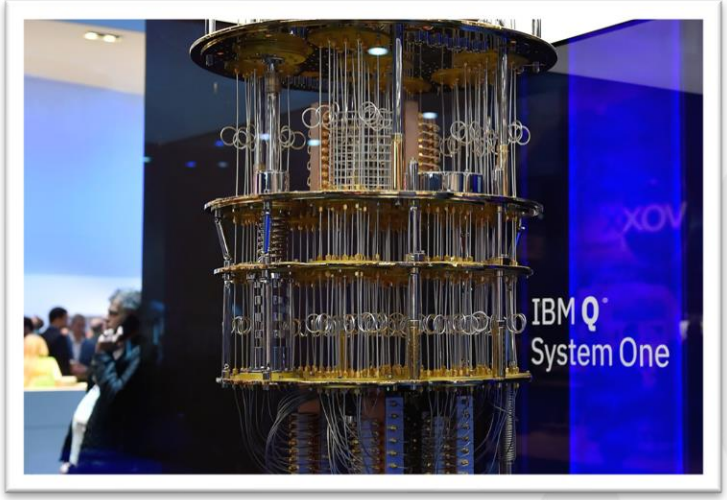
IBM® z/OS® Security Server RACF® Update Spring 2023 Edition

Ross Cooper, CISSP®
RACF Design and Development, IBM Poughkeepsie
May, 2023



IBM Poughkeepsie Lab

RACF Update Agenda

SHARE
EDUCATE • NETWORK • INFLUENCE

z/OS RACF V3R1

- Custom field information in ACEE

Post V2R5 – Continuous Delivery:

- Passphrase Interval
- Support for the IBM Z Security and Compliance Center
- Center for Internet Security (CIS) IBM z/OS V2R5 with RACF Benchmark
- Encrypted RACF VSAM data set as RACF database
- Ability to Disable Additional logon attempts for a RACF-SPECIAL user after exceeding the SETROPTS PASSWORD(REVOKE(nnn)) value
- Sharing RACF data base with RACF on z/VM

z/OS RACF V2R5:

- Enhanced PassTickets
- Health Checks
- RACF/SAF C Header Files
- Restrict ALTER access from managing discrete profiles
- Certificate Fingerprint Support
- RACF VSAM Database

(V3.1 STATEMENT OF DIRECTION)

CUSTOM FIELD INFORMATION IN ACEE

Custom Fields Overview

- Custom fields are fields within the RACF database that an installation can customize to store security information in RACF profiles:
  - Users, Groups
  - Data Sets and General Resources (starting in V2.4)

- The names and attributes of custom fields can be tailored.
- Once a custom field is defined, use RACF commands, such as the **ALTUSER, ALTGROUP, ALTDSD** and **RALTER** to add data to a custom field in a profile.
- Custom Fields are defined in the **CSDATA** segment of the **CFIELD** class.

Custom Fields Example

Define a new USER class field for the employee Serial Number called EMPSER:

```
RDEFINE CFIELD USER.CSDATA.EMPSER UACC(NONE)
     CFDEF(TYPE(NUM) FIRST(NUMERIC) OTHER(NUMERIC) MAXLENGTH(8)
          MINVALUE(100000) MAXVALUE(99999999)
          HELP('EMPLOYEE SERIAL NUMBER, 6 - 8 DIGITS') LISTHEAD('EMPLOYEE SERIAL='))
```

Activate the CFIELD class:

```
SETR CLASSACT(CFIELD)
```

Update RACF command dynamic parse:

```
IRRDPI00 UPDATE
```

Use the custom field to assign a user a Serial Number:

```
ALTUSER COOP CSDATA(EMPSER(123456))
```

List the custom field:

```
LISTUSER COOP CSDATA NORACF
USER=COOP
CSDATA INFORMATION
-----------------------------------------
EMPLOYEE SERIAL= 123456
```

Custom Fields in ACEE (V3.1)

- **ACEEs and Authentication:**
  - During user authentication, RACF reads certain fields from the user profile in the RACF database and builds a security environment (ACEE)
  - The ACEE is used by RACF to satisfy authorization and auditing requests

- **Custom Fields in the ACEE:**
  - Starting with z/OS V3R1, you can direct RACF to place custom field information from a user profile into the ACEE for retrieval by the R_GetInfo (IRRSGI00) callable service.

- **New ACEE(YES|NO) on CFIELD definition:**
  - `RDEFINE CFIELD USER.CSDATA.EMPSER UACC(NONE) CFDEF(TYPE(NUM) FIRST(NUMERIC) OTHER(NUMERIC)MAXLENGTH(8) MINVALUE(100000) MAXVALUE(99999999)` **`ACEE(YES)`**
    `HELP('SERIAL NUMBER, 6 - 8 DIGITS')LISTHEAD('EMPLOYEE SERIAL=‘))`
- **Refresh dynamic parse:** `IRRDPI00 UPDATE`
- **Add custom field to user:** `ADDUSER JOE CSDATA(EMPSER(123456))`
- **Now JOE’s EMPSER can be retrieved using the R_GetInfo service.**

Custom Fields in ACEE – R_GetInfo

- **R_GetInfo -** New Function Code 3 **-** Get CSDATA from ACEE

- **Authorization:**
  - FLAC – Field Level Access Checking – Granted via profiles in FIELD class
    - Determines which fields (including custom fields) the caller can view or modify
  - Authorized callers can optionally skip FLAC
  - Authorized callers can provide an ACEE_ptr to extract CSDATA from.

- **Invocation:**

CALL IRRSGI00 (

…
Num_parms, - New Value: 16 for function code X'0003'
…
Function_code, - New value: X'0003'- Get CSDATA from ACEE
Option, - Single / All fields? NOFLAC*? (sup. only)
…
Result_entries, - For FC 3 - CSDATA fields return area
CSDATA_keyword_name, - **New:** Field to retrieve or null for all
ACEE_ptr) - **New:** ACEE address

PASSWORD PHRASE INTERVAL

Password Interval Current Processing

SHARE
EDUCATE • NETWORK • INFLUENCE

RACF Password Change Interval:

- Defines the interval that users must change their password *or password phrase*
- Range: 1-254 days
- A system default can be specified
  - `SETROPTS PASSWORD(INTERVAL(<days>))`
- A user default can be specified
  - `PASSWORD USER(<user>) INTERVAL(<days>)`
  - `PASSWORD USER(<user>) NOINTERVAL`
- RACF uses the shorter of the system level and user specific interval as a user's effective password interval

Q: Is the 254-day limit appropriate for password phrases?

- Clients are requesting a longer RACF password phrase interval to match other platforms.
- NIST Special Publication 800-63B:
  - "Do not require that memorized secrets be changed arbitrarily (e.g., periodically) unless there is a user request or evidence of authenticator compromise. "

New Password Phrase Change Interval

New: PassPhrase Change Interval

- **With RACF APAR OA61951 (PTF UJ90043) and SAF APAR OA61952 (PTF UJ90042) (V2R5):**
  - RACF provides a new separate password phrase specific change interval which can be different than the existing password interval and supports much longer values.

- The password phrase interval can be set at:
  - The system level with the SETROPTS command
  - The user level with the PASSWORD/PHRASE command.

