

# RACF<sup>®</sup> for z/OS<sup>®</sup> V2.4 Update

Mark Nelson, CISSP<sup>®</sup>, CSSLP<sup>®</sup>

IBM

November 2019

Session **FA**



# RACF for z/OS V2.4 Preview

- **PassTickets Enhancements**
- **Custom Fields Enhancements**
- **R\_Admin & IRRXUTIL Enhancements**
- **Dynamic RRSF VSAM Data Set Re-allocation**
- **ACEE Modification Detection**
- **Pervasive Encryption**
- **Identity Token Support**
- **Common Criteria Evaluations**
- **Additional Sources of Information**

 RACF

# Just Announced and Delivered: The IBM z15!

- **Next generation of IBM Z Technology**

- Up to 190 client configurable cores
- 14% Single Thread Performance Improvement
- 25% maximum system capacity growth over z14
- New on-chip acceleration of compression for faster processing and more efficient storage of data
- System Recovery Boost
- Improved SSL/TLS handshake performance on z15 with Crypto Express7S compared to z14 with Crypto Express6S
- Statement of direction: FICON® or FCP Links from the z15 to the next generation of the IBM DS8900F storage family to be encrypted and protected



# PassTicket Enhancements

# PassTickets Overview

## What is a PassTicket?

- A one-time-use password substitute based on a **user ID**, an **application name**, the **current time**, and a **shared symmetric key** between the application generating the PassTicket and the application (RACF) evaluating it.
- Also known as 'Secured Signon'

## PassTicket Usage:

- PassTickets can be generated on z/OS or off platform – The algorithm is published
- **Applications:** Session managers, z/OS Comm Server - Express Logon Facility, WebSphere ..



## Learn more:

- RACF Security Administrator's Guide – 'Using the secured signon function' section
- RACF Macros and Interfaces – 'The RACF secured signon PassTicket'

# PassTickets Overview ...

**PassTicket Keys are defined in the SSIGNON segment of a PTKTDATA class profile:**

- The **KEYMASKED** option results in a masked key stored in the RACF database.
- The **KEYENCRYPTED** option results in an encrypted key stored in an ICSF key token. The *generated* ICSF CKDS key label is stored in the RACF database.

## Examples:

```
RDEFINE PTKTDATA MYAPPL SSIGNON(KEYMASKED(1234567812345678))
```

```
RDEFINE PTKTDATA MYAPPL SSIGNON(KEYENCRYPTED(1234567812345678))
```

## PassTicket Keys must be protected:

- Any entity that has access to the PassTicket keys defined on the system can logon to any user who is authorized to use that application.



# PassTickets – Key Label Reporting

## PassTickets SSIGNON Segment Key Label reporting:

- Currently, **RLIST** reports the following information for the **SSIGNON** segment:
  - When **KEYMASKED**: KEYMASKED DATA NOT DISPLAYABLE
  - When **KEYENCRYPTED**: KEYENCRYPTED DATA NOT DISPLAYABLE



**NEW** In V2.4, **RLIST** will report the ICSF Key Label name:

- When **KEYENCRYPTED**:  
 KEYENCRYPTED LABEL: IRR.SSIGNON.SY1.07192018.185056.915782

- Additional SSIGNON Key Label reporting:
  - **DBUNLOAD**, **R\_Admin** and **IRRXUTIL** are also enhanced to report the SSIGNON segment ICSF Key Label

# PassTickets – KEYMASKED Migration

**NEW**

## Migrate KEYMASKED to KEYENCRYPTED:

- The new **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'
```





# PassTickets – KEYLABEL Keyword

## Creating a PassTicket Key:

- Currently the only way to create a PassTicket key is through RACF commands.

