RACF PassTickets

Trademarks

The following are trademarks of the International Business Machines Corporation in the United States and/or other countries.

IBM*
ibm.com*
IBM logo*

*** Registered trademarks of IBM Corporation**

Adobe, the Adobe logo, PostScript, and the PostScript logo are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States, and/or other countries.
IT Infrastructure Library is a Registered Trade Mark of AXELOS Limited.
ITIL is a Registered Trade Mark of AXELOS Limited.
Linear Tape-Open, LTO, the LTO Logo, Ultrium, and the Ultrium logo are trademarks of HP, IBM Corp. and Quantum in the U.S. and other countries.
Intel, Intel logo, Intel Inside, Intel Inside logo, Intel Centrino, Intel Centrino logo, Celeron, Intel Xeon, Intel SpeedStep, Itanium, and Pentium are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.
Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.
Zowe™, the Zowe™ logo and the Open Mainframe Project™ are trademarks of The Linux Foundation.
Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.
Java and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.
Cell Broadband Engine is a trademark of Sony Computer Entertainment, Inc. in the United States, other countries, or both and is used under license therefrom.
UNIX is a registered trademark of The Open Group in the United States and other countries.
VMware, the VMware logo, VMware Cloud Foundation, VMware Cloud Foundation Service, VMware vCenter Server, and VMware vSphere are registered trademarks or trademarks of VMware, Inc. or its subsidiaries in the United States and/or other jurisdictions.
Other product and service names might be trademarks of IBM or other companies.

Notes:

Performance data contained herein was generally obtained in a controlled, isolated environments. Customer examples are presented as illustrations of how those customers have used IBM products and the results they may have achieved. Actual performance, cost, savings or other results in other operating environments may vary.
IBM products are manufactured from new parts or new and used parts. In some cases, a product may not be new and may have been previously installed. Regardless, our warranty terms apply.”
All customer examples cited or described in this presentation are presented as illustrations of the manner in which some customers have used IBM products and the results they may have achieved. Actual environmental costs and performance characteristics will vary depending on individual customer configurations and conditions.
This publication was produced in the United States. IBM may not offer the products, services or features discussed in this document in other countries, and the information may be subject to change without notice. Consult your local IBM business contact for information on the product or services available in your area.
All statements regarding IBM's future direction and intent are subject to change or withdrawal without notice, and represent goals and objectives only.
Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products about this publication and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products.
Prices subject to change without notice. Contact your IBM representative or Business Partner for the most current pricing in your geography.
Information regarding potential future products is intended to outline our general product direction and it should not be relied on in making a purchasing decision.
The information mentioned regarding potential future products is not a commitment, promise, or legal obligation to deliver any material, code or functionality. Information about potential future products may not be incorporated into any contract.
This information provides only general descriptions of the types and portions of workloads that are eligible for execution on Specialty Engines (e.g, zIIPs, zAAPs, and IFLs) ("SEs"). IBM authorizes customers to use IBM SE only to execute the processing of Eligible Workloads of specific Programs expressly authorized by IBM as specified in the “Authorized Use Table for IBM Machines” provided at www.ibm.com/systems/support/machine_warranties/machine_code/aut.html (“AUT”). No other workload processing is authorized for execution on an SE. IBM offers SE at a lower price than General Processors/Central Processors because customers are authorized to use SEs only to process certain types and/or amounts of workloads as specified by IBM in the AUT.

What is a PassTicket?

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.
- **AKA:** “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’

User Authentication with PassTickets

User Authentication:

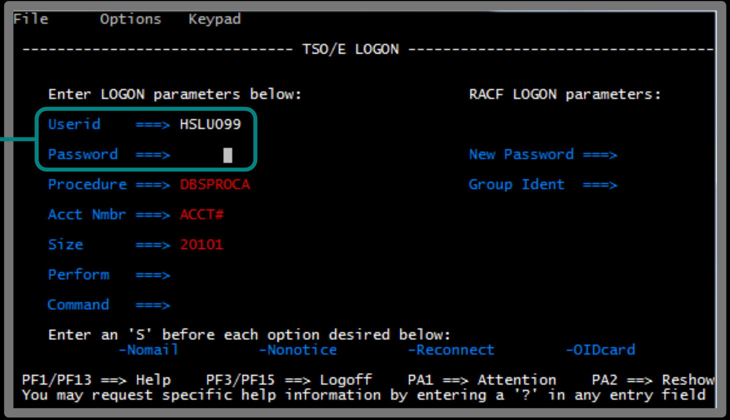
- Users are authenticated on z/OS by applications by prompting a user for a user ID and password / authenticator and calling SAF/RACF authentication APIs.

User Authentication APIs:

- RACROUTE REQUEST=VERIFY
- initACEE – SAF Callable Service
- UNIX APIs: __passwd(), BPX1PWD
- z/OS Java: PlatformUser.Authenticate()

All these authentication APIs support PassTickets:

- When PassTickets are configured for the Application, and the user provides a password sized credential, it is checked as both the user's password and as a PassTicket.



```
File      Options    Keypad
 ------------------------------- TSO/E LOGON ----------------------------------

   Enter LOGON parameters below:                        RACF LOGON parameters:

   Userid     ===> HSLU099

   Password   ===>                                      New Password ===>

   Procedure  ===> DBSPROCA                             Group Ident  ===>

   Acct Nmbr  ===> 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
```

RACF
RACROUTE REQ=VERIFY:

- Check as Password
- Check as PassTicket

PassTicket Configuration

Configured via profiles in the PTKTDATA Class:

PTKTDATA Class:
Must be ACTIVE and RACLISTED

Profile names:
Defined to match the <u>application name </u>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
```

NEW - Enhanced PassTickets – Design Goals

Enhanced PassTickets:

- Intended to function the same way as “Legacy” PassTickets while modernizing the 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

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 PassTickets - 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 PassTickets – Type MIXED Considerations

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

Application Support for Enhanced PassTickets

Vendors that implement the PassTicket algorithm in their own software will need to:

- Add new configuration settings:
  - Which type of PassTicket is to be generated - Legacy / Enhanced UPPER / Enhanced MIXED
  - Configure new Enhanced PassTicket HMAC key
- Add a capability to generate either Legacy or Enhanced PassTickets based on configuration
- Add support for generation of Enhanced PassTickets

Request enhanced PassTicket Support:

- Please contact your software vendors and request that they add support for enhanced PassTickets.

Enhanced PassTickets – More Details

Enhanced PassTickets are now available on z/OS V2R4 and V2R3 via the PTFs:

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

Thank You!

Ross Cooper
rdc@us.ibm.com