z/OS 3.2 IBM Education Assistant

Solution Name: ICSF Support for CCA 8.3 QSA Update

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

Over the past few years, IBM z has added support for the various rounds of Crystals-Dilithium and Crystals-Kyber post-quantum cryptography (PQC) algorithms that have come out of the NIST PQC competition. NIST has now standardized these algorithms. The standard forms of Crystals-Dilithium and Crystals-Kyber are:

- Module Lattice – Digital Signature Algorithm (ML-DSA) defined by FIPS-204 (https://csrc.nist.gov/pubs/fips/204/final) and
- Module Lattice – Key Encapsulation Mechanism (ML-KEM) defined by FIPS-203 (https://csrc.nist.gov/pubs/fips/203/final) respectively.

The Crypto Express8 HSM is adding support for these standardized algorithms. ICSF is adding API support and management features which allow customers to leverage the hardware support.

Note: PQC is the industry term. Quantum-safe is IBM's term. This presentation uses the term Quantum-safe from hereon.

Overview

- Who (Audience)
  - Application Programmers, Security Architects
- What (Solution)
  - Standardized Quantum-safe algorithms
- Wow (Benefit / Value, Need Addressed)
  - Protect data from threats posed by a cryptographically relevant quantum computer (CRQC) i.e. a large-scale quantum computer
  - Interoperability with other systems implementing quantum-safe algorithms

Usage & Invocation

ML-DSA, ML-KEM keys can be created just like any other PKA key using the CSNDPKB, CSNDPKG, CSNDPKI services. They may also be created using the PKA Key Generation Panel (CSFPKY22).

The ML-DSA algorithm is used to calculate digital signatures using the following services:

- CSNDDSG – Generate a standardized, quantum-safe digital signature
- CSNDDSV – Verify a standardized, quantum-safe digital signature

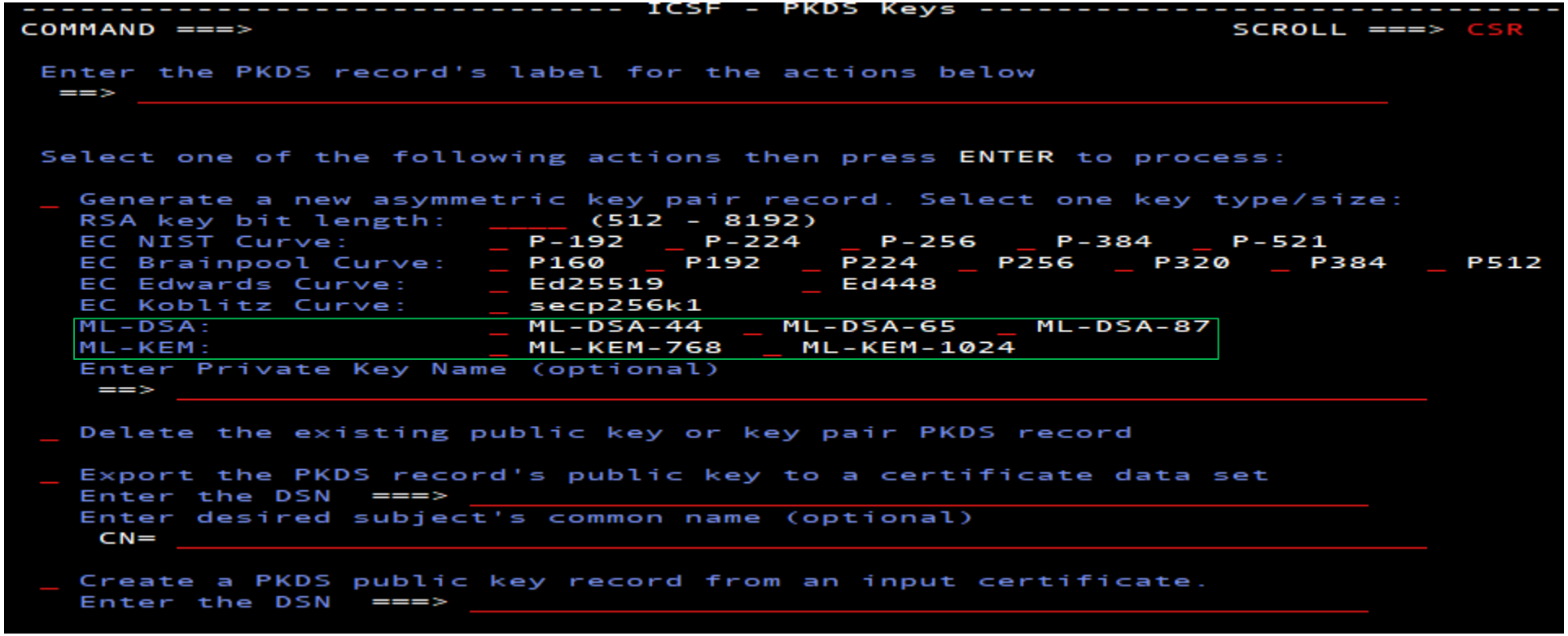
The ML-KEM algorithm is used to encapsulate/decapsulate a random value using the following services:

- CSNDPKE – Generate and encapsulate (analogous to an encrypt) a random number under a public key. The encapsulated random number can then be sent to the party holding the private key (party B).
- CSNDPKD – Decapsulate (analogous to a decrypt) an encapsulated value using the private key to obtain the clear value. This function is used by party B mentioned above.

The combination of these services allows two parties to establish a shared secret which can then be used to create a secure communication channel.

All general key management services and capabilities will support the new algorithms.

PKA Key Generation Panel (CSFPKY22)



Interactions & Dependencies

- Software Dependencies
  - N/A
- Hardware Dependencies
  - N/A
- Exploiters
  - N/A
- Exploitation: Crypto Express8 HSM or later with version CCA 8.3 or later is required to exploit the capability

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: OA66396
- List anything that doesn't work the same anymore: N/A

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 adding API and key management support for the Quantum-safe ML-DSA and ML-KEM algorithms.

Appendix

- ML-DSA: Module Lattice – Digital Signature Algorithm
  - Standards document: https://csrc.nist.gov/pubs/fips/204/final
- ML-KEM: Module Lattice – Key Encapsulation Mechanism
  - Standards document: https://csrc.nist.gov/pubs/fips/203/final
- Publications
  - z/OS Cryptographic Services ICSF Overview
  - z/OS Cryptographic Services ICSF Application Programmers Guide
  - z/OS Cryptographic Services ICSF Administrators Guide
  - z/OS Cryptographic Services ICSF System Programmers Guide