```
RDEFINE PTKTDATA MYAPPL SSIGNON (KEYMASKED (1234567812345678) )
```

```
RDEFINE PTKTDATA MYAPPL SSIGNON (KEYENCRYPTED (1234567812345678) )
```



## KEYLABEL keyword:

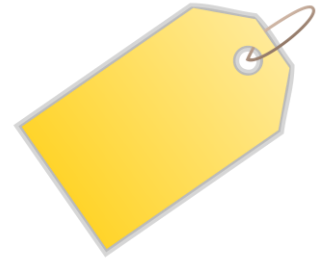
- In V2.4, the new **KEYLABEL** keyword can be used to associate an existing ICSF key with a PTKTDATA class profile:

```
RALTER PTKTDATA MYAPPL SSIGNON (KEYLABEL (IRR.PASSTICKET.MYAPPL.KEY) )
```

- Allows the installation to set its own ICSF key label naming convention.
- Listing the MYAPPL application will show the updated the PassTicket key:

```
RLIST PTKTDATA MYAPPL SSIGNON
```

```
KEYENCRYPTED LABEL: IRR.PASSTICKET.MYAPPL.KEY
```



# PassTickets – Configuration Simplification

## ICSF modules in LPA Requirement:

- Currently, RACF requires that a number of ICSF modules are copied into the Link Pack Area (LPA) in order to use the KEYENCRYPTED option.
- Failure to do so can result in some difficult to diagnose errors when generating or evaluating a PassTicket.



In V2.4, RACF no longer requires ICSF Modules in LPA.



# PassTickets - Diagnostics

## PassTickets Diagnostics:

- When a PassTicket does not evaluate successfully, debugging can be difficult.

## SMF Type 80 Event Code 1 (RACINIT) Relocate 443:

- When MFA support was added to RACF, relocate section 443 was added to all of the SMF type 80 event code 1 records to indicate details about the authentication attempt.
- Relocate 443 indicates whether a PassTicket was used for authentication and whether it was successful.
  - When not successful, the record includes internal return and reason codes

In V2.4, Relocate 443 will also include:

- NEW** • New reason code which indicates how far the PassTicket was from validity (time offset)
- The application name used in the evaluation process (caller provided or derived internally)

## RCVTPTGN:

- The RCVT anchored PassTicket generation service can be difficult to debug

- NEW** In V2.4, Register 0 will contain a failure Reason Code



# CUSTOM Fields Enhancements

# Custom Fields Overview

- Custom fields are fields within the RACF database that you customize to store security information about the users and groups at your installation.
- You can tailor the names and attributes of custom fields.
- Once you define custom fields, use RACF commands, such as the **ALTUSER** and **ALTGROUP** to add data to custom fields.
- Fields are stored in the **CSDATA** segment



# 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
```

# What about General Resource and Dataset profiles?!?!

# Custom Fields – General Resource and Dataset Profiles

**NEW** In V2.4, Custom Fields will support General Resource and Dataset class profiles!

- Works in the a consistent fashion with the existing ability for user and group profiles.

- For example, to create a DATASET profile field to contain character data:

```
RDEFINE CFIELD DATASET.CSDATA.MYFIELD  
        CFDEF (TYPE (CHAR) MAXLENGTH (50))
```

- To create a similar General Resource field:

```
RDEFINE CFIELD GENERAL.CSDATA.MYFIELD  
        CFDEF (TYPE (CHAR) MAXLENGTH (50))
```

- Note that a general resource field will apply to any general resource class by default.
  - You can write an exit to restrict the field to certain resource classes.



# Custom Fields – Validation Exit

**NEW** New VALREXX keyword:

- Identifies a REXX exec to be used to validate the field.
- Supported by all class types (USER, GROUP, DATASET and General Resource)
- Same exit can optionally be shared by multiple fields.

- Example VALREXX:

```
RALTER CFIELD DATASET.CSDATA.MYFIELD  
CFDEF (VALREXX (VALMYFLD) )
```



- **Note:** The existing IRRVAF01 dynamic exit is supported for the DATASET and general resource fields.