System PassPhrase Interval

Set System Password Phrase Interval:

```
SETROPTS PASSWORD(PHRASEINT(365))
```

- **Range:** 0-65,534 days (179 years)
- **Default value:** 0 - (Password phrase interval is not in effect)
- **Authorization:** Must have the RACF SPECIAL attribute
- **Details:**
  - A PHRASEINT value of zero indicates that the system does not have a phrase interval set and, in this case, the existing password interval controls the change interval for both passwords and password phrases.
  - When PHRASEINT is set to a non-zero value, it overrides the existing system level password interval control for password phrases.

System PassPhrase Interval…

Set System Password Interval to 90 days and Password Phrase Interval to 365 days:

```
SETROPTS PASSWORD(INTERVAL(90) PHRASEINT(365))
SETR LIST…
PASSWORD CHANGE INTERVAL IS 90 DAYS.
PASSWORD PHRASE CHANGE INTERVAL IS   365 DAYS.
```

Set System Password Interval to 30 days and Password Phrase Interval to zero (not in effect):

```
SETROPTS PASSWORD(INTERVAL(30) PHRASEINT(0))
SETR LIST…
PASSWORD CHANGE INTERVAL IS 30 DAYS.
PASSWORD CHANGE INTERVAL IS IN EFFECT FOR PASSWORD PHRASES.
```

User PassPhrase Interval

Set User Specific Password Phrase Interval:

```
PASSWORD USER(RACFU01) PHRASEINT(356)
```

- **Range:** 0-65,534 days (179 years)
- **Default:** 0 (User does not have a password phrase interval set)
- **Authorization:** SPECIAL or GROUP SPECIAL (Users can not set their own PHRASEINT)
- **Details:**
  - A PHRASEINT value of 0 indicates that the user does not have a phrase interval set. In this case, when the system level password phrase interval has a non-zero value it is used as the effective password phrase change interval and otherwise the existing password interval is used instead.
  - When the user's PHRASEINT is set to a non-zero value, it is used as the effective password phrase change interval and it overrides the system level password phrase interval control and system level password interval control.

User PassPhrase Interval…

Set User Level Password Phrase Interval to 365:

```
PASSWORD USER(RACFU01) INTERVAL(30) PHRASEINT(365)
LISTUSER RACFU01…
PASS-INTERVAL=30
PHRASE-INTERVAL=00365
```

Set User Level Password Phrase Interval to Never Expire:

```
PASSWORD USER(RACFU01) NOINTERVAL NOPHRASEINT
LISTUSER RACFU01…
PASS-INTERVAL=N/A
PHRASE-INTERVAL=N/A
```

Set User Level Password Phrase Interval to Zero (not in Effect):

```
PASSWORD USER(RACFU01) INTERVAL(30) PHRASEINT(0)
LISTUSER RACFU01…
PASS-INTERVAL=30
```

* (Password phrase interval line not listed when zero)

PassPhrase Interval – SMF

SMF Record Type 80:

- Data Type 6 command related data is updated to support the new PHRASEINT keyword of the SETROPTS and PASSWORD/PHRASE commands.
  - **SETROPTS command** - Update relocate to hold the new phrase interval
  - **PASSWORD/PHRASE commands** - Update relocate to hold the phrase interval
    - ‘FFFF’x in new field means NOPHRASEINT

SMF Record Type 81:

- The RACF SMF record type 81 RACF initialization record is updated to add a new field for the password phrase interval.
  - **RACF Initialization** – New field to hold new phrase interval setting

PassPhrase Interval – RRSF

Command direction Considerations:

- PASSWORD PHRASEINT(nnn) and NOPHRASEINT will not work on a remote node without this support.
- SETR PASSWORD(PHRASEINT(nnn)) will not work on a system that does not have this support

Handshaking Considerations:

- Update node def block to include 2-byte phrase interval for handshake (reuse reserved space)
- Lower-level system will ignore the new phrase interval field and not issue a message
- Up level systems will compare the phrase interval field. When not equal, issue message

```
IRRI007I ATTENTION: LOCAL NODE localnode HAS A DIFFERENT
SETROPTS PASSWORD(option) THAN PARTNER NODE partnernode.
```

PassPhrase Interval – Other

R_Admin Callable Service:

- Updated to support the new PHRASEINT keyword of the PASSWORD/PHRASE commands.
- Updated to support the new PHRASEINT keyword of the SETROPTS command.

DBUNLOAD – RACF Database Unload Utility:

- Unloads the new base segment user field for phrase interval
- DB2 samples are updated: RACDBUTB & RACDBULD

RACF_PASSWORD_CONTROLS Health Check does not examine the phrase interval

- RFE?

Effective Interval Examples

System and User Password and Phrase Change Interval Settings				Effective Password and Phrase Interval	
SETROPTS Password Interval	**User Password Interval**	**SETROPTS Phrase Interval**	**User Phrase Interval**	**Effective Password Interval**	**Effective Phrase Interval**
90	30	0	0	30	30
30	90	0	0	30	30
90	90	365	0	90	365
90	90	0	365	90	365
90	90	365	200	90	200
90	90	365	500	90	500

SUPPORT FOR THE IBM Z SECURITY AND COMPLIANCE CENTER

RACF SMF 1154 Subtype 83

- **Applications can request that participating z/OS applications cut security related SMF records:**
  - Request comes from a zOSMF REST API (such the IBM Z Security and Compliance Center)
  - RACF will create an SMF 1154 Subtype 83 record which contains compliance information.

- RACF SMF Records are documented in RACF Macros and Interfaces

RACF SMF 1154 Subtype 83 Contents

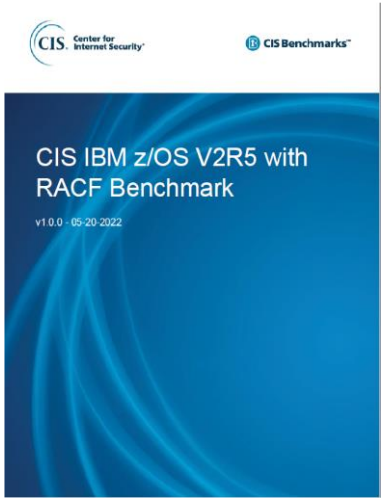
SMF Record Section	Contents
RACFSMRY: RACF Summary information (SETROPTS, etc.)	RACF ACTIVE/INACTIVE, definition of IBMUSER, SAUDIT,CMDVIOL, OPERAUDIT, MIXEDCASE, password rules, password exit status, password interval, password history, maximum failed password attempts, user inactivity, default RVARY passwords, password encryption algorithm, CATDSNS, ERASE, ACEECHK, BATCHALLRACF…
RACFCRIT: Critical RACF general resources	UACC, ID(*), WARNING AUDIT, GAUDIT information for critical RACF general resources (e.g. BPX.SUPERUSER)
RACFAPFL: Critical data set	UACC, ID(*), WARNING information for APF, RACF, LINKLIST, RRSF and PARMLIB data sets.
RACFACTL: Programs defined in the RACF Authorized Callers Table (Non-recommended options)	Module name and module location (LPA, not in LPA).

CENTER FOR INTERNET SECURITY (CIS) IBM Z/OS V2R5 WITH RACF BENCHMARK

CIS Benchmark for z/OS

- **The Center for Internet Security, Inc. (CIS®):**
  - Community-driven not-for-profit organization responsible for the CIS Controls® and CIS Benchmarks™, best practices for securing IT systems and data.

