z/OS 3.2 IBM Education Assistant

Solution Name: ICSF Updates Crypto Insights

Solution Element(s): ICSF

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.

- Additional Trademarks: None

Objectives

This solution has 3 goals.

- Identify the job instances associated with a crypto request
- Provide the ability to associate crypto usage from different sources to their relevant job instance
- Present the lengths of keys that are normally obfuscated (hidden)

Overview

- Who (Audience)
  - z Crypto Discovery and Inventory (zCDI) solution
  - Security Architects, Application Programmers

- What (Solution)
  - Identify the job instances associated with a crypto request
  - Provide the ability to associate crypto usage from different sources to their relevant job instance
  - Present the lengths of keys that are normally obfuscated (hidden)

- Wow (Benefit / Value, Need Addressed)
  - Make it easier for a customer to understand their crypto posture
  - Make it easier to go from a weaker classical crypto posture to a stronger one
  - Make it easier to go from a non-quantum safe posture to one that is quantum-safe

Usage & Invocation

The information is presented via the ICSF SMF records which contain crypto usage information.

SMF Type 82 Subtype 31 (Crypto statistics), 40-42 (Key lifecycle), 44-47 (Key Usage) records will:

- Identify the job instances associated with a crypto request
- Provide the ability to associate crypto usage from different sources (e.g. SMF records) to their job instance
- Present the lengths of keys that are normally obfuscated (hidden)

SMF Type 82 Subtype 48 (Compliance Warning) records will:

- Present the lengths of keys that are normally obfuscated (hidden)

Interactions & Dependencies

- Software Dependencies
  - None

- Hardware Dependencies
  - None

- Exploiters
  - z Crypto Discovery and Inventory (zCDI) solution

Upgrade & Coexistence Considerations

- To exploit this solution, all systems in the Plex must be at the new z/OS level: No

- List any toleration/coexistence APARs/PTFs: None

- List anything that doesn't work the same anymore: None

Installation & Configuration

- List anything that a client needs to be aware of during installation and include **examples** where appropriate - clients appreciate these: N/A

Summary

ICSF is including additional data in SMF Type 82 Subtypes 31, 40-42, 44-47 that will:

- Identify the job instances associated with a crypto request

- Provide the ability to associate crypto usage from different sources to their job instance

- Present the lengths of keys that are normally obfuscated (hidden)

ICSF is including additional data in SMF Type 82 Subtype 48 records that allows the following:

- Present the lengths of keys that are normally obfuscated (hidden)

Appendix

- Publications
  - z/OS Cryptographic Services ICSF System Programmers Guide