# R\_Admin & IRRXUTIL Enhancements

# R\_Admin Overview

## R\_Admin Callable service:

- RACF/SAF callable service which provides a programming interface to perform RACF administrative functions and retrieve RACF security data.
  - **Run RACF Commands**
  - **Retrieve Security Configuration:**
    1. RACF Profiles: USER, GROUP, General Resource classes (***not DATASET class profiles***)
    2. SETROPTS Configuration
    3. RACF Remote Sharing (RRSF) Configuration information
  - **Update Security Configuration:**
    1. RACF Profiles: USER, GROUP, General Resource classes, DATASET profiles
    2. SETROPTS Configuration

# R\_Admin Enhancements

## R\_Admin Callable service:

- RACF/SAF callable service which provides an API to perform RACF administrative functions and retrieve RACF security data.
  - **Run RACF Commands**
  - **Retrieve Security Configuration:**
    1. RACF Profiles: USER, GROUP, General Resource classes, **DATASET** (~~not DATASET class profiles~~)
    2. SETROPTS Configuration
    3. RACF Remote Sharing (RRSF) Configuration information
  - **Update Security Configuration:**
    1. RACF Profiles: USER, GROUP, General Resource classes, DATASET profiles
    2. SETROPTS Configuration



In V2.4, R\_Admin can retrieve DATASET class profile fields!

**Authority Required:** READ access to IRR.RADMIN.LISTDSD in the FACILITY class

# IRRXUTIL Overview

IRRXUTIL is a program that creates a set of REXX stem variables for several categories of RACF information.

- 1. RACF Profiles:**

USER, GROUP, General Resource classes, (**not DATASET profiles**)

- 2. SETROPTS Configuration**

- 3. RACF Remote Sharing (RRSF) Configuration information**

# IRRXUTIL Enhancements

IRRXUTIL is a program that creates a set of REXX stem variables for several categories of RACF information.

## 1. RACF Profiles:

USER, GROUP, General Resource classes, **DATASET**

## 2. SETROPTS Configuration

## 3. RACF Remote Sharing (RRSF) Configuration information

## 4. **Class Descriptor Table (CDT) Entries**


 NEW

In V2.4, IRRXUTIL can retrieve DATASET class profiles!




 NEW

In V2.4, IRRXUTIL can retrieve CDT entries!

- Supports both static and dynamic classes
- The current SETROPTS settings for the class can optionally be returned

# Dynamic RRSF VSAM Data Set Re-Allocation

# Dynamic RRSF VSAM Data Set Re-Allocation

- The RACF Remote Sharing Facility (RRSF) allows you to link together RACF data bases without requiring shared access to the DASD device which contains the RACF data sets
- RACF data base changes are propagated using either APPC or TCP/IP
- Data in flight can be encrypted in-flight (APPC:DES, TCP/IP: TLS)
- One pair of VSAM data sets per connected node
  - Data at rest in the VSAM data sets is masked
  - VSAM data sets are allocated on the RRSF TARGET command. Data set allocation is fixed at the time of first use
- 
 • The TARGET command now has two new keywords (NEWPREFIX and NEWWORKSPACE) which allow the allocation and use of new RRSF VSAM data sets
  - Without requiring a subsystem restart
  - Without losing any in-flight work
- 
 • The new VSAM data sets can be encrypted VSAM data sets!



# ACEE Modification Detection

# ACEE Overview

- **The Accessor Environment Element (ACEE) is a control block to represent a user's security environment.**
- The ACEE is created by RACF/SAF when a user authenticates to a z/OS application.
- **The contents are derived from information in the USER profile, containing:**
  - The user ID
  - List of GROUPs
  - Various authorities (SPECIAL, AUDITOR, OPERATIONS, etc)
  - Lots of other security environment details
- **The ACEE is used by RACF commands and RACF authorization checking to determine authority and access to resources.**
  - Does this USER have the authority required to perform this action (SPECIAL, AUDITOR...)
  - Does this USER have this level of access to this RESOURCE in this CLASS of resources.
- **It is anchored in the address space, or task, or created by an authorized application and passed explicitly to various SAF services.**

# ACEE Modification Detection

NEW

In V2.4, RACF can detect changes to a user's ACEE that result in elevated privilege:

- A new message is issued when such a modification is detected.
- Exceptions can be defined for trusted applications in order to suppress the message for users of such an application.

## Fingerprint:

- New fingerprint field in ACEE is created with RACROUTE REQ=VERIFY
- Fingerprint encapsulates the User ID and various authority-related fields (SPECIAL, TRUSTED...)