- **The z/OS V2R5 with RACF Benchmark:**
  - Contains 219 recommendations across 9 domains
  - TBD: list the 9 domains



- https://www.cisecurity.org/benchmark/ibm_z
  - Provide contact information, link e-mailed

RACF
VSAM DATABASE

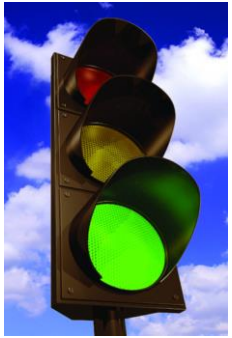
RACF VSAM Data Set Support

V2.5 VSAM RACF DB Support:

- RACF V2.5 has support for using a VSAM dataset as the RACF database

Base z/OS V2.5 restrictions

- Non-shared (may be on a device marked as shared)
- Non-split RACF data set
- Non-SMS managed (which means not encrypted)
- Not in RACF sysplex communications mode or RACF data sharing mode
- All systems sharing the RACF DB must be at z/OS V2.5
- Not defined in MSTRJCL
- Running in application identity mapping (AIM stage 3)
- That is free from internal errors (IRRUT200 and IRRDBU00 run without error)



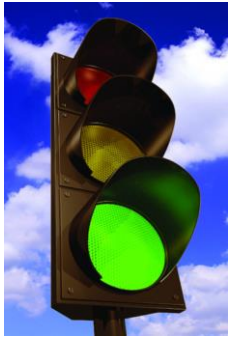
Encrypted VSAM Data Set Support in RACF

Encrypted RACF DB:

- V2.5 APAR OA62267 allows an encrypted DB and removes several restrictions

Base z/OS V2.5 restrictions, removed with APAR OA62267

- ~~Non-shared (may be on a device marked as shared)~~
- ~~Non-split RACF data set~~
- ~~Non-SMS managed (which means not encrypted)~~
- ~~Not in RACF sysplex communications mode or RACF data sharing mode~~
- All systems sharing the RACF DB must be at z/OS V2.5
- Not defined in MSTRJCL
- Running in application identity mapping (AIM stage 3)
- That is free from internal errors (IRRUT200 and IRRDBU00 run without error)



RACF APAR OA62267:

- PTF UJ08531, available 8 June 2022

Changes with a RACF VSAM Data Set

- **No change to the RACF programming interfaces:**
  - RACROUTE, ICHEINTY, RACF Callable Services, IRRXUTIL, RACF commands
- **No changes to the RACF serialization structure:**
  - Major names of SYSZRACF, SYSZRACn
  - But there is a new SYSVSAM ENQ.
- **Applications which read the RACF data base directly *may* have actions to take to support VSAM**
  - Disclosed at the vendor disclosure meeting in April 2020 and September 2020 and through ICN 1775 (18 August, 2020)

DISABLING ADDITIONAL LOGON ATTEMPTS FOR RACF SPECIAL USERS

SPECIAL User Excessive Password Prompt

- **SETROPTS PASSWORD(REVOKE(nnn))**
  - Establishes the maximum number of incorrect authentication attempts before a user is revoked.

- **When an incorrect logon attempt exceeds the REVOKE limit:**
  - Non-SPECIAL users are revoked immediately
  - Users with the SPECIAL attribute a message to the console asks the operator if the user should be revoked or allow an additional attempt

- **ICH301I MAXIMUM PASSWORD ATTEMPTS BY SPECIAL USER *userid* [AT TERMINAL *terminalid*.]**
  - **ICH302D REPLY Y TO ALLOW ANOTHER ATTEMPT OR N TO REVOKE USERID *userid*.**
    - Y – Allows the attempt to logon and does not revoke the user
    - N – Revokes the user

SPECIAL User Excessive Password Prompt Disablement

- **With OA63091 (V2.3, V2.4, V2.5) you can disable additional logon attempts for a RACF SPECIAL user once the SETROPTS PASSWORD(REVOKE(nnn)) value has been exceeded**
  - The disablement can be enabled on an application-by-application basis

- **Enabled with the definition of an XFACILIT class discrete profile of the name:**
  - **`IRR.DENY.SPECIAL.USER.ADDITIONAL.PASSWORD.ATTEMPTS.APPL.appl-name`**
  - The appl-name must match the APPL= value on the RACROUTE REQUEST=VERIFY.
  - If no appl-name was specified on the REQUEST=VERIFY, then it defaults to the same derivation method as used in PassTicket application name derivation.
  - This is a profile existence check only. No profile attributes (UACC, access list, etc.) are considered.

SHARING A RACF DB WITH Z/VM

Sharing a z/OS RACF DB with z/VM

- **Starting with z/VM 7.3, RACF z/OS and z/VM will not be able to share the RACF database.**
  - Attempts to IPL z/OS with a z/VM 7.3 RACF database will fail and the operator will be prompted for a different RACF database.
  - This change comes with APAR OA62875.
  - For details, see: https://www.vm.ibm.com/zvm730/announce.html

PASSTICKETS

PassTickets Overview

Password Alternative:

- A PassTicket is **an authentication token which can be used in place of a RACF password**. It is used for authentication of a RACF user ID. It is a character value that looks like a password and is accepted by RACF as if it is a valid password.
- The security of a PassTicket is **based on proof of possession of a secret DES key.**
- **Originally called** “Secured Signon” – Name mostly updated to PassTickets in 2.4 publications

Usage:

- PassTickets are useful in situations where a trusted application must pass a client's RACF user ID and “password” to another application, but the trusted application doesn't have the client's RACF password.
- Can be generated on-platform or off-platform. Algorithm is documented.
- **Example Applications:**
  - Session Managers, ELF (Express Logon Feature), Db2, CICS, WebSphere, Many others

More Details:

- RACF Security Administrator's Guide – Chapter - ‘Using PassTickets’
- RACF Macros and Interfaces – Chapter - ‘The RACF PassTicket’

PassTickets Configuration

Configured via profiles in the PTKTDATA Class:

PTKTDATA Class:
Must be ACTIVE and RACLISTED

Profile names:
Defined to match the application name of the authenticating application
Applications identify themselves to SAF/RACF authentication processing with an 8-character application name specified via RACROUTE REQ=VERIFY APPL='applname' parameter.

RDEFINE/RALTER Commands - SSIGNON Segment:

[SSIGNON([KEYMASKED(key-value)	- Specified key is masked in RACF DB
| KEYENCRYPTED(key-value)	- Specified key is encrypted in ICSF (Label in RACF DB)
| ENCRYPTKEY	- Migrates an existing masked key to encrypted
| KEYLABEL(label-value)])]	- Specified ICSF Label is stored in RACF DB

Migrating Masked PassTickets Keys

Migrate KEYMASKED to KEYENCRYPTED:

- The V2R4 **ENCRYPTKEY** keyword can be used to encrypt a **KEYMASKED** key and move it into ICSF.

```
RALTER PTKTDATA MYAPPL SSIGNON(ENCRYPTKEY)
```

- PassTicket KEYMASKED Keys can be converted in bulk with the SEARCH command:
  - Generate the CLIST:

```
SEARCH CLASS(PTKTDATA) CLIST('RALTER PTKTDATA ' '  SSIGNON(ENCRYPTKEY)')
```

  - Review results which are saved in the dataset:

```
'MYUSER.EXEC.RACF.CLIST'
```

  - Run the Exec:

```
EXEC 'MYUSER.EXEC.RACF.CLIST'
```

NEW in V2R5 – Enhanced PassTickets

Enhanced PassTickets:

- Intended to function the same way as “Legacy” PassTickets while modernizing the algorithm
- Same capabilities as Legacy PassTickets:
  - Generated by a trusted application to allow it to authenticate users to other z/OS applications
  - Specified in the 8-Character Password field of an application logon screen
  - Generated from shared secret key
  - Can be generated on-platform or off-platform

Enhancements:

- Generation and evaluation algorithm updates
  - Update from DES to a modern cryptographic algorithm (HMAC with SHA-512)
  - Optional expanded character set
  - Configurable validity period

Enhanced PassTickets - Configuration

Configured via profiles in the PTKTDATA Class:

- Same class, profile name and segment as Legacy PassTickets:
- PTKTDATA class must be ACTIVE and RACLISTED
- Same profile name structure – Matches application name
- New keywords in SSIGNON segment

RDEFINE/RALTER Commands – New SSIGNON Segment Keywords:

[SSIGNON([KEYMASKED(key-value)	- Specified Legacy key is masked in RACF DB
| KEYENCRYPTED(key-value)	- Specified Legacy key is encrypted in ICSF (Label in RACF)
| ENCRYPTKEY	- Migrates an existing masked Legacy key to encrypted
| KEYLABEL(label-value)	- Specified ICSF Label of a Legacy key is stored in RACF DB
| NOLEGACYKEY]	**- NEW - Remove Legacy PassTicket key from the profile**
[EPTKEYLABEL(label-value)]	**- NEW - Identify Enhanced PassTicket Key Label in ICSF**
[TYPE(UPPER | MIXED)]	**- NEW - Enhanced PassTicket type**
[TIMEOUT(timeout-seconds)]	**- NEW - Enhanced PassTicket validity period**
[REPLAY (YES | NO)]	**- NEW - Enhanced PassTicket can be replayed?**
)]	

Enhanced PassTickets – SSIGNON Segment

NOLEGACYKEY – Remove an existing Legacy PassTicket key:
- There is no keyword currently documented to remove the existing Legacy PassTicket key

EPTKEYLABEL – Enhanced PassTicket ICSF Key Label:
- Identifies the ICSF HMAC Key used to generate and evaluate an Enhanced PassTicket

TYPE – Enhanced PassTicket type
- Specifies the character set to use for generating and evaluating an Enhanced PassTicket.
  - **UPPER** – Uppercase characters A-Z and digits 0-9.
  - **MIXED** – (default) Uppercase characters A-Z, lowercase characters a-z, digits 0-9 and the symbols dash '-' and underscore '_'.
    - Using type MIXED is recommended as it provides a larger set of possible PassTicket values and therefore provides more security. Type UPPER may be required when an application or installation does not yet support mixed case passwords (SETR PASSWORD(NOMIXED)).

TIMEOUT – Enhanced PassTicket Expire Time:
- Legacy PassTickets have a defined life of 10 minutes before or after issue time. Enhanced PassTickets have a configurable expire time.
- Defines how many seconds an Enhanced PassTicket is valid before it expires.
- Allows for clock skew and network delays.
- Valid range: 1-600 seconds. Default value: 60 seconds

REPLAY – Enhanced PassTicket Replay Allowed:
- Defines if the Enhanced PassTicket can be Replayed within the TIMEOUT expire time.
- Does not use the APPLDATA field that Legacy PassTickets use.
- Default value: NO

PassTicket APIs

z/OS applications can call SAF APIs to generate and evaluate PassTickets.

RCVT function and SAF/RACF Callable services:

- **RCVTPTGN** – Generate PassTickets (or Enhanced PassTickets)
- **R_Gensec** – Generate and Evaluate PassTickets (or Enhanced PassTickets)
- **R_TicketServ**– Generate and Evaluate PassTickets (or Enhanced PassTickets)

These services will generate and evaluate Enhanced PassTickets when they are configured via the SSIGNON segment without any changes to the calling application.

- No parameter changes
- No Return Code changes

Improved PassTicket API Diagnostics:

- Detailed error reason codes can be returned.
- RCVTPTGN – Reason code in REGISTER 0

R_Gensec & R_TicketServ:

- Evaluate Extended sub-function code – Returns new reason codes
- **NEW:** Generate extended sub-function code – Same function, but returns detailed failure reason codes
- Calling applications should capture these reason codes in trace records for diagnostics.
- They will also appear in relevant SMF records

PassTicket Auditing

Unconditional Auditing:

- RACF always logs information about certain events because knowing about these events is essential to an effective data-security mechanism.
  - Successful RACROUTE REQUEST=VERIFY authentication using a PassTicket
    - Authentication with an Enhanced PassTicket will also trigger an audit record

SMF Type 80 Audit Records for Enhanced PassTickets:

- **Event 1(1):** JOB INITIATION/TSO LOGON/TSO LOGOFF
  - Existing Event Code qualifiers:
    - 32 (20) SUCCESSFUL INITIATION USING PASSTICKET Logon was achieved using a PassTicket.
    - 33 (21) ATTEMPTED REPLAY OF PASSTICKET Logon was rejected because of attempted replay of a PassTicket.
  - Relocate 443 – Records authenticator types
    - **New bits will indicate Enhanced PassTicket was evaluated and/or successful**
- **Event 81 (51):** PassTicket Evaluation
  - Will indicate PassTicket evaluation details via new Relocate 67
- **Event 82 (52):** PassTicket Generation
  - Will indicate PassTicket evaluation details via new Relocate 67
- These audit records can be used to determine which type of PassTickets are being used per application on the system.

Enhanced PassTicket - Migration

z/OS Applications which use SAF PassTicket generation / Evaluation APIs:

- Should not need to be updated to support Enhanced PassTickets.
- The system configuration will determine which type of PassTicket to generate or evaluate.

Migration to enhanced PassTickets:

- To assist installation migration from Legacy PassTickets to Enhanced PassTickets, both can be configured in the same PTKTDATA class profile.

When both Legacy PassTickets and Enhanced PassTickets are configured:

- SAF/RACF Generation (RCVTPTGN, R_Gensec, R_Ticketserv):
  An enhanced PassTicket will be generated.
- SAF/RACF Evaluation (R_Gensec, R_Ticketserv, RACROUTE REQ=VERIFY, initACEE):
  The input value will be evaluated as both a Legacy PassTicket and Enhanced PassTicket

Enhanced PassTicket - Migration

Enhanced PassTickets with type MIXED have some additional considerations for applications and installations:

Type MIXED includes a larger character set than type UPPER:

- UPPER: A-Z, 0-9 (Same as Legacy PassTickets)
- MIXED: A-Z, a-z, 0-9,-_

The installation must have mixed case passwords enabled via SETROPTS:

- SETROPTS PASSWORD(MIXED)

z/OS Applications:

- Must support mixed case passwords
- Must not fold the PassTicket value to uppercase
- Must support the special chars “-” and “_” in the password field

Enhanced PassTickets – More Details

Enhanced PassTicket support is available now on z/OS V2R3 and V2R4 via the PTFs for:
RACF APAR: OA59196
SAF APAR: OA59197

