Crypto Agility

Transition to post-quantum safe algorithms for secure key exchange and certificate generation

Graduate

Petra Heeb

Lara Gubler

Christopher Hilfing

Advisor
Prof. Dr. Mitra Purandare

Co-Examiner
Dr. Bernhard Tellenbach, Cyber-Defence Campus, Zürich, ZH

Subject Area
Security

Project Partner
IBM Research Europe, Zürich, ZH

Introduction: The quantum era is arriving, which poses a significant threat to traditional encryption and public-key cryptography standards.
Quantum computing breaks many cryptographic algorithms as the underlying mathematical problems could be solved by quantum computers within a short time. With the arrival of quantum computers, cryptographic algorithms have also evolved. New quantum-safe algorithms have been recently standardised, but only a few applications already use them. To ensure a secure environment this will need to change.
Faced with these challenges and the rapid improvements in the area of quantum computing, the global cybersecurity landscape plunges into a highly precarious state.

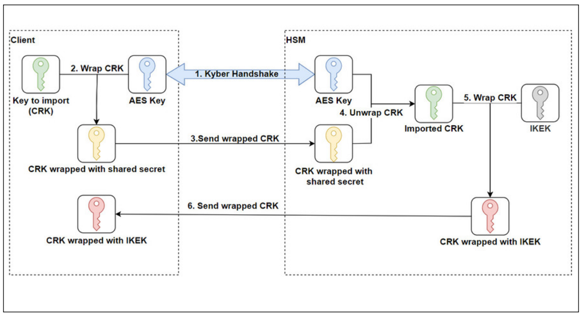
Approach: This bachelor thesis aims to demonstrate how two recently standardized post-quantum secure algorithms can be used by testing their compatibility with a Hardware Security Module (HSM) in a controlled environment. To demonstrate how these could be implemented in a quantum-safe manner at a later stage, two different use cases will be realized. The used quantum-resistant algorithms CRYSTALS-Kyber and CRYSTALS-Dilithium are based on the module lattices problem.

First, two Proof of Concepts (PoCs) were implemented, that demonstrate the compatibility between the HSM and the two CRYSTALS algorithms. The use case: Bring Your Own Key (BYOK) demonstrates how locally generated keys can be imported into the HSM in a quantum-safe manner. In this demonstration, the Key Encapsulation Mechanism (KEM) CRYSTALS-Kyber is used to generate a shared secret so that the client application can communicate to the HSM using Advanced Encryption Standard (AES).
The second use case focuses on a Public Key Infrastructure (PKI) based on a post-quantum secure infrastructure. The HSM is used as a key store to secure the identity of the Root Certificate Authority (CA), which acts as the root of trust. This ensures that keys are never exposed in clear text in memory. Furthermore, the quantum-safe signature scheme CRYSTALS-Dilithium is used to sign certificates which further increases security.

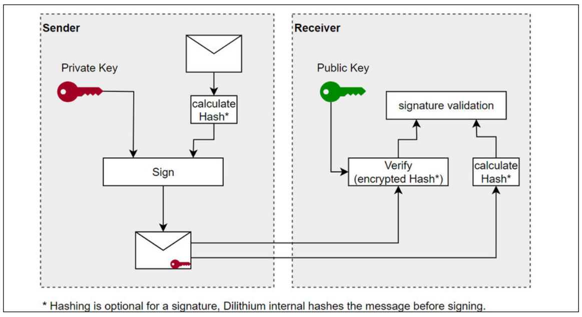
Result: The outcomes of this research provide valuable insights into the implementation of quantum-safe algorithms in practical high security scenarios. In addition, the implementations facilitate the replication of a similar use case for an enterprise architecture and the transition from today's legacy algorithms to the new secure post-quantum algorithms with increased efficiency.

Both the BYOK and PKI implementations could also be extended to provide more functionality, and higher security standards based on the algorithm versions or protocol used. The PKI implementation could also be further improved by using a quantum-safe variant of Transfer Layer Security (TLS).

Bring Your Own Key (BYOK) Vision (simplified)
Own presentment

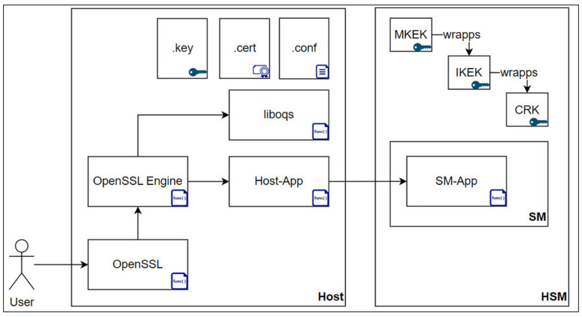


Signature Process
Own presentment



* Hashing is optional for a signature, Dilithium internal hashes the message before signing.

Public Key Infrastructure (PKI) Vision
Own presentment


.key
.cert
.conf
liboqs
OpenSSL Engine
Host-App
OpenSSL
User
Host
MKEK
wrapps
IKEK
wrapps
CRK
SM-App
SM
HSM