## Value:

- Useful in detecting programs that fall outside your security policy
- Useful in detecting programs that might be requesting more privilege than absolutely necessary

## Support rolled back to z/OS V2R3 with OA56851

- Details in <ftp://public.dhe.ibm.com/s390/zos/racf/pdf/oa56851.pdf>

# ACEE Modification Detection...

## What type of applications would modify an ACEE?

- A perfectly well-behaved and well-intentioned one that has no good alternatives
- A perfectly well-behaved and well-intentioned one that could, in fact, better use features of RACF to make the modification unnecessary
- A perfectly well-intentioned one that nonetheless does not adhere to the principle of least privilege
- A customer-written program that may or may not fall within the security policy of that installation (e.g. a system programmer's "productivity aid" in the form of a "magic SVC")
- Malware planted by an insider or intruder
- Malware exploiting a vulnerability in system software to regain control in an authorized state

# ACEE Modification Detection - Configuration

## ACEECHK Class:

- ACEE fingerprint is verified when **ACEECHK** class is active
- New message **IRR421I** is issued when privilege escalation is detected

```
IRR421I ACEE modification detected  
for user TSOUSR8 in address space ID 0x00000026 running under user  
TSOUSR8 and job name TSOUSR8 while program ADDUSER is running. The  
RACF function detecting the modification is IRRENV00.  
Rsn=0x60000000. (ACEEPRIV is ON) (ACEESPEC is ON). Occurrences 1.  
Command=ADDUSER. Call chain: ADDUSER <- IKJEFT02 <- IKJEFT01
```



## Program Exceptions:

- **IRR421I** can be suppressed for trusted programs by defining exception profiles in the **ACEECHK** class along the lines of:

```
RDEFINE ACEECHK IRR.EXCLUDE.TESTPROG
```

- When **IRR.ABEND.ON.FAILURE** is defined in the **ACEECHK** class:
  - When privilege escalation is detected and no exception is defined then **ABEND 4C6** is issued with new reason code **2766(X'ACE')**.

# Pervasive Encryption Support

# Pervasive Encryption – JES SPOOL Data Sets

**NEW** JES segment, intended for profiles in the JESJOBS class, containing a KEYLABEL field.

- As with data set (pervasive) encryption, the label refers to the ICSF encryption key to be used while encrypting JES spool data.
- Support delivered with APAR **OA57466**

**RALTER**

**JES | NOJES**

**JES**

Specifies the JES information for the profile being changed.

**KEYLABEL**(key-label) | **NOKEYLABEL**

**KEYLABEL**(key-label)

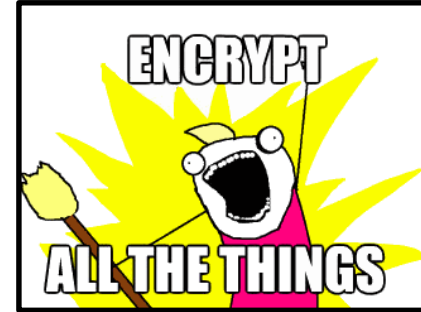
Specifies the name of an ICSF key label to be used when encrypting spool data for resources that are covered by the profile.

**NOKEYLABEL**

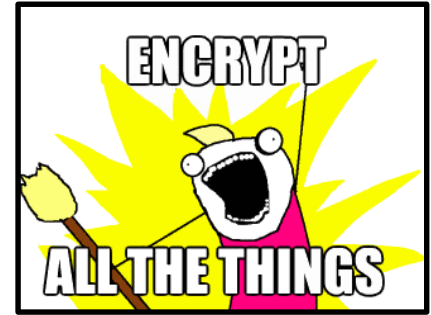
Specifies that you want to delete the key-label from the JES segment of the profile.

**NOJES**

Specifies that you want to delete the JES segment from the profile.



# Pervasive Encryption



**Are you thinking about or using pervasive encryption?  
Please tell us!**

<http://ibm.biz/p-e-survey>



# Identity Token Support

# Identities in RACF

## Identities in z/OS can be assigned:

- **Directly** with the presentation of a user ID and an authenticator
  - TSO logon, batch job with user ID and password/password phrase
- **By inheritance**
  - Submitting a batch job from an authenticated session
- **By mapping**, where an external identity is asserted and then is mapped to a z/OS identity
- **By assertion**, as in the authentication is done outside of RACF and the authenticated identity is trusted
  - Resource manager specification of target identity
  - Surrogate job submission
  - PASSTICKETs

A gold circular icon with the word "NEW" in blue capital letters.