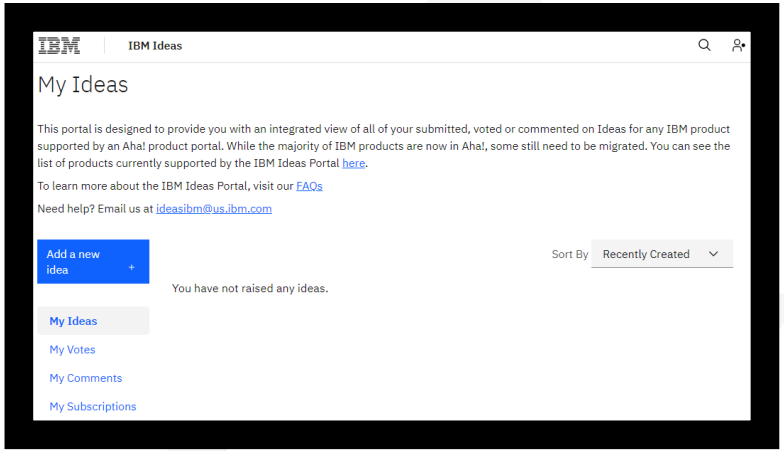
Links:

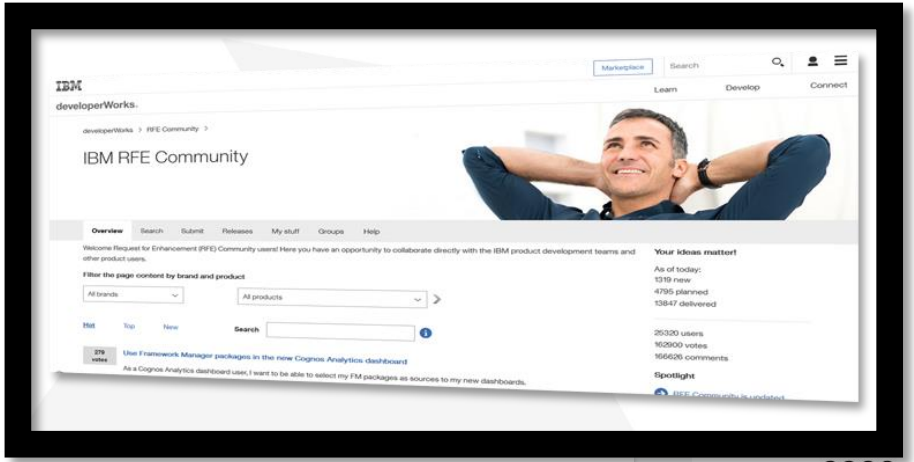
- **RACF APAR:** https://www.ibm.com/support/pages/apar/OA59196
- **SAF APAR:** https://www.ibm.com/support/pages/apar/OA59197
- **APAR DOC:** ftp://ftp.software.ibm.com/s390/zos/racf/pdf/oa59196.pdf

RFE / IDEAS

Request For Enhancements (RFE) / Ideas

- **Requirements should be submitted to IBM via RFE / Ideas:**
  - Reviewed by the design and development teams
  - Facilitates a dialog between clients and IBM
  - **RFE Link:** https://www.ibm.com/developerworks/rfe
  - **Ideas Link:** https://ideas.ibm.com





IBM® z/OS® Security Server RACF® Update Spring 2023 Edition

Ross Cooper, CISSP®
RACF Design and Development, IBM Poughkeepsie
May, 2023

HEALTH CHECKS

IBM Health Checker for z/OS

- **IBM Health Checker for z/OS – Monitors the health of your system:**
  - Identify configuration outside of recommendations
  - Helps avoid outages
  - Helps with release migration
- **RACF Health Checks:**
  - Write your own RACF resource checks!
  - RACF_AIM_STAGE
  - RACF_AUDIT_CONTROLS
  - RACF_BATCHALLRACF
  - RACF_CERTIFICATE_EXPIRATION
  - RACF_classname_ACTIVE
  - RACF_ENCRYPTION_ALGORITHM
  - RACF_GRS_RNL
  - RACF_IBMUSER_REVOKED
  - RACF_ICHAUTAB_NONLPA
  - RACF_PASSWORD_CONTROLS
  - RACF_RRSF_RESOURCES
  - RACF_SENSITIVE_RESOURCES
  - RACF_UNIX_ID
  - ZOSMIGV2R1_DEFAULT_UNIX_ID
  - …

New V2R5 RACF Health Checks

- **RACF is introducing five new health checks:**
  1. Verify all data sets are protected by RACF
  2. Ensure all residual information is erased when data sets are deleted
  3. Verify that all PassTicket keys are encrypted and stored in ICSF
  4. Verify that RACF is enabled for Sysplex Communications
  5. Verify that the RACF address space is active

- **All these checks run every 24 hours**
  - You can change the severity, interval, or active / inactive status

- **See “Appendix A: New RACF Health Checks” at the end for more details.**

SAF & RACF
C HEADER FILES

SAF & RACF C Header files

- Shipped in /usr/include/zos and SYS1.SIEAHDR.H (along with many other header files for many other components)

File name	Description
ichsafp.c	SAF (RACROUTE) parameter list (SAFP)
ifasmfr9.c	SMF 80, 81, and 83 mappings
ihaacee.c	Accessor Environment Element (ACEE)
irrpcomp.c	SAF callable services parameter lists (COMP and others)
irrpcomx.c	64-bit SAF callable services parameter lists (COMX and others)
irrpcomy.c	64-bit SAF callable services parameter lists (COMY and others)
irrpripl.c	RACROUTE REQUEST=TOKENBLD, VERIFY, and VERIFYX request-specific parameter list (RIPL)

PROFILE MANAGEMENT WITH ALTER ACCESS

RACF Administrative Authority

- **RACF Administrative Authority can be granted in many ways:**
  - **User attributes** (SPECIAL, AUDITOR, ROAUDIT):
    - Grants broad authority to perform security administration and auditing
  - **Profile Ownership:**
    - Ownership of a profile allows administration
  - **Class Authorization (CLAUTH)**
    - Can create profiles for a specific class
  - **Class Specific Profiles** (FACILITY, UNIXPRIV…)
    - Grants authority to perform specific administrative functions
  - **Field Level Access Checking (FLAC):**
    - Grants authority to modify non-base segment fields in profiles

ALTER Access Administrative Authority

Profile Access:

- Authority to a RACF profile is used by the resource manager to determine permission to a resource.
- Resource Authorities:

  NONE, EXECUTE, READ, UPDATE, CONTROL, ALTER

ALTER Access:

- A user with ALTER access to a discrete DATASET or general resource profile not only gets access to the resource protected by the profile but can also manage the profile.
- This creates a separation-of-duties problem:
  - Some resource managers may assign meaning to ALTER access to a profile which in turn grants that user the authority to manage the profile

ALTER Access

Ways a user might have ALTER access to a discrete profile:

- A user ID (standard) access list entry with ALTER
- A group (standard) access list entry with ALTER
- A (standard) access list entry for ID(*) with ALTER
- A universal access (UACC) of ALTER
- ALTER access to a matching GLOBAL class member (Global Access Table)

ALTER Access Administrative Authority

SHARE
EDUCATE • NETWORK • INFLUENCE

ALTER access to a discrete profile allows a user to:

- **List / Copy Access Lists:**
  - List the access list (RLIST AUTHUSER, LISTDSD AUTHUSER, R_admin profile extract)
  - Copy the access list from another profile (RDEFINE FROM, ADDSD FROM, PERMIT FROM) to which you have ALTER access
- **Modify / Delete Profiles:**
  - Modify (RALTER, ALTDSD) the base segment of the profile, excluding the OWNER keyword.
  - Modify the access list (PERMIT)
  - Delete the profile (RDELETE, DELDSD)
- **Create ‘conflicts’:**
  - Define a discrete GLOBAL entry when you have ALTER access to the matching ‘base class’ profile
  - Define a matching grouping class member when you have ALTER access to the discrete member class profile
  - Define a discrete member class profile when you have ALTER access to a grouping class profile that has a matching member (also requires CLAUTH)
  - Define a discrete member class profile, or grouping class member, when you have ALTER access to a generic profile which currently covers the discrete name

ALTER Access – New Control

NEW - Restrict ALTER access from managing discrete profiles:

- A security administrator can define a FACILITY profile to prevent users with ALTER access to a discrete profile from managing the profile
- Exceptions can be made

Value:

- Eliminates one vector for an insider attack
- Easily provable to auditors
- Application designers need not strictly avoid incorporating ALTER access into their security designs

ALTER Access – New Control

Restrict ALTER access from managing discrete profiles:

- New FACILITY class profile:

  IRR.ALTER.*class-name*

- Authority to the IRR.ALTER.*class-name* profile:
  - **UPDATE** – ALTER access to a discrete profile continues to allow the user to manage that profile.
  - **Not at least UPDATE** – ALTER access to a discrete profile no longer allows the user to manage that profile.

