# z/OS V2.5 IBM Education Assistant

Solution Name: Enforce SAF checking of private-key name in ECC tokens

Solution Element(s): ICSF in z/OS V2.5

August 2021

# 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

- Describe updates in ICSF made to enable SAF CSFKEYS profile checking support for private-key name for ECC keys consistent with other PKA key key private-key name checking for ECC and QSA

# Overview

- Who (Audience)
  - System Administrators
- What (Solution)
  - ICSF will allow System Administrators to turn on ECC private-key name checking.
  - Once turned on, the ECC private-key name checking setup and function will be the same existing setup and function uses for RSA and QSA keys.
- Wow (Benefit / Value, Need Addressed)
  - Administrators can configure ICSF to do the same SAF checking of the private-key name in ECC keys that is always done for RSA and QSA keys.

# Usage and Invocation

A new message indicating ECC private-key name checking is enabled/disabled will be issued

- When the new XFACILIT profile is defined at ICSF initialization
- When the new XFACILIT profile is updated after ICSF initialization

CSFM726I CSFKEYS PKA ECC PRIVATE-KEY NAME CHECKING CONTROL IS enabled/disabled

# Usage and Invocation

- A new XFACILIT profile checked by ICSF has been defined – this enables the function, but does not alone cause private-key name checking to be done
- For example

  RDEF XFACILIT CSF.CSFKEYS.PKAECC.PRIVATEKEYNAME.ENABLE

  SETR CLASSACT(XFACILIT) RACLIST(XFACILIT)

  SETR RACLIST(XFACILIT) REFR
- The new XFACILIT profile name is described under Key Store Policy controls
- The administrator would need to enable Key Store Policy checking for the PKDS and optionally define a CSFKEYS profile with the same name as the private-key name

# Usage and Invocation

EXAMPLE

1. Define the XFACILIT profile that enables private-key name checking for ECC keys (this new and additional step for ECC keys is not needed for RSA and QSA tokens) .
    1. SETR CLASSACT(XFACILIT) RACLIST(XFACILIT)
    2. RDEF XFACILIT CSF.CSFKEYS.PKAECC.PRIVATEKEYNAME.ENABLE
    3. SETR RACLIST(XFACILIT) REFR
2. Turn on Key Store Policy for PKDS (needed for all private key-name checking)
    1. RDEF XFACILIT CSF.PKDS.TOKEN.CHECK.LABEL.FAIL
3. Define a CSFKEYS profile using the private-key name in the token (optional)
    1. RDEF CSFKEYS ECC#PRIVATE#KEYNAME UACC(READ)
    2. SETR RACLIST(CSFKEYS) REFR

# Usage and Invocation

4. try to use the key via CSNDDSG -> RC 0
5. RALT  CSFKEYS ECC#PRIVATE-KEYNAME UACC(NONE)
6. try to use the key via CSNDDSG -> RC8 Reas 3E84

# Usage and Invocation

The ICSF Query Facility (CSFIQF and CSFIQF6) reports the XFACILIT setting for private-key name checking

**ICSF Query Facility (CSFIQF and CSFIQF6)**

*Table 464. Output for option ICSFST2*

| Element Number | Name | Description |
|---|---|---|
| ……. Version 2 fields | | |
| 13 | ICSF Status Field 10 | …. The second character in this string indicates the state of the CSFKEYS PKA ECD private-key name checking (XFACILIT profile CSF.CSFKEYS.ECC.PRI-VATEKEYNAME.ENABLE) Number Meaning |

# Interactions & Dependencies

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

# Upgrade & Coexistence Considerations

- To exploit this solution, all systems in the sysplex must be at the new z/OS level: NO
- No toleration/coexistence APARs/PTFs.
- No upgrade actions
- No Coexistence actions

# Installation & Configuration

- List anything that a client needs to be aware of during installation and include **examples** where appropriate - clients appreciate these:
  - Are any APARs or PTFs needed for enablement? no
  - 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? Yes - to use the function see next slide
  - Are there any planning considerations? No
  - Are any special web deliverables needed? No
  - Does installation change any system defaults? No

# Installation & Configuration

As documented in ICSF System Programmer's Guide - Chapter 3. Migration there is a new optional migration action needed to enable the new function:

Actions to perform after the first start of ICSF in z/OS V2.5 (FMID HCR77D2)

To enable CSFKEYS checking of the private-key name in ECC private key tokens, the XFACLIT profile CSF.CSFKEYS.ECC.PRIVATEKEYNAME.ENABLE must be defined. In HCR77D2 ICSF has implemented CSFKEYS checking of the private-key name in PKA ECC private key tokens. CSFKEYS checking of the private-key name in PKA RSA and PKA QSA private key tokens has not changed and will continue to be done.

Also documented is the method to disable or correct authority problems indicated by RACF message ICS408I

- Disable the XFACILT profile instructions –OR-
- Define the CSFKEYS profiles needed for the private-key name

* See migration action has more details (required HW none, z/OS 2.5 SW, and summary of activation steps documents in the ICSF Admin Guide

# Summary

- A new XFACILIT profile has been defined to enable RACF checking of the private-key name in ECC tokens
- The profile must be defined to enable CSFKEYS private-key name checking for ECC keys
- As before, Key Store Policy must be enabled for the PKDS for private-key name RACF checking to be performed
- As before, a CSFKEYS profile with the same name as the private-key name would optionally be defined

# Appendix

z/OS ICSF Application Developers Guide

Chapter 14. Utilities -ICSF Query Facility (CSFIQF and CSFIQF6)

z/OS ICSF Administrator’s Guide

Chapter 3 Managing Cryptographic Keys

Chapter 5. Controlling who can use cryptographic keys and services

z/OS ICSF Messages

z/OS ICSF System Programmer’s Guide, Chapter 3. Migration