**With z/OS V2.4, RACF is introducing a new assertion mechanism, the JSON web token (pronounced “jot”)**



# Identity Token Support Overview

## Identity Token:

- An Identity Token is used to assert user claims which can be trusted by the consumer of the token.
- RACF 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 Overview...

## 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.





# Identity Token Support Overview ...

## 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 proof of that authentication which can be supplied back to RACROUTE in other credentials like a password.
  - Signed JWTs can be returned to an end user for later use by the application.





# JWT – JSON Web Token

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>



## JWT:

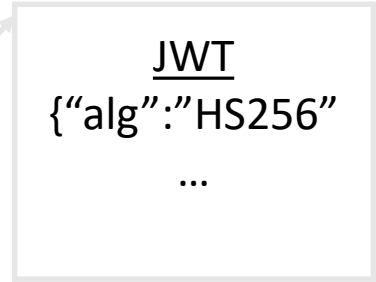
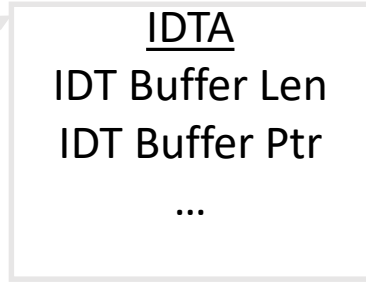
- **Header (JOSE):**
  - {"alg": "HS256" or "none"} – Signature Algorithm: **HS256** = HMAC with **SHA-256**, none = unsecured
- **Body Claims – (JWS Payload):**
  - {"jti": "cb05...", – JWT Unique identifier
  - "iss": "saf", – Issuer name – Entity that created the JWT
  - "sub": "USER01", – Subject (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)**
  - 389A21CD32108C3483DA – Encoded in Binary



# Identity Token Externals – RACROUTE REQ=VERIFY

- **New RACINIT Parameter: IDTA**

```
RACROUTE REQUEST=VERIFY  
  
, ...  
, IDTA=idta_data_addr  
, RELEASE=PLV0001  
  
, ...
```



**IDTA** - Specifies the address of the data structure that describes the identity token data. The address points to a data structure defined in a new SAF mapping macro named IRRPIDTA. The IDTA keyword can only be specified when RELEASE is set to PLV0001 or higher.



# Identity Token Externals – RACROUTE RELEASE

- **RELEASE=number**

specifies the release level of the parameter list to be generated by this macro. Through RACF 2.2, it corresponds to the FMID of the RACF release. After that, when RACF became solely an element of OS/390® or z/OS, it corresponds to the FMID of the RACF.

**NEW:** Starting with HRF77C0, the naming convention for the RELEASE keyword is updated to correspond to a parameter list version number. Version PLV0001 is the initial parameter list version number and contains all parameters in HRF77C0 and earlier.

...

77A0 corresponds to FMID HRF77A0 (z/OS Security Server V2R2)

77B0 corresponds to FMID HRF77B0 (z/OS Security Server V2R3)

PLV0001 corresponds to FMID HRF77C0 (z/OS Security Server V2R4)



# Administrative Control over IDTs

## IDTDATA Class profiles and IDTPARMS segment:

- Security administrators can control the use of tokens by defining profiles in the new IDTDATA general resource class, using a new IDTPARMS segment

## IDTDATA class:

- Must be **ACTIVE** before Identity Tokens will be generated or validated
- Must be **RACLISTed** before any profiles in the class will be used

## IDTDATA profile format: <IDT Type>.<application name>.<user ID>.<IDT issuer name>

- IDT Type – “JWT”
- Application name – The value specified in the APPL= parameter
- User ID – the user being authenticated
- IDT issuer name – “SAF”



