUT200 can only activate the data set on the system on which the utility is running
- To activate the backup data set on the sharing systems, you must issue an `RVARY ACTIVE` command

Synchronised copy of RACF data base with IRRUT200

- Steps to take with zOS 1.8 and above:
 - ▶ Verify Input database using IRRUT200
 - ▶ Inactivate the backup database
 - ▶ Delete the backup database
 - ▶ Run IRRUT200 to allocate & copy new database, using the PARM='ACTIVATE' parameter
 - ▶ Primary & Backup are synchronised and Active

Synchronised copy of RACF data base with IRRUT200

- What happens:
 - ▶ PARM=ACTIVATE does no verification; SYSPRINT and SYSIN DD statements are ignored.
 - ▶ SYSUT1 is the target of the output and must be the in-use inactive backup associated with the SYSRACF in-use active primary
 - ▶ IRRUT200 gets exclusive serialisation of the Primary RACF database
 - ▶ When the copy is complete, an internal RVAR Y ACTIVE command is done against the
 - ▶ SYSUT1 (target of output) backup and serialisation of the Primary database is released

IRRUT200 & IRRUT400 Safety Features

- The new safety features for both utilities are very similar
- New checks which take volume labels into account are added
- The utilities no longer allow use of:
 - ▶ the same data set for *target* and *source*
 - ▶ the use of an active in-use data set as a *target*
- There are no changes to the JCL because whenever you invoke IRRUT200 and IRRUT400 the safety features are integrated

LDAP Change Logs Enhancements

- The change log is a set of entries in the directory that contain information about changes to objects
- Depending on configuration options, information about a change to a TDBM entry or to an object controlled by an application (for example, a RACF user, group, or user-group connection profile) can be saved in a change log entry
- An LDAP search operation can be used to retrieve change log entries to obtain information about what changes have taken place

The change log is a set of entries in the directory that contain information about changes to objects. Depending on configuration options, information about a change to a TDBM entry or to an object controlled by an application (for example, a RACF user, group, or user-group connection profile) can be saved in a change log entry. An LDAP search operation can be used to retrieve change log entries to obtain information about what changes have taken place.

Currently, z/OS LDAP supports the query and update of USER, GROUP, and group connection attributes using the SDBM back end to talk to RACF. RACF currently supports LDAP change logging of updates to USER profiles. Thus, there is a functionality missing in RACF change logging with respect to the RACF functions supported by z/OS LDAP. z/OS V1R8 includes a support change for logging of group and connection updates.

LDAP Change Logs Enhancement

- Group change logging
 - ▶ Group change logging now allows an LDAP client to be notified of a RACF-initiated change for any of the profile types supported by the z/OS LDAP server
 - ▶ RACF can now be configured to create LDAP change log entries in response to changes in user and group profiles
 - ▶ In addition, all password changes are logged whether they are enveloped or not
 - ▶ This provides an open, remote method of change notification
 - ▶ An LDAP client can read the LDAP change log, detect updates to RACF users, groups, and group membership, and then retrieve RACF entries using only LDAP interfaces
 - ▶ To use this function, the LDAP server must be configured to enable the SDBM back end

Group change logging

Group change logging now allows an LDAP client to be notified of a RACF-initiated change for any of the profile types supported by the z/OS LDAP server. RACF can now be configured to create LDAP change log entries in response to changes in user and group profiles. In addition, all password changes are logged whether they are enveloped or not. This provides an open, remote method of change notification. An LDAP client can read the LDAP change log, detect updates to RACF users, groups, and group membership, and then retrieve RACF entries using only LDAP interfaces. To use this function, the LDAP server must be configured to enable the SDBM back end.

RACF Profiles required as follows to activate:

```
RDEF RACFEVNT NOTIFY.LDAP.USER UACC(NONE)
SETR RACLIST(RACFEVNT) REFRESH
```

Event notifications

Event notifications, through the creation of LDAP change log entries, are controlled by RACF resources in the RACFEVNT class. Two new resource profiles have been created in this class for group and connect to allow LDAP change log entries to be created for the corresponding event types on a system-wide basis. In addition, a new line in the LISTUSER command output has been added to demonstrate the existence of password envelopes, and there is now unconditional change logging of all password updates. This enhancement solves the problems from previous releases that there was no indication in the LISTUSER command as to existence of a password envelope and no change log entry was created for a new password which was not enveloped.