Upgrade Considerations:

- Not defining the IRR.ALTER.*class-name* profile or defining it with a universal access of UPDATE access allows continuance of existing behavior.
- The covering profile must start with “IRR.ALTER.”:
  - This avoids a migration action in the event you have an existing backstop FACILITY profile (e.g. ** or IRR.*) with UACC(NONE), which would otherwise change the default behavior.

Examples

Restrict ALTER access from granting administrative authority for all classes:

```
RDEFINE FACILITY IRR.ALTER.* UACC(NONE)
```

To allow the behavior for user ANDREW, but only for the $MYCLASS class:

```
RDEFINE FACILITY IRR.ALTER.$MYCLASS UACC(NONE)
PERMIT IRR.ALTER.$MYCLASS CLASS(FACILITY) ID(ANDREW)
ACCESS(UPDATE)
```

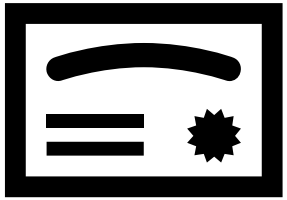
User ANDREW has administrative authority to any profiles he has ALTER access to in the $MYCLASS class.

CERTIFICATE FINGERPRINT

Certificate Fingerprint Support - Overview

Digital Certificates are widely used on z/OS:

- Server Authentication
- Client Authentication
- Program Signing
- Encrypted Packages



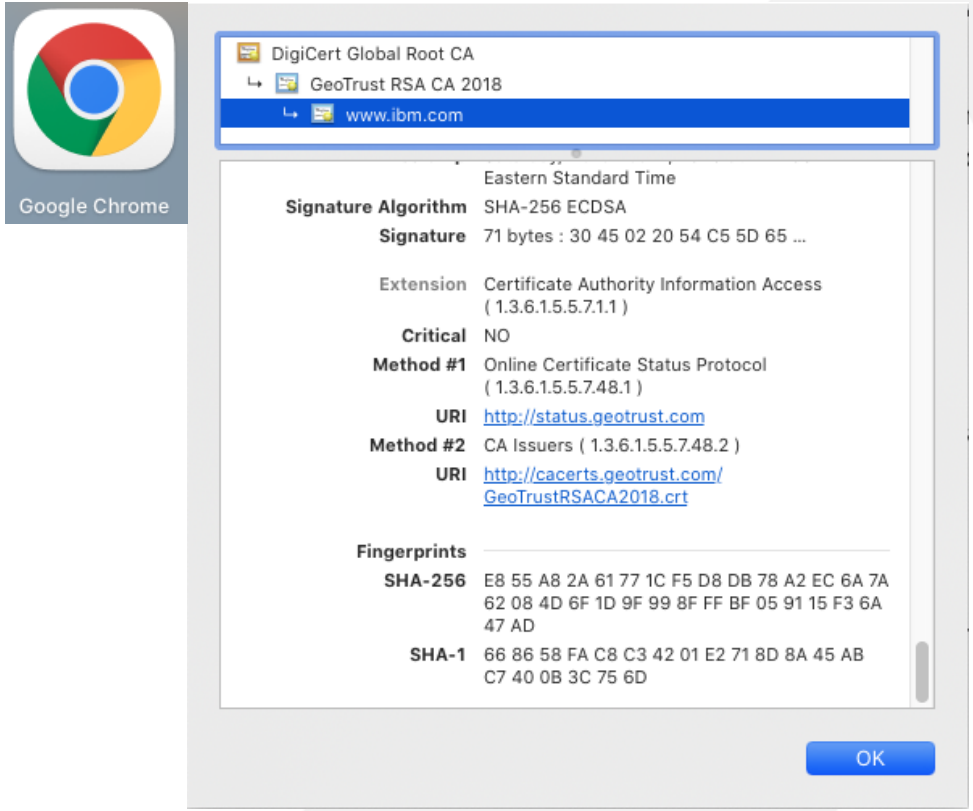
Challenges:

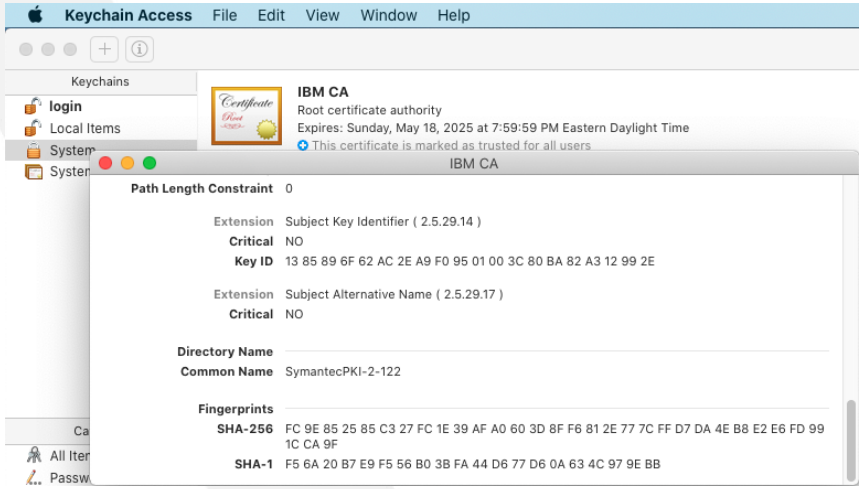
- How can a certificate be tracked across its life cycle:
  Generated / imported, accessed, expired and deleted?

Solution:

- Wouldn't it be nice if there was a way to uniquely identify a certificate in a standard way?

