z/OS V2.5 IBM Education Assistant

Solution Name: RACF enhanced PassTicket

Solution Element(s): RACF

Agenda

- Trademarks
- Objectives
- Overview
- Usage & Invocation
- Interactions & Dependencies
- Upgrade & Coexistence Considerations
- Installation & Configuration
- Summary
- Appendix

Trademarks

- See url http://www.ibm.com/legal/copytrade.shtml for a list of trademarks.
- Additional Trademarks:
  - None

Objectives

- **RACF PassTickets are widely used by many clients:**
  - Useful in a variety of situations
  - Supported by virtually all z/OS applications

- **Existing PassTicket support:**
  - Introduced in 1993
  - Underlying cryptographic algorithm is DES
  - It’s time for a new optional PassTicket algorithm option

Overview

- **Who (Audience)**
  - Many z/OS installations use RACF/SAF PassTicket technology.
- **What (Solution)**
  - Enhanced PassTickets - RACF has introduced a new PassTicket algorithm option called Enhanced PassTickets
- **Wow (Benefit / Value, Need Addressed)**
  - Stronger cryptographic algorithm
  - Configurable validity period
  - Optionally expanded character set
  - Migration path is supported from Legacy to Enhanced
  - Improved error diagnostics and additional information logged in SMF

PassTicket 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.
- Also known as: “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

New – Enhanced PassTickets

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

New – 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?
)]

New – 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

PassTickets 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

PassTickets 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 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

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.

Interactions & Dependencies

- **Software Dependencies**
  - Enhanced PassTicket support requires ICSF running with a variable record length CKDS
- **Hardware Dependencies**
  - Enhanced PassTicket support requires a crypto coprocessor in CCA mode.
    - ICSF support for HMAC clear keys is in progress (does not require a coprocessor)
- **Exploiters**
  - Native z/OS applications that generate, evaluate and authenticate PassTickets:
    - Automatically support enhanced PassTickets without any changes.
    - SAF services – RACROUTE, R_GenSec, R_TicketServ, RCVTPTGN – support enhanced PassTickets
  - Applications that implement the PassTicket generation algorithm:
    - PassTicket algorithms are documented in RACF publications and some vendors implement it off platform
    - Will need to be updated to support the new enhanced PassTicket algorithm.

Upgrade & Coexistence Considerations

- **Exploitation:**
  - Enhanced PassTicket support is now available on supported previous releases (V2R4 & V243):
    - **RACF:** OA59196
    - **SAF:** OA59197

- **Upgrade actions or Coexistence:**
  - No upgrade actions or coexistence apars required:
    - Existing legacy PassTicket support continues to work in the same way

Installation & Configuration

- List anything that a client needs to be aware of during installation:
  - **APARs or PTFs needed for enablement:**
    - None, but there is support on V2R3 and V2R4
  - **Other:**
    - No specific hardware configuration for install
    - No PARMLIB statements or members are needed
    - No system programmer procedures required
    - No special web deliverables needed
    - No changes any system defaults

Summary

- Enhanced PassTickets:
  - RACF has introduced a new PassTicket algorithm option called Enhanced PassTickets:
    - Stronger cryptographic algorithm
    - Configurable validity period
    - Optionally expanded character set
    - Migration path is supported from Legacy to Enhanced
    - Improved error diagnostics and additional information logged in SMF
  - In base release of V2.5 and already available via continuous delivery:
    - RACF APAR OA59196 and SAF APAR OA59197
    - Available on z/OS V2.3 and later.

Appendix

- **Publications (V2R4 pubs updated):**
  - RACF Security Administrator's Guide – Chapter - ‘Using PassTickets’
  - RACF Macros and Interfaces – Chapter - ‘The RACF PassTicket’
  - RACF Command Language Reference – ADDUSER / ALTUSER SSIGNON segment
  - RACF Callable Services – R_Gensec / R_TicketServ
  - RACF Data Areas
  - RACF Messages and Codes

- **Enhanced PassTickets are now available on z/OS V2R4 and V2R3 via the PTFs for:**
  - RACF APAR: OA59196
  - SAF APAR: OA59197

- **APAR 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*