**Note:** Generics are allowed. When a user is authenticated with a JWT, the best matching profile is used.

# Administrative Control over IDTs ...

IDTPARMS segment RALTER command keywords

```
[ IDTPARMS(
```

```
  [ SIGTOKEN(pkcs11-token-name) | NOSIGTOKEN ]
```

```
  [ SIGSEQNUM(pkcs11-sequence-number) | NOSIGSEQ ]
```

```
  [ SIGCAT(pkcs11-category) | NOSIGCAT ]
```

```
  [ SIGALG( HS256 | HS384 | HS512 ) | NOSIGALG ]
```

```
  [ ANYAPPL(YES | NO) ]
```

```
  [ TIMEOUT(timeout-minutes) ]
```

```
)
```

```
NOIDTPARMS ]
```

Location of the signing key

Signature algorithm to use

Whether token can be used by other applications

Validity interval of a token

# TSO Exploitation of Identity Tokens

- **TSO Logon process is updated to specify the new RACROUTE IDTA parameter.**
  - Supported in both pre-prompt and normal logon screens.
- **Improves logon experience for IBM MFA users:**
  - When multiple authentication API calls are required, the Identity Token keeps track of the current authentication state.
  - **Scenarios:**
    - Expired MFA PIN or expired Password, RSA Next Token Code Mode and MFA protocols which required multiple steps.

**Note:** Support is not activated in RACF until the IDTDATA class is ACTIVE.

```

File      Options  Keypad
-----
----- TSO/E LOGON -----
Enter LOGON parameters below:
Userid   ==>> HSLU099
Password ==>>
Procedure ==>> DBSPROCA
Acct Nbr ==>> ACCT#
Size     ==>> 20101
Perform  ==>>
Command  ==>>

Enter an 'S' before each option desired below:
-Nomail      -Nonotice    -Reconnect   -OIDcard

PF1/PF13 ==> Help   PF3/PF15 ==> Logoff  PA1 ==> Attention  PA2 ==> Reshow
You may request specific help information by entering a '?' in any entry field
  
```

# Other z/OS Security Enhancements/Changes

# Common Criteria Evaluations

- **z/OS**
  - **z/OS V2R3 EAL4+:** 31 July, 2019
  - **z/OS V2R3 RACF EAL5+:** 16 September, 2019
  - **z/OS V2R2 EAL4+:** 10 July, 2017
  - **z/OS V2R3 RACF EAL5+:** 25 August, 2017
- **z/VM**
  - **V6R4:** 24 April, 2018
  - **V6R3:** 3 March, 2015
- **PR/SM**
  - **PR/SM for IBM z14 and IBM LinuxONE Driver D32L with Bundle S35:** 5 April, 2019
  - **PR/SM for IBM z14 and IBM LinuxONE Driver D32L with Bundle S29:** 3 September, 2018
  - **PR/SM for IBM z13 GA2, z13s GA1, and IBM LinuxONE Driver Level D27i:** 14 September, 2016
  - **PR/SM for IBM z13 EC GA1 Driver Level D22H:** 15 October, 2015
- **Details:** <https://www.commoncriteriaportal.org/>

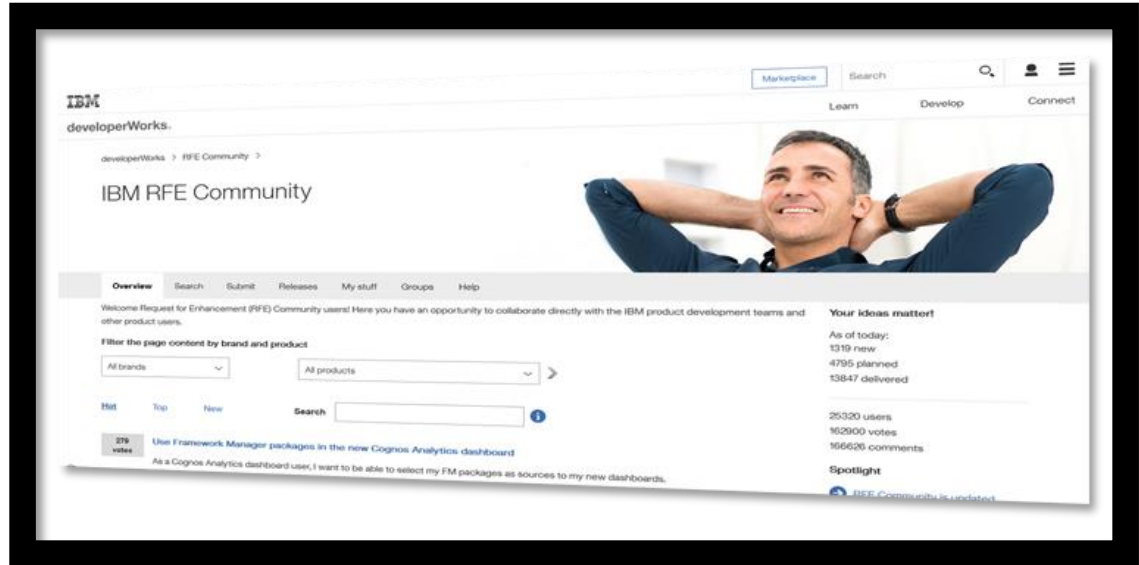
# Non-RACF z/OS Security Enhancements/Changes

