KubeCon | CloudNativeCon

North America 2024

Running Quantum-Safe Applications on Kubernetes

Paul Schweigert & Michael (Max)imilien, IBM

psschwei.com @maximilien

Agenda

1. Understand the Risk

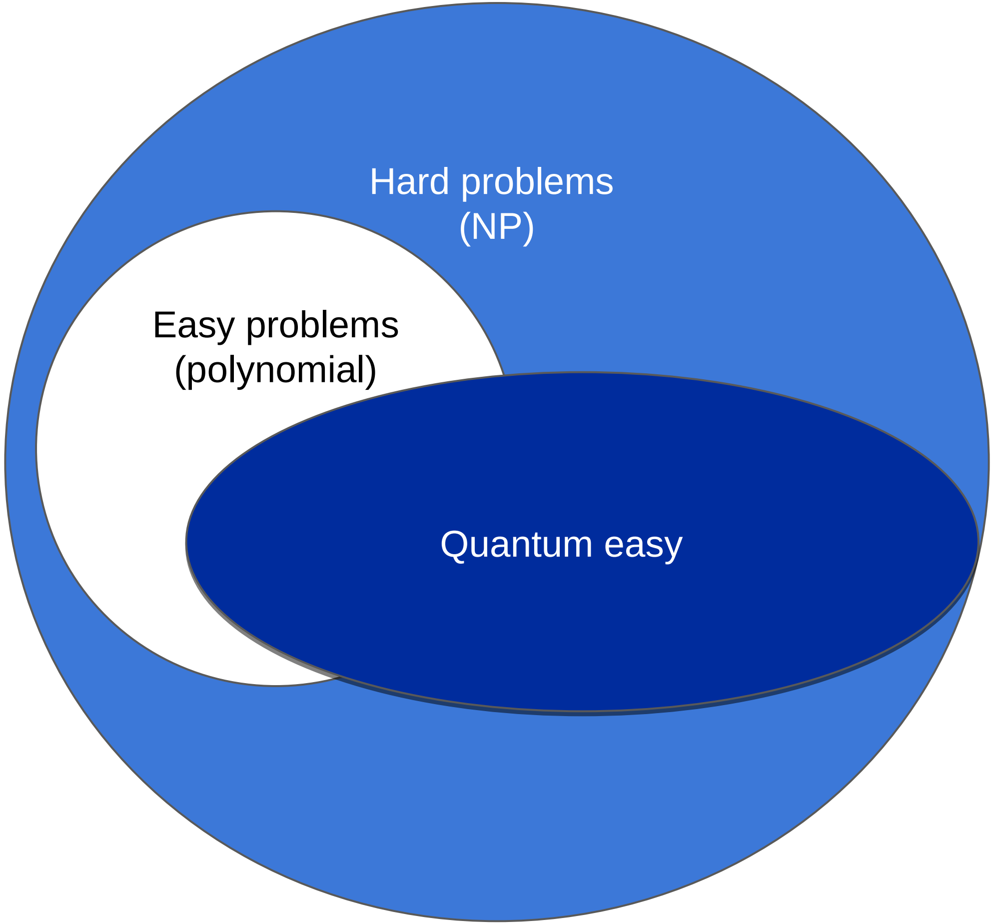
2. Becoming Quantum Safe

3. Protecting Applications

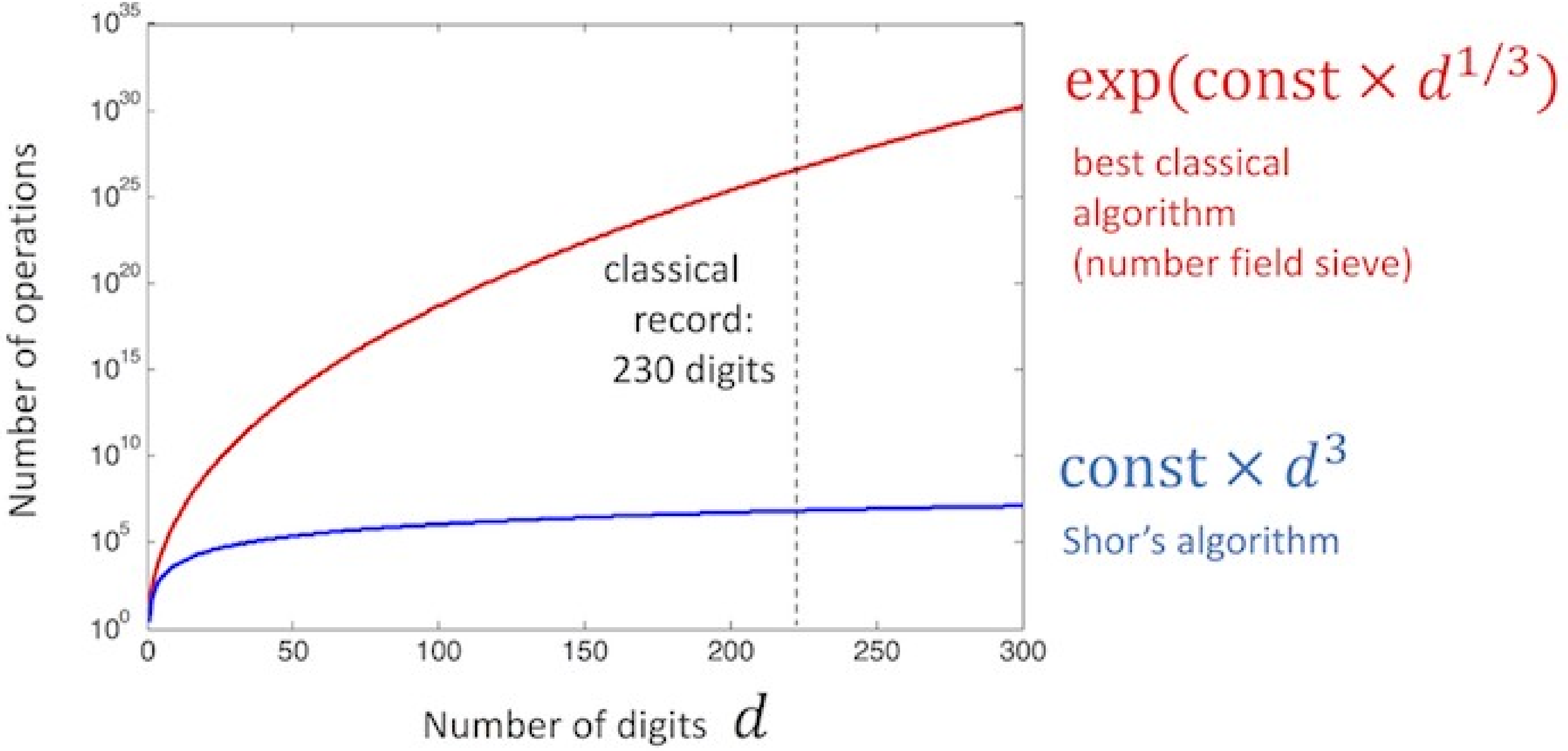
4. Next Steps

1. Understand the Risk
2. Becoming Quantum Safe
3. Protecting Applications
4. Next Steps

Why quantum?



Ex: Shor's algorithm for factoring



Current cryptography is at risk

Prime factors

$= p \times q$

2048-bit composite integer

```
25195908475657893494027183240048398571429282126204032027777137836043662020707595556264018525880784406918290641249515082189298559149176184502808489120072844992687392807287776735971418347270261896375014971824691165077613379859095700097330459748808428401797429100642458691817195118746121515172654632282216869987549182422433637259085141865462043576798423387184774447920739934236584823824281198163815010674810451660377306056201619676256133844143603833904414952634432190114657544454178424020924616515723350778707749817125772467962926386356373289912154831438167899885040445364023527381951378636564391212010397122822120720357
```

Expected computation time

The most powerful computer **today:**

Millions of years

Shor’s quantum algorithm:

Hours

Per Shor’s algorithm, all public key crypto standards are vulnerable to attacks from large scale quantum computers