Certificate Fingerprint





Certificate Fingerprint or Thumbprint:

- Uniquely identifies a certificate
- Hash of the DER encoded x.509 certificate
- Most common certificate fingerprint hash algorithm used is SHA-256

Certificate Fingerprint Support

RACF is adding support to calculate and display the certificate fingerprint:

- RACDCERT certificate list commands
- RACF Database Unload
- Certificate SMF Records

PKI Services is adding support to calculate and display the certificate fingerprint:

- Webpage certificate list
- PKI Utilities
- Certificate SMF records

RACF Certificate Fingerprint Support

- **RACDCERT LIST, LISTCHAIN and CHECKCERT display SHA256 certificate fingerprint**

```
Label: samplecert
  Certificate ID: 2QbmxsPI1smJl4OFmaPy
  Status: TRUST
  Start Date: 2019/08/02 00:00:00
  End Date:   2024/08/02 23:59:59
…
  Certificate Fingerprint(SHA256):
      9C:3E:4A:FC:C4:91:DF:D3:32:F3:08:9B:85:42:E9:46:
      17:D8:93:D7:FE:94:4E:10:A7:93:7E:E2:9D:96:93:DE
```

RACF Certificate Fingerprint Support

RACF certificate SMF records now includes the SHA256 Certificate fingerprint:

- RACDCERT (Event code 66)
  - Generate, add, map, delete, connect…
- INITACEE (Event code 67)
  - APIs to Add and delete
- R_DATALIB (Event code 84)
  - APIs to Add, delete, connect to keyring, remove from keyring…

RACF certificate Database unload records now includes the SHA256 Certificate fingerprint:

```
CREATE TABLE USER01.GENR_CERTN_DATA (
     CERTN_NAME          CHAR(246)      NOT NULL,
     CERTN_CLASS_NAME    CHAR(8)        NOT NULL,
     CERTN_ISSUER_DN     VARCHAR(1024)  NOT NULL,
     CERTN_SUBJECT_DN    VARCHAR(1024)  NOT NULL,
     CERTN_SIG_ALG       CHAR(16)       NOT NULL,
     CERTN_CERT_FGRPRNT  CHAR(64)        NOT NULL
     )
     IN RACFDB2.IRRDBU00;
```

PKI Certificate Fingerprint Support

- Fingerprint is displayed with the other existing information from the result page of the query

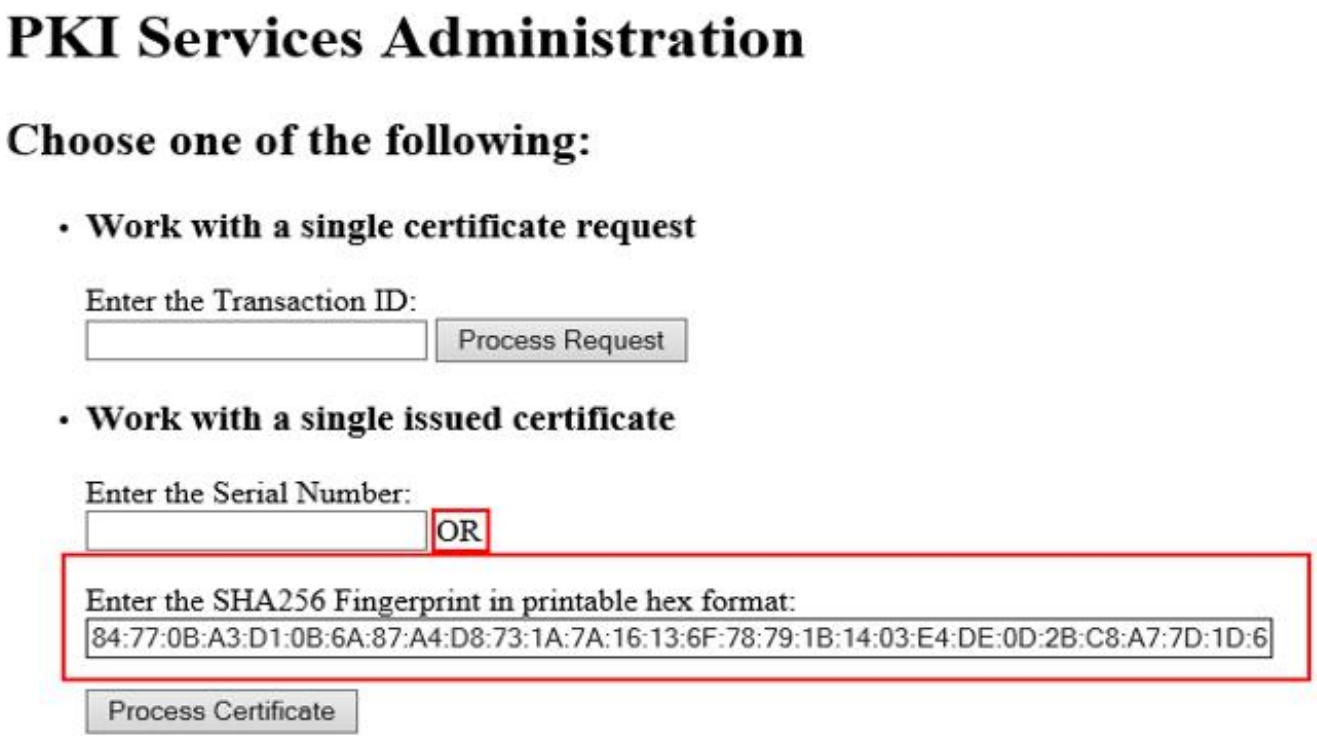
Issued Certificates

The following issued certificates matched the search criteria specified:

All ☑	Requestor	Certificate Information	Status	Key archived	Dates
☑	Joe Smith	**Serial #:** 13 **Template:**1-Year PKI SSL Browser Certificate **Subject:** CN=ServerA.pok.ibm.com,OU=PKI,O=The Firm **SHA256 fingerprint:**06:3E:4A:FA:C4:91:DF:D3:32:F3:08:9B:85:42:E9:46:17:D8:93:D7:FE:94:4E:10:A7:93:7E:E2:9D:96:93:C0	Active	No	**Created:** 2019/07/29 **Modified:**2019/07/29
☑	Mary Lee	**Serial #:** 14 **Template:**1-Year PKI SSL Browser Certificate **Subject:** CN=ServerB.pok.ibm.com,OU=PKI,O=The Firm **SHA256 fingerprint:**56:3T:4A:FA:C4:91:DF:D3:31:F3:08:9B:85:42:E9:46:17:D8:93:D1:FE:94:4E:10:A7:93:7E:E2:9D:96:93:K3	Active	No	**Created:** 2019/07/31 **Modified:**2019/07/31

PKI Certificate Fingerprint Support

- Fingerprint can be used as a search input



IDENTITY TOKENS

Identity Token Support

Identity Token:

- An Identity Token is used to assert user claims which can be trusted by the consumer of the token.
- Our use adheres to the JSON Web Token (JWT) IETF specifications: RFC 7519

RACROUTE Support for Identity Tokens:

- RACROUTE authentication processing can generate and validate Identity Tokens (IDT).
- **Generation -** Applications can request that an IDT be returned from RACROUTE.
- **Validation -** Applications can supply an IDT to authenticate a user instead of other credentials.

IDT Configuration:

- The security administrator can create profiles in the IDTDATA class:
  - Configure how certain fields in an IDT are generated and validated

Identity Token Support

Linking Multiple Authentication API Calls:

- In some cases, user authentication requires multiple steps:
  - **Expired Password / Invalid New Password / MFA Expired PIN …**
- **Problem:**
  - MFA credentials are one time use.
  - When multiple authentication calls are required, an already consumed MFA token will fail.
- **Solution:**
  - The Identity Token can be used to link authentication status information between multiple authentication API calls without replaying the MFA credentials.

Replaying Proof of Authentication:

- Some applications authenticate a user and “replay” that authentication multiple times.
- **Problem:**
  - Some applications cache the user provided credential and replay it back again later.
  - For users with one time use MFA tokens, this does not work.
- **Solution:**
  - The Identity Token support allows applications to authenticate a user and receive proof of that authentication which can be supplied back to RACROUTE in place of other credentials like a password.
  - Signed JWTs can be returned to an end user for later use by the application.

