z/OS 2.4 IBM Education Assistance (IEA)

Solution (Epic) Name: RSASSA-PSS Certificates

Element(s)/Component(s): PKI Services, RACF, System SSL

Agenda

- Trademarks
- Session Objectives
- Overview
- Usage & Invocation
- Interactions & Dependencies
- Migration & Coexistence Considerations
- Session Summary
- Appendix

Trademarks

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

Session Objectives

- At the end of this presentation, you will have an understanding of:
    - Why x.509 certificates were enhanced to support signing of certificates with RSASSA-PSS digital signatures?
    - How to use these enhancements to recreate and manage these types of certificates through PKI Services, RACF and System SSL.
    - Understand how these enhancements affect installation, migration and coexistence.

Overview

- Who (Audience)
  - System Administrators whose companies' secure connections are protected using System SSL's TLS that are moving to TLS 1.3 (updated TLS 1.2) and want to utilize certificates signed with the improved RSASSA-PSS digital signature.
- What (Solution)
  - To give administrators this capability, PKI services, RACF's RACDCERT and System SSL's gskkyman and certificate APIs will be updated to support the creation and management of these certificates.
- Wow (Benefit / Value, Need Addressed)
  - For protected TLS connections that are moved to TLS 1.3 or the enhanced TLS 1.2, and both ends of the secure connection support RSASSA-PSS, installations that wish to utilize certificates signed using the RSASSA-PSS digital signatures now will have this capability.

Note: Support requires signing RSA key to be of type RSAEncryption (1.2.840.113549.1.1.1).

Overview – RACF

- Using the enhanced RSASSA-PSS capabilities within RACF's RACDCERT certificate command, a system administrator can use:
    - RACDCERT ADD to add a certificate with RSASSA-PSS signature to the SAF database and connect it to a SAF key ring through RACDCERT CONNECT.
    - RACDCERT CHECKCERT to check if a dataset contains a certificate with a RSASSA-PSS signature
    - RACDCERT LIST and LISTCHAIN to display a certificate with RSASSA-PSS signature
    - RACDCERT GENCERT and REKEY to generate a certificate with RSASSA-PSS signature using a new keyword SIGATTR
        - RSAPSS is the only acceptable value for this new keyword
        - the keyword only applies to a RSA signing key

Usage & Invocation - RACF

- RACDCERT GENCERT SUBJECT(…) RSA SIGATTR(RSAPSS)…
- RACDCERT GENCERT SUBJECT(…) RSA(PKDS(*)) SIGATTR(RSAPSS)…
- RACDCERT GENCERT SUBJECT(…) RSA(TOKEN(MYTOKEN.TOKEN1)) SIGATTR(RSAPSS)…
  - Signing digest for the digital signature is dependent on the RSA key size

- RACDCERT REKEY(LABEL(‘<RSA cert>’)) RSA SIGATTR(RSAPSS)…
- RACDCERT REKEY(LABEL(‘<RSA cert>’)) RSA(PKDS(*)) SIGATTR(RSAPSS)…
- RACDCERT REKEY(LABEL(‘<RSA cert>’)) RSA(TOKEN(MYTOKEN.TOKEN1)) SIGATTR(RSAPSS)…
- RACDCERT ADD(<dataset contain one or more certs which has RSASSA-PSS signature>)…
- RACDCERT LIST /LISTCHAIN/ CHECKCERT display the RSASSA-PSS signature, eg.

```
Signing Algorithm: sha256RSAPSS (if the signing key is 2048 bits)
Key Type: RSA
Key Size: 2048

Signing Algorithm: sha512RSAPSS (if the signing key is 4096 bits)
Key Type: RSA
Key Size: 4096
```

Overview - System SSL

- Using the enhanced RSASSA-PSS capabilities within System SSL users and application writers can:

  - Use the gskkyman certificate management utility to:
    - create RSA certificates and certificate requests with RSASSA-PSS signatures
    - using a RSA CA certificate, sign another certificate with a RSASSA-PSS signature.
    - Store the certificates into a key database file or PKCS#11 token
    - List RSASSA-PSS signed certificates

  - Application writers, through the Certificate Management APIs, can:
    - create RSA certificates and certificate requests with RSASSA-PSS signatures
    - using a RSA CA certificate, sign another certificate with a RSASSA-PSS signature.
    - Store the certificates into a key database file
    - Create PKCS #7 Cryptographic Message Syntax signed data message using a RSASSA-PSS signature

Usage & Invocation – System SSL

Certificate Management Services (CMS) APIs updated to support creation of certificates/CRLs signed using RSASSA-PSS, PKCS#7 signed data messages, direct calls to perform RSASSA-PSS digital signing/verification and certificate validation.

gsk_construct_certificate()
gsk_construct_renewal_request()
gsk_construct_self_signed_certificate()
gsk_construct_signed_certificate()
gsk_construct_signed_crl()
gsk_create_certification_request()
gsk_create_database_renewal_request()
gsk_create_database_signed_certificate()
gsk_create_self_signed_certificate()
gsk_create_signed_certificate_record()
gsk_create_signed_crl_record()

gsk_create_revocation_source()
gsk_validate_certificate_mode()

gsk_make_signed_data_content()
gsk_make_signed_data_content_extended()
gsk_make_signed_data_msg()
gsk_make_signed_data_msg_extended()
gsk_read_signed_data_content()
gsk_read_signed_data_content_extended()
gsk_read_signed_data_msg()
gsk_read_signed_data_msg_extended()

gsk_sign_certificate()
gsk_sign_crl()
gsk_sign_data()
gsk_verify_certificate_signature()
gsk_verify_crl_signature()
gsk_verify_data_signature()

Usage & Invocation – System SSL

When creating a self signed certificate using an RSA key with an RSASSA-PSS signature there is a new option.

```
      Select certificate usage (press ENTER to return to menu):
          Certificate Key Algorithm

        1 - Certificate with an RSA key
        2 - Certificate with a DSA key
        3 - Certificate with an ECC key
        4 – Certificate with an RSA key and RSASSA-PSS signature algorithm
```

Note:

A similar new option is present when creating a signed certificate authority or end user certificate with a RSA Certificate authority certificate.

gskkyman supports creation with RSA key sizes of 2048 and 4096

Usage & Invocation – System SSL

Displaying a certificate with an RSASSA-PSS signature, the digest size and mask algorithms are displayed individually

```
Label: RSASSA_PSS_CA
             Record ID: 8
      Issuer Record ID: 8
               Trusted: Yes
               Version: 3
         Serial number: 5994505b0008ac16
           Issuer name: RSASSA_PSS_CA
                        IBM
                        US
          Subject name: RSASSA_PSS_CA
                        IBM
                        US
        Effective date: 2017/08/16
       Expiration date: 2018/08/16
   Signature algorithm: rsassa-pss
      Digest Algorithm: sha256Digest
        Mask Algorithm: Mgf1                       Note: Mgf1 is the only supported mask alg value
      Issuer unique ID: None
     Subject unique ID: None
  Public key algorithm: rsaEncryption
       Public key size: 2048
```

Usage & Invocation – System SSL

The RSASSA-PSS support signature type defined in gskcms.h are:

- **x509_alg_mgf1Sha256WithRsaSsaPss (102)**
  - RSASSA-PSS using SHA-256 digest with mask generation algorithm 1
- **x509_alg_mgf1Sha384WithRsaSsaPss (103)**
  - RSASSA-PSS using SHA-384 digest with mask generation algorithm 1
- **x509_alg_mgf1Sha512WithRsaSsaPss (104)**
  - RSASSA-PSS using SHA-512 digest with mask generation algorithm 1

RSA *key* sizes 2048 through 4096 inclusive are supported.

Overview - PKI Services

- Using the enhanced RSASSA-PSS capabilities within PKI Services, a system administrator can:

  - generate certificates with an RSASSA-PSS signature
    - Make use of System SSL's new support on gsk_sign_data

  - use an RSASSA-PSS CA certificate to sign certificates
    - Make use of RACDCERT's new support on GENCERT/ADD for the root CA instance

  - sign CRL / OCSP response with an RSASSA-PSS signature
    - Make use of System SSL's new support on gsk_construct_signed_crl and gsk_sign_data

Usage & Invocation – PKI Services

- Configuration through pkiserv.conf
  - New entries for the RSASSA-PSS signature algorithm are defined in the [OID] section as the encryption OID and hash OIDs:

    ```
    [OIDs]
    …
    rsassa-pss=1.2.840.113549.1.1.10
    sha-256Hash=2.16.840.1.101.3.4.2.1
    sha-384Hash=2.16.840.1.101.3.4.2.2
    sha-512Hash=2.16.840.1.101.3.4.2.3
    ```

  - Specify the SigAlg1 entry in the CertPolicy section with the above values for the corresponding OIDs. Hash OID string must be specified after the rsassa-pss algorithm string, separated by a comma. For example:

    ```
    [CertPolicy]
    SigAlg1=rsassa-pss,sha-256Hash
    ```

- Displaying the signature algorithm for Certificate requests and Certificates that were created with an RSASSA-PSS algorithm, which will appear as a single string value, e.g:

  ```
  sha-256WithRSAPSS
  sha-384WithRSAPSS
  sha-512WithRSAPSS
  ```

Interactions & Dependencies

- To exploit this item, all systems in the Plex must be at the new z/OS level:
  - Yes – if PKI Services is running as the same CA instance on multiple members of the plex and sharing the same pkiserv.conf file.
  - Yes – RACF (for generating and adding)
- Software Dependencies
  - None
- Hardware Dependencies
  - Crypto express cards as usual when keys are stored in PKDS or TKDS
- Exploiters
  - Exploiters of System SSL (ie. AT-TLS, Tivoli Directory Server) using TLS 1.2 or TLS 1.3 that want to use RSASSA-PSS signed certificates for their connections

Migration & Coexistence Considerations

- Ensure the ECC master key which protects the RSA private key is activated before issuing RACDCERT commands with the RSASSA-PSS signature keyword.
  - You may check it by using ICSF panel option 1 to look at the CCA coprocessor's ECC master keys status

- To utilize RSA certificates created through RACDCERT prior to 2.4 with their keys in the PKDS, to sign using RSASSA-PSS, the key format must be changed. See sample –
  - https://www.ibm.com/developerworks/community/blogs/79c1eec4-00c4-48ef-ae2b-01bd8448dd6c/entry/Translate_an_existing_RSA_private_key_to_be_used_in_PKCS_PSS_digital_signature_formatting_method?lang=en
  - Sample uses ‘FR-PSS ' (format restriction keyword), it will prevent you from signing with the RSASSA-PKCS1-v1_5 RSA signature
  - Specifying ‘FR-NONE’ allows RSA key to be used for both RSASSA-PSS and RSASSA-PKCS1-v1_5

Session Summary

- You should now be able to:
  - Understand the RSASSA-PSS support in PKI Services, RACF and System SSL
  - Understand the Migration and Coexistence Considerations
  - Be able to identify relevant documentation
- Any Questions?

Appendix

- z/OS Cryptographic Services PKI Services Guide and Reference
- z/OS Cryptographic Services System SSL Programming
- z/OS Security Server RACF Command Language Reference