PKI Enhancements

- With z/OS V1R8, the restriction is removed that prevents multiple copies of the PKI Services started task, so now:
 - Each started task instance can operate as a different CA
 - This allows customers to operate multiple CAs.
- (SCEP) Simple Certificate Enrolment Protocol
 - Support for the Simple Certificate Enrollment Protocol is now part of PKI Services
 - This includes support when a device submits an encrypted and signed certificate request, and polls for a response
 - This support uses HTTP messages in the PKCS#7 data format
 - You can configure PKI Services to respond automatically to some (or all) SCEP certificate requests, or to submit some (or all) SCEP certificate requests to the PKI administrator for approval or rejection. When you enable automatic enrolment, certificate requests can be automatically approved and synchronously fulfilled, based on the requestor's knowledge of a predetermined secret, the challenge passphrase.

The Simple Certificate Enrollment Protocol (SCEP) allows you to securely issue certificates to large numbers of network devices using a primarily automatic enrollment technique. The network devices, usually IPSEC devices such as Cisco routers, must be SCEP-enabled and preregistered (to your CA domain) before they can successfully request certificates from you.

To request a certificate, the preregistered SCEP client sends a message (the certificate request) to your CA using the HTTP protocol. Prior to z/OS V1R8, PKI Services does not support a wire protocol for receiving and fulfilling certificate requests. A Web page interface is the only means of submitting certificate requests. Due to an increasing use of certificates in routers, VPNs, and other such devices, much manual work to set up proper security had to be done.

z/OS V1R8 support

Support for the Simple Certificate Enrollment Protocol is now part of PKI Services. This includes support when a device submits an encrypted and signed certificate request, and polls for a response. This support uses HTTP messages in the PKCS#7 data format. This should reduce manual administration.

You can configure PKI Services to respond automatically to some (or all) SCEP certificate requests, or to submit some (or all) SCEP certificate requests to the PKI administrator for approval or rejection. When you enable automatic enrollment, certificate requests can be automatically approved and synchronously fulfilled, based on the requestor's knowledge of a predetermined secret, the challenge passphrase.

Support for SAF Identity Tokens

- SAF identity token now provides increased user accountability and audit resources by providing end-to-end auditing that tracks the identity initially used for authentication as well as the identity on the current platform
- This support is especially valuable to customers maintaining heterogeneous environments, where requests and entry points to network resources come from a variety of platforms

Support for Virtual Key Rings

- This support is intended to treat the collection of all the certificates owned by one userID, including the SITE and CERTAUTH reserved IDs, as an independent key ring
- The use of the CERTAUTH virtual key ring is intended to eliminate the need to manually created multiple key rings for SSL enabled applications such as FTP.

A key ring is a collection of certificates that identify a networking trust relationship. In a client-server network environment, entities identify themselves using digital certificates. Server applications on z/OS that wish to establish network connections to other entities can use RACF key rings and other related services to determine the trustworthiness of the client or peer entity.

Key rings contain the public keys that are associated with signers of certificates. These public keys are, in reality, contained in certificates themselves. Therefore, verifying one certificate requires the use of a different certificate, the signer's certificate. In this fashion, a chain of certificates is established, with one certificate being verified by using another certificate and that certificate being verified by yet another certificate, and so on. A certificate, and its

associated public key, can be defined as a *root* certificate. A root certificate is self-signed, meaning that the public-key contained in the certificate is used to sign the certificate. Using a root certificate implies that the user trusts the root certificate.

Key rings are associated with specific RACF user IDs and a RACF user ID can have more than one key ring. Key rings are managed using the RACDCERT RACF command, and are maintained in the general resource class DIGTRING.

A virtual key ring is the set of certificates used by a user or server application to determine the trustworthiness of a client or peer. Real key rings must be created and populated as required by the application. However, a virtual key ring does not need to be added to RACF. Each RACF user ID is associated with a virtual key ring. The most common type is the CERTAUTH virtual key ring, which contains all the

Intrusion Detection Services (IDS)

- Support for defining Intrusion Detection Services (IDS) policies in a policy agent configuration file as well as an LDAP server
- This solution provides an IDS policy solution that is consistent with other policy types for those installations that do not have an LDAP infrastructure in place or that prefer using configuration files instead of LDAP

DB2 Version 9 Support

- The IRR@XACS exit is no longer shipped with RACF in SYS1.SAMPLIB
- It has changed substantially and is now shipped with DB2 as FMID HDRE810
- As a result of this the previous exit is no longer usable with DB2 V9
- If you have the RACF/DB2 external security module installed it will be necessary to migrate to the new RACF access control module for DB2 V9

Remote authorisation and auditing

- RACF now provides the capability of processing remote authorisation and auditing requests as the z/OS security server
- These features will employ a standard LDAP protocol to enable requests from various system platforms, ensure an auditable level of trust between the z/OS security server and requesting applications, use familiar SMF logging capability for recording audit data, and support the unloading of that data
- IBM's customers increasingly look for value in a centralized directory such as z/OS LDAP to locate and manage people, objects, and services for the enterprise
- Middleware application hosting environments, WebSphere® and Tivoli®, have embraced LDAP for that purpose
- Leveraging these new z/OS LDAP extended operations, middleware and applications can achieve distributed authorisation and auditing function that can be managed by the z/OS security administrator

IRRSDA00 enhancements

- RACF provides an enhancement to IRRSDA00 to support using RACROUTE REQUEST=FASTAUTH when the RACF profile is RACLISTed
- Currently the CIM Server is using `__check_resource_auth_np` to make sure that the CIM client can access the CIM Server
- The existing `__check_resource_auth_np` logic translates to UNIX System Services invoking IRRSDA00 using RACROUTE REQUEST=AUTH function
- Since the CIM Server RACF profile is RACLISTed, changing IRRSDA00 to recognise the RACLISTed profile to do a FASTAUTH check will have performance benefits for all `__check_resource_auth_np()` invokers checking on RACLISTed profiles
- The IRRSDA00 has added logic to create an ACEE for the input user ID for the FASTAUTH check on the RACLISTed profiles
- This change gives better performance on `__check_resource_auth_np` when the RACF profile is RACLISTed

z/OS Security Server (RACF) Update




z/OS V1R9

	<h2 style="margin: 0;">z/OS V1R9 Preview</h2> <ul style="list-style-type: none"> ▪ PKCS #11 support <ul style="list-style-type: none"> ▸ ICSF ▸ RACF ▪ PKCS (Public Key Cryptography Standards) is offered by RSA Laboratories of RSA Security Inc. (TM) PKCS #11, also known as Cryptoki, is the cryptographic token interface standard. It specifies an application programming interface (API) to devices, referred to as tokens. The PKCS #11 API is an industry-accepted standard commonly used by cryptographic applications. PKCS #11 applications developed for other platforms can be recompiled and run on z/OS.

•z/OS V1.9 is planned to provide support for the PKCS#11 standard. PKCS (Public Key Cryptography Standards) is offered by RSA Laboratories of RSA Security Inc. (TM) PKCS #11, also known as Cryptoki, is the cryptographic token interface standard. It specifies an application programming interface (API) to devices, referred to as tokens. The PKCS #11 API is an industry-accepted standard commonly used by cryptographic applications. PKCS #11 applications developed for other platforms can be recompiled and run on z/OS.

•Integrated Cryptographic Services Facility (ICSF) plans to support PKCS #11, providing an alternative to IBM's Common Cryptographic Architecture (CCA) and broadening the scope of cryptographic applications that can make use of zSeries cryptography.