Identity Token Support

A JSON Web Token (JWT) is used to assert claims between multiple parties. They are often used to prove a user has been authenticated.

- **JWT RFC7519:** https://tools.ietf.org/html/rfc7519
- **Used by common authentication protocols:** OpenID Connect, Oauth2

JWT:

- **Header (JOSE):**
  - **{“alg” : “HS256” or “none”}** – Signature Algorithm: **HS256** = HMAC with **SHA-256**, none = unsecured
- **Body Claims – (JWS Payload):**
  - **{“jti” : “cb05…”,** – JWT Unique identifier
  - **“iss” : “saf”,** – Issuer name – Entity that created the JWT
  - **“sub” : “USER01”,** – Subject (the authenticated user)
  - **“aud” : “CICSLP8”,** – Audience – Target consumer of the JWT
  - **“exp” : 1486744112,** – Expiration time - (Seconds since 1970 - Expired tokens should be rejected)
  - **“iat”: 1486740112,** – Issued at – The time at which the JWT was issued.
  - **“amr”:[”mfa-comp”,”saf-pwd”]}** – Authentication Method References - Indicates how the subject was authenticated
- **Signature (JWS)** – Encoded in Binary
  - 389A21CD32108C3483DA

APPENDIX A: NEW RACF HEALTH CHECKS

New Check: RACF_PROTECTALL_FAIL

```
CHECK(IBMRACF,RACF_PROTECTALL_FAIL)
SYSPLEX:    LOCAL     SYSTEM: RACFR25
START TIME: 09/12/2020 00:23:53.548133
CHECK DATE: 20190520  CHECK SEVERITY: MEDIUM

* Medium Severity Exception *

IRRH333E SETROPTS NOPROTECTALL is in effect.

  Explanation:  The RACF_PROTECTALL_FAIL check has determined that
    SETROPTS NOPROTECTALL is in effect.  This may allow unexpected
    access to data sets on this system. IBM recommends that the
    appropriate profiles be defined before enabling SETROPTS
    PROTECTALL(FAIL) to allow the appropriate access to data sets on
    this system.
    RCVTPRO = 0 RCVTPROF = 0
  System Action:  The check continues processing. There is no effect on
    the system.

  Operator Response:  Report this problem to the system security
    administrator. Do not enable SETROPTS PROTECTALL(FAIL) without
    defining the appropriate profiles.

  System Programmer Response:  None.

  Problem Determination:  None.
```

RACF_PROTECTALL_FAIL

- Verify all datasets are protected by RACF
- Verify SETROPTS PROTECTALL(FAILURES) option is in effect

New Check: RACF_ERASE_ON_SCRATCH

```
CHECK(IBMRACF,RACF_ERASE_ON_SCRATCH)
SYSPLEX:    LOCAL     SYSTEM: RACFR25
START TIME: 09/12/2020 00:23:53.547910
CHECK DATE: 20190614  CHECK SEVERITY: MEDIUM

* Medium Severity Exception *

IRRH335E SETROPTS NOERASE is in effect.

  Explanation:  The RACF_ERASE_ON_SCRATCH check has determined that
    SETROPTS NOERASE is in effect. IBM recommends that all data set
    space which is freed during a SCRATCH or RELEASE operation be
    erased. This prevents the inadvertent disclosure of this data and
    can be enabled with RACF's SETROPTS ERASE(ALL) command.
    RCVTEOS = 0 RCVTEOSL = 0 RCVTEOSA = 0

   See the z/OS Security Server RACF Security Administrator's Guide for
   more information on SETROPTS ERASE. For more information on data set
   erasure, please see the Erasing DASD Data section in z/OS DFSMS
   Using Data Sets.

 System Action:  The check continues processing. There is no effect on
   the system.

 Operator Response:  Report this problem to the system security
   administrator. SETROPTS ERASE(ALL) should only be enabled after a
   careful evaluation of the potential performance impact of the data
   erasure.

 System Programmer Response:  None.
```

RACF_ERASE_ON_SCRATCH

- Ensure all residual information is erased when data sets are deleted
- Verify that SETROPTS ERASE(ALL) is enabled

New Check: RACF_PTKTDATA_CLASS

```
CHECK(IBMRACF,RACF_PTKTDATA_CLASS)
SYSPLEX:    LOCAL     SYSTEM: RACFR25
START TIME: 09/12/2020 00:23:54.645149
CHECK DATE: 20200701  CHECK SEVERITY: HIGH

                          RACF PassTicket Report

S Profile Name                     Key Label
- ------------------------------- ------------------------------------
E TSOIM13                          *MASKED*

* High Severity Exception *

IRRH339E One or more PassTicket keys is stored masked in the RACF
database.


 Explanation:  The RACF_PTKTDATA_CLASS check has determined that one or
   more profiles in the PTKTDATA class have a masked key.

 System Action:  The check continues processing. There is no effect on
   the system.

 Operator Response:  Report this problem to the system security
   administrator.

 System Programmer Response:  None.

 Problem Determination:  None.
```

RACF_PTKTDATA_CLASS

- Verify that all PassTicket keys are encrypted and stored in ICSF
- No MASKED PassTicket keys

New Check: RACF_SYSPLEX_COMMUNICATION

```
CHECK(IBMRACF,RACF_SYSPLEX_COMMUNICATION)
SYSPLEX:    LOCAL     SYSTEM: RACFR25
START TIME: 09/12/2020 00:23:53.547777
CHECK DATE: 20191008  CHECK SEVERITY: MEDIUM

* Medium Severity Exception *

IRRH342E RACF sysplex communication mode is not enabled.

  Explanation:  The RACF_SYSPLEX_COMMUNICATION check has determined that
    RACF sysplex communication mode is not enabled. IBM recommends RACF
    sysplex communication mode to be enabled to simplify security
    management.

    See z/OS Security Server RACF System Programmer's Guide for more
    information about RACF sysplex communication mode.

 System Action:  The check continues processing. There is no effect on
   the system.

 Operator Response:  Report this problem to the system programmer.

 System Programmer Response:  None.
```

RACF_SYSPLEX_COMMUNICATION

- Verify that RACF is enabled for Sysplex Communications

Sysplex Communication provides:

- Consistent RACF data set usage (data set names table, data set range table, buffer definition
- Propagation of certain RACF administrative commands (such as SETROPTS RACLIST(classname) REFRESH)
- Improved RACF cache granularity for the deletion of cached data

New Check: RACF_ADDRESS_SPACE

```
CHECK(IBMRACF,RACF_ADDRESS_SPACE)
SYSPLEX:    LOCAL     SYSTEM: RACFR25
START TIME: 09/12/2020 00:48:26.633163
CHECK DATE: 20200701  CHECK SEVERITY: MEDIUM

* Medium Severity Exception *

IRRH344E RACF address space is inactive.

  Explanation:  The RACF_ADDRESS_SPACE check has determined that the
    RACF address space is inactive. IBM recommends that you configure
    the RACF address space. This allows you to issue RACF commands from
    a logged-on MVS console, without requiring JES or TSO.

  System Action:  The check continues processing. There is no effect on
    the system.

 Operator Response:  Report this to the system programmer.

 System Programmer Response:  Configure the RACF Address Space.
```

RACF_ADDRESS_SPACE

- Verify that the RACF address space is active

The RACF Address space:

- Required for the remote execution of RACF commands, issuing RACF commands from the MVS console and RACF remote sharing.