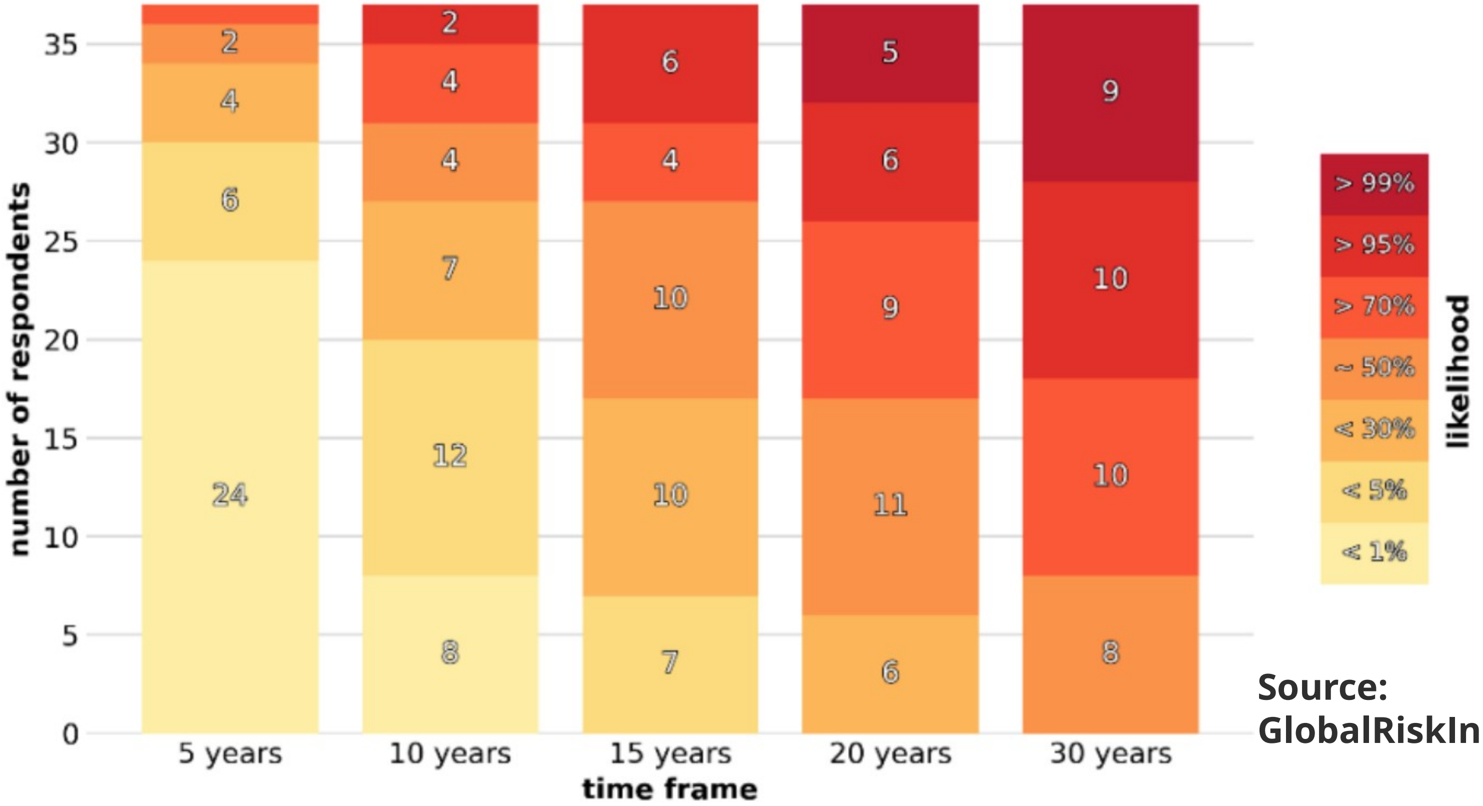
Public Key Encryption	RSA
Digital Signatures	DSA, ECDSA
Key Exchange Algorithms	Diffie-Hellman, ECDH

What will a cybercriminal be able to do?

- Fraudulent authentication
- Forge digital signatures
- Harvest now, decrypt later

2023 EXPERTS' ESTIMATES OF LIKELIHOOD OF A QUANTUM COMPUTER ABLE TO BREAK RSA-2048 IN 24 HOURS

Number of experts who indicated a certain likelihood in each indicated timeