z/OS V1R13

RACF: Hardware ECC support for RACDCERT

Session objectives

- Digital certificates usage has been growing
- Continuous enhancements to fulfill customer requirements
- Two main components on certificate support:
  - RACF: RACDCERT command and the R_datalib callable service
  - PKI Services
- At the end of this presentation, you should have an understanding of the support from:
  - RACF:
    - Hardware Elliptic Curve Cryptography (ECC) support
  - PKI Services:
    - Hardware Elliptic Curve Cryptography (ECC) support

Overview

- Problem Statement / Need Addressed
  - In z/OS V1R12, through the ICSF PKCS#11 support, RACF and PKI Services started the support on Elliptic Curve Crypto (ECC) based certificates. However the implementation was based on software only, which can't provide the level of protection on key as the hardware.
  - The way used to name different key types in RACF was not clear. For example key types Non-ICSF, ICSF, PCICC in fact are all RSA keys. Adding support for more key types worsen the situation.
- Solution
  - In this release, RACF can generate keys with the ECC algorithm through the hardware using a new crypto function which exploits the new Crypto Express 3 Cryptographic Coprocessor (CEX3C) and stores the key in PKDS protected by the Master Key; PKI Services can use a hardware ECC certificate as its CA certificate.
  - We restructure the key types in the RACDCERT command to make them more intuitive and more consistent for input and output.
  - There are 4 public/private key types supported in RACF: RSA, DSA, NIST ECC and Brainpool ECC. Except for DSA, you have a choice to generate/store the key in ICSF PKDS protected by the Master Key. We use both the key type and the place it is stored to clear the confusion.

INPUT KEY TYPE IN RACDCERT GENCERT	**KEY TYPE DISPLAYED IN RACDCERT LIST**
NISTECC	Key Type: NISTECC (no PKDS label entry)
NISTECC(PKDS)	Key Type: NISTECC PKDS Label: <system generated label>
NISTECC(PKDS(<specified label>))	Key Type: NISTECC PKDS Label: <specified label>
BPECC	Key Type: BPECC (no PKDS label entry)
BPECC(PKDS)	Key Type: BPECC PKDS Label: <system generated label>
BPECC(PKDS(<specified label>))	Key Type: BPECC PKDS Label: <specified label>
RSA = no key type specified	Key Type: RSA (no PKDS label entry)
RSA(PKDS) = PCICC	Key Type: RSA PKDS Label: <system generated label>
RSA(PKDS(<specified label>))	Key Type: RSA PKDS Label: <specified label>

- Benefit / Value
  - This new support is intended to allow you to expand your use of certificates with ECC keys protected by hardware and simplify the key type usage in the RACDCERT command.
  - Consolidate the key types to make it more comprehensive

Usage and invocation

- RACDCERT command and panels
  - New sub keyword PKDS is added to indicate the key is a hardware key. For examples:
    - Generate a certificate with NIST ECC key stored in PKDS with system generated key label
      - RACDCERT GENCERT SUB(CN('Company A')) WITHLABEL('New NISTECC cert') **NISTECC(PKDS)**

        - Generate a certificate with Brainpool ECC key stored in PKDS with key label BPECCFORA
            - RACDCERT GENCERT SUB(CN('Company A')) WITHLABEL('New BPECC cert') **BPECC(PKDS(BPECCFORA))**
    - Panels and corresponding help panels for GENCERT and REKEY will be updated to handle the new types.
- R_datalib callable service
    - New private key types X'00000009' (ECC key token), will be handled by functions DataGetFirst and DataGetNext
- PKI Services IKYSETUP (A REXX script to set up authorization for PKI)
    - Update the key_type value to 6 for hardware NISTECC, 7 for hardware BPECC
        - key_type=6
        - key_type=7

Interactions and dependencies

- Software Dependencies
    - ICSF web deliverable #10
- Hardware Dependencies
    - Crypto Express3 Coprocessor (CEX3C) card on IBM zEnterprise server
- Exploiters
    - System SSL

Migration and coexistence considerations

- None

Installation

- None

Session summary

- You should now have an understanding of the support from:
    - **RACF:**
        - Hardware Elliptic Curve Cryptography (ECC) support
    - **PKI Services:**
        - Hardware Elliptic Curve Cryptography (ECC) support

Appendix - References

- Publication references
    - PKI Services Guide and Reference (*SA22-7693*)
    - Security Server Command Language Reference *(SA22-7687)*