z/OS 3.2 IBM Education Assistant

Solution Name: ICSF Support for IBM z17 GA1

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

- Review ICSF support for z17 GA1 CPACF
    - MSAE11: HMAC generation/verification
    - MSAE12: SHA-3 hashing and SHAKE XOF

Overview

- Who (Audience)
  - ICSF application programmers
- What (Solution)
  - Utilize new CPACF functionality available on z17 GA1
- Wow (Benefit / Value, Need Addressed)
  - Improved performance/reduced CPU cost for
    - HMAC generation/verification
    - SHA-3 hashing and SHAKE XOF

Usage & Invocation

- Use of the new CPACF functionality is automatic. Customers do not need to perform any actions to take advantage of this.

Interactions & Dependencies

- Software Dependencies
  - None

- Hardware Dependencies
  - z17 GA1 added two message-security-assist extensions (MSAE11 and MSAE12) that are used for this initiative.
    - This is only a dependency for better performance.

- Exploiters
  - N/A (no external changes)

Upgrade & Coexistence Considerations

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

- No toleration/coexistence APARs/PTFs

Installation & Configuration

- No special installation or configuration actions are needed

Summary

- ICSF will utilize updated CPACF functionality to improve performance and reduce CPU utilization for HMAC generation/verification, SHA-3 hashing, and SHAKE XOF operations.