•RACF is planned to provide PKCS#11 support. The RACF RACDCERT command will provide token management of certificate, public key, and private key objects

<p>z/OS V1R9 Preview</p> <ul style="list-style-type: none">▪ RACF<ul style="list-style-type: none">▸ Java Interface to administer / query RACF user / group profiles▸ Password Phrase extension<ul style="list-style-type: none">– 9-13 characters will be supported when activated by a RACF exit– Sample exit provided▪ Network Authentication Service (Kerberos)<ul style="list-style-type: none">– AES added to crypto suite <p style="text-align: right;">continued </p>
--

•In z/OS V1.9, RACF plans to provide a Java interface to administer or query users and groups in RACF. This is intended to increase the accessibility and usability of RACF by allowing programmatic access to RACF from Java programs.

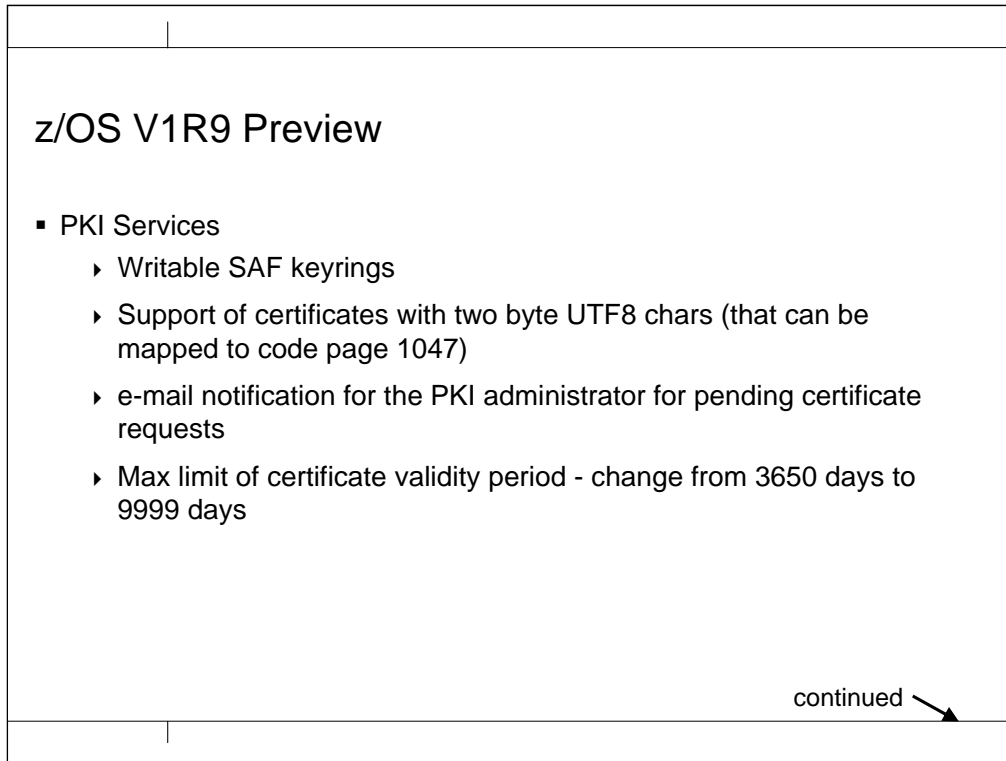
•The z/OS Network Authentication Service is planned to be enhanced to support the AES cryptographic algorithm. This support will enhance interoperability with other Kerberos implementations by extending the z/OS's cipher suite. Because RACF can act as the registry for the z/OS Network Authentication Service, RACF provides the management interfaces for cryptographic keys. RACF commands are planned to be extended to allow the specification of AES as a supported cipher.

•In z/OS V1.9 an extension is planned to be added to the Password Phrase support first available in z/OS V1.8. The minimum length of a password phrase has been lowered from 14 characters to 9. Password phrases from 9 to 13 characters in length can be used in conjunction with a new password phrase exit (ICHPWX11) you can write to determine whether to accept them. A sample exit is provided, which uses the new System REXX facility to call a REXX exec in which you can code password phrase quality rules. A sample REXX exec is provided. Also, password change logging and enveloping functions are extended to include RACF password phrases

•In z/OS V1.9, RACF plans to provide a Java interface to administer or query users and groups in RACF. This is intended to increase the accessibility and usability of RACF by allowing programmatic access to RACF from Java programs

z/OS V1R9 Preview

- System SSL
 - ▶ Tuning capabilities for CRL checking
 - ▶ Callback re-handshake notification
 - ▶ Hostname validation granularity
 - ▶ Notification on switch from HW crypto to software



Within z/OS V1.9 the following enhancements to PKI Services and RACF digital certificate are planned:

- Writeable SAF Key rings are intended to enable z/OS applications to programmatically populate certificates in SAF/RACF key rings.
- Support of certificates with two byte UTF8 characters that can be mapped to code page 1047 is planned. Such certificates can be installed in RACF, managed and exploited through the RACDCERT functions. They can also be used for authentication to RACF. For example, the Spanish letter 'n' with tilde will be able to be included in a distinguished name.
- Allow the use of SDBM credential for the LDAP administrator in PKI Services - the LDAP server has multiple backends. It allows ACLs for entries using X.500 type userid or RACF-style userid. Currently PKI Services only accepts the X.500 type userid. The PKI daemon code will be enhanced to accept the RACF userid credential.
- Provide an e-mail notification for the PKI administrator for pending certificate requests. Currently, administrators must submit a query to determine whether there are pending approval requests.
- Change the maximum limit of the certificate validity period - the limit will be changed from 3650 days to 9999 days.
- Allow a query on expiring certificates based on the number of days until they will become expired.
- Automated certificate renewal will be designed to send renewal certificates via e-mail when the expiration dates for older certificates are approaching.
- A new REFRESH reminder message is planned to be issued after changes made to a certificate or a certificate filter profile through the RACDCERT command, to indicate that a refresh to the DIGTCERT or DIGTMAP class is needed after the affected RACDCERT commands when the DIGTCERT or DIGTNMAP class is RACLISTed.

z/OS V1R9 Preview

- PKI Services

- ▶ Query on expiring certificates based on the number of days until expiration
- ▶ Automated certificate renewal to send renewal certificates via e-mail when the expiration dates for older certificates are approaching
- ▶ A new REFRESH reminder message is planned to be issued after changes made to a certificate or a certificate filter profile through the RACDCERT command, to indicate that a refresh to the DIGTCERT or DIGTMAP class is needed after the affected RACDCERT commands when the DIGTCERT or DIGTMAP class is RACLISTed
- ▶ The generation of unused serial numbers will be avoided in the event of an ICSF failure when the PKI CA has a hardware key

<h2>z/OS V1R9 Preview</h2> <ul style="list-style-type: none"> ▪ z/OS Communications Server <ul style="list-style-type: none"> ▸ Network Security Services function providing: <ul style="list-style-type: none"> – centralized IPsec certificate services ▸ IKE Daemon to be configurable as a Network Security client ▪ FTP server, FTP Client, and TN3270 <ul style="list-style-type: none"> ▸ Application Transparent TLS (AT-TLS) to manage security

z/OS Communications Server is planning a new Network Security Services function to provide centralized certificate services, monitoring and management for IPsec security across z/OS systems within and across sysplexes. Network Security Services will allow IPsec certificates to be kept in a single location, rather than having them reside on each z/OS node. The z/OS Communications Server IKE daemon is planned to be enhanced so that it can be configured to act as a Network Security client. Configuration is on a per-stack basis, such that each NSS-enabled stack will appear to the Network Security Server as an independent client. For TCP/IP stacks that are not configured to use Network Security Services, the IKE daemon will continue to manage certificates out of a local key ring.

The FTP server, FTP client, and TN3270 server are planned to use Application Transparent TLS (AT-TLS) to manage TLS security. AT-TLS supports several security functions that the FTP server, FTP client, and TN3270 servers do not. For example, AT-TLS is designed to allow you to:

- Specify the label of the certificate to be used for authentication instead of using the Default certificate
- Use an LDAP server to validate certificates
- Support SSL Session Key Refresh
- Support SSL Sysplex Session ID Caching
- Support new or multiple key rings
- Under security administrator control, optionally trace decrypted SSL data in a data trace
- Receive more detailed diagnostic messages in syslogd

Thanks..

Thanks for listening.

Any Questions?

Mark Wilson

markw@rsmpartners.com

Mark.wilson@uk.logicalis.com

www.gse.org.uk/tyc