- **Pervasive Encryption: z/OS V2R4 introduces pervasive encryption for these types of data sets:**
  - PDSE (including directory and member generations), with the exception that program objects cannot reside in encrypted PDSEs
  - Sequential basic format and large format SMS managed data sets using standard BSAM and QSAM (with APAR OA56622, 1Q2020)
    - Programs which are using EXCP can use a new access method encryption callable service
- **Quantum safe digital signatures for z/OS SMF records written to a log stream (requires z15)**
- **z/OS Data Privacy for Diagnostics is a z/OS capability exclusive to z15 with the ability to control access to data shared with business partners and eco-systems**
- **z/OS Network Authentication Services (NAS) support for Flexible Authentication Secure Tunneling (FAST)**
- **z/OS PKI Services support for Enrolment over Secure Transport (EST)**
- **User key common storage can no longer be allocated. APARs OA53355 and OA56180 are available on lower z/OS releases to assist in migration and identification of programs access user key common storage.**
  - The new Restricted Use Common Service Area (RUCSA) uses SAF checks to control access to common storage.
- **z/OS V2R4 is planned to be the last release that supports Enterprise Identity Mapping (EIM), Open Cryptographic Service Facility (OCSF), Open Cryptographic Enhanced Plug-in (OCEP), and PKI Services Trust Policy (PKITP)**

# REQUEST FOR Enhancements (RFE)

# Request for Enhancements (RFE)

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





# Want More?

# Shameless Plug #1: Podcasts

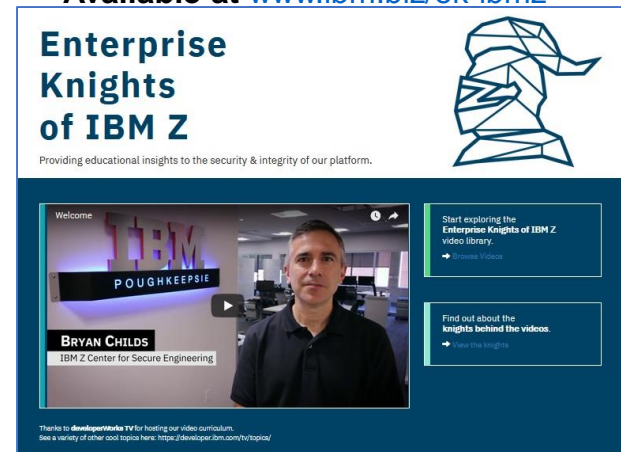
- **IBM Developer Works: Mainframe, Performance, Topics**
  - Hosts: Marna Walle, Martin Packer
  - <https://developer.ibm.com/tv/category/mpt/>
  
- **Terminal Talk**
  - Hosts: Frank DeGillio, Jeff Bisti
  - <http://terminaltalk.net/>



# Shameless Plug #2: The Enterprise Knights of IBM Z

- The Enterprise Knights of IBM Z have produced a series of short videos that provide educational insights to the security and integrity of the IBM Z platform
- Videos is short (less than ten minutes each) and cover a range of topics:
  - IBM Security Portal
  - CVSS Scores
  - AT-TLS
  - Authorized QNAMES
  - ETDEF
  - SSL/TLS Cipher Lists
  - Buffer Overflows
  - Untrusted Indirect Parameters
  - Pervasive Encryption
  - zERT
  - Untrusted Registers for PCs/SVCs
  - Asymmetric Encryption
  - The RACF\_SENSITIVE\_RESOURCES Health Check

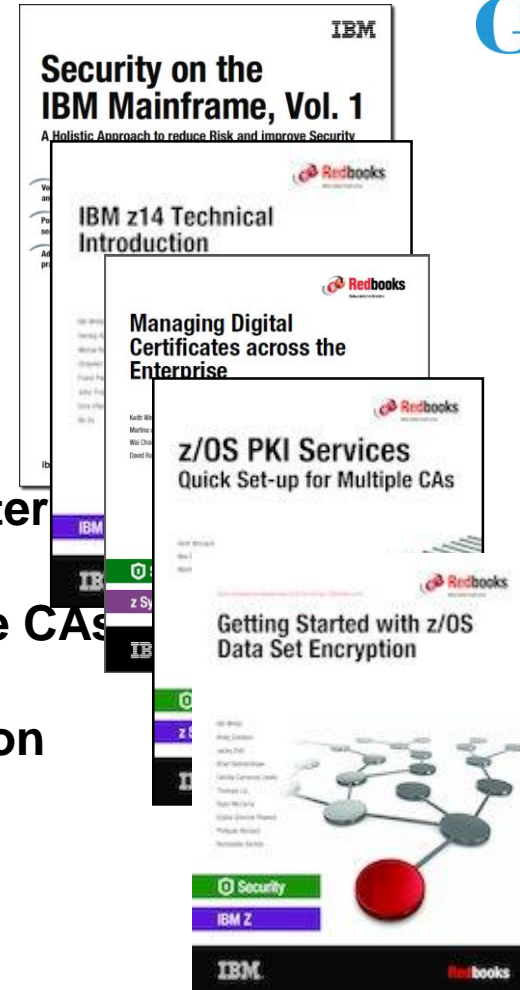
Available at [www.ibm.biz/ek-ibmz](http://www.ibm.biz/ek-ibmz)



The screenshot shows the landing page for the Enterprise Knights of IBM Z. At the top, the title "Enterprise Knights of IBM Z" is displayed in a large, bold, blue font. To the right of the title is a stylized blue knight chess piece icon. Below the title, a tagline reads "Providing educational insights to the security & integrity of our platform." The main content area features a video player on the left showing a man, Bryan Childs, in a dark shirt, with a name tag that says "BRYAN CHILDS" and "IBM Z Center for Secure Engineering". To the right of the video player are two blue call-to-action buttons: "Start exploring the Enterprise Knights of IBM Z video library." with a right-pointing arrow, and "Find out about the knights behind the videos." with a right-pointing arrow. At the bottom of the page, there is a small thank you message: "Thanks to developerWorks TV for hosting our video curriculum. See a variety of other cool topics here: <https://developer.ibm.com/tv/topics/>".

# Shameless Plug #3: Redbooks

- Security on the IBM Mainframe
- IBM z14 Technical Introduction
- Managing Digital Certificates across the Enterprise
- z/OS PKI Services: Quick Set-up for Multiple CAs
- Getting Started with z/OS Data Set Encryption



# Shameless Plug #4: zPet Test Community and Blog

## •IBM Z Platform Evaluation Test Community and Blog

- Real-world experiences configuring and operating the latest IBM Z technologies

- <http://ibm.biz/zPETBlog>

### LCST/e System z Platform Evaluation Test The Final Verification

z/OS | CICS | IMS | DB2 | WebSphere MQ |  
WebSphere Application Server | Tivoli | InfoSphere



We are a team of system programmers and testers that run a Parallel Sysplex on which we perform the final verification of a z/OS release and System z hardware and System Storage before they become generally available to clients. We gather our experiences and recommendations and document them here in our blog.



# RACF<sup>®</sup> for z/OS<sup>®</sup> V2.4 Update

Mark Nelson, CISSP<sup>®</sup>, CSSLP<sup>®</sup>

IBM

November 2019

Session **FA**

