z/OS 3.2 IBM Education Assistant

Solution Name: RACF AES Password and Password Phrase Enveloping Support

Solution Element(s): z/OS Security Server RACF

July 2025

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.

Objectives

The Challenge: Prior to this support RACF password and password phrase envelope processing only supports non-quantum safe encryption (3DES, DES, RC2) and signing (MD5, SHA1) cryptographic algorithms.

The Objective: Add support for quantum-safe encryption (AES) and signing (SHA2) cryptographic algorithms for RACF password and password phrase enveloping processing.

Overview

- **Who (Audience)**
  - RACF installations who sync z/OS passwords (and password phrases) with other platforms using password envelope support.
- **What (Solution)**
  - RACF password envelope support is enhanced to support for quantum-safe encryption (AES) and signing (SHA2) cryptographic algorithms.
- **Wow (Benefit / Value, Need Addressed)**
  - Stronger protection for passwords being shared with other platforms.
  - Regulatory compliance.

Usage & Invocation (1)

RACF password and password phrase enveloping allows installations to detect RACF password and password phrase changes and create an encrypted version to sync with other systems.

How Enveloping Works:

- When an eligible user's password or password phrase is changed, the new value is encrypted under a public key within a key ring associated with the user ID of the RACF subsystem address space. The encrypted value is then stored in the user's profile.
- When an application requests the password or password phrase, RACF decrypts the value, and then encrypts it in PKCS #7 format for recipients whose digital certificates have been placed on the same RACF key ring.
- An authorized application can then decrypt the envelope using the recipient's private key.
- The R_Admin callable service (IRRSEQ00) provides the interface by which an application can retrieve an envelope.

Password Enveloping Cryptographic Algorithms:

- Configuring the cryptographic algorithms:

```
RDEFINE RACFEVNT PASSPHRASE.ENVELOPE APPLDATA('MD5/STRONG’)
RDEFINE RACFEVNT PASSWORD.ENVELOPE APPLDATA('MD5/STRONG')
```

- **Signing Options:** SHA1 or MD5
- **Encryption Options:** STRONG (Triple DES), MEDIUM(DES) or WEAK(RC2)
- Not NIST approved. Not quantum-safe.

Usage & Invocation (2)

Starting with z/OS 3.2 and PTF for APAR OA66067 (z/OS 3.1) RACF password and password phrase enveloping is enhanced to support the AES encryption and SHA2 signing algorithms.

New Password Enveloping Cryptographic Algorithms:

- **New SHA2 signing hash algorithms:**
  - x509_alg_sha512Digest, x509_alg_sha384Digest, x509_alg_sha256Digest
- **New AES encryption algorithm is:**
  - x509_alg_aesCbc256

Example:

```
RALTER RACFEVNT PASSWORD.ENVELOPE APPLDATA('x509_alg_sha512Digest/x509_alg_aesCbc256')
```

Usage & Invocation (3)

Steps to exploit AES encryption for Password and Password Phrase Envelopes:

1. **Confirm AES password envelope support is available:**
   - Be on z/OS 3.2 (or) apply PTF for OA66067 (z/OS 3.1) and IPL (all systems that share the RACF database)
   - AES algorithm should not be configured for password envelopes until all systems sharing the RACF database have the support available.
     - When RACF password and password phrase enveloping is configured with AES encryption or SHA2 signing introduced by APAR OA66067 a system that does not have RACF AES password and password phrase enveloping support installed will create password and password phrase envelopes with the default encryption strength (STRONG) and default signing algorithm (MD5)
   - Ensure all consumers of envelopes have support for these cryptographic algorithms
2. **Configure AES/SHA2 Envelopes:**
   - Update RACFEVNT class profiles to use AES encryption and SHA2 signing:

```
RDEFINE RACFEVNT PASSWORD.ENVELOPE APPLDATA('x509_alg_sha512Digest/x509_alg_aesCbc256’)
RDEFINE RACFEVNT PASSPHRASE.ENVELOPE
APPLDATA('x509_alg_sha512Digest/x509_alg_aesCbc256’)
```

3. **Envelope Passwords:**
   - User’s passwords are enveloped with the currently configured algorithm when their password is changed.

Interactions & Dependencies

- Software Dependencies
  - None
- Hardware Dependencies
  - None
- Exploiters
  - None

Upgrade & Coexistence Considerations

- To exploit this solution, all systems in the Plex:
  - Must be at the new z/OS level (or)
  - Must be on z/OS 3.1 with PTF for APAR OA66067 applied
  - When password envelopes are configured with AES encryption or SHA2 signing A system that does not have RACF AES password enveloping support in the base or with the required PTFs installed:
    - Will create password envelopes with the default encryption strength (STRONG - TDES) and default signing algorithm (MD5).
    - When unrecognized APPLDATA values are encountered a message is issued: **IRRC133I**
- List any toleration/coexistence APARs/PTFs: None
- List anything that doesn't work the same anymore:
  - When configured, RACF can create password and password phrase envelopes with stronger cryptographic algorithms.

Installation & Configuration

- Are any APARs or PTFs needed for enablement? Not on 3.2.
  - Function is also available on 3.1 via PTF for OA66067
- What jobs need to be run? None
- What hardware configuration is required? None
- What PARMLIB statements or members are needed? None
- Are any other system programmer procedures required? No
- Are there any planning considerations? No
- Are any special web deliverables needed? No
- Does installation change any system defaults? No

Summary

- RACF password and password phrase enveloping processing now supports quantum-safe encryption (AES) and signing (SHA2) cryptographic algorithms for RACF password and password phrase enveloping processing which provides stronger protection for passwords being shared with other platforms and regulatory compliance.

Appendix (1)

IBM Publications

- *SA23-2289-xx - z/OS Security Server RACF - Security Administrator's Guide*
  - *Chapter 25. Password and password phrase enveloping*

APAR Details:

https://www.ibm.com/support/pages/apar/OA66067

Appendix (2)

Terminology:

- **Password Envelope** – Function in RACF used to sync passwords changed on RACF with other platforms.
- **PKCS#7** – ASN1 encoded Industry standard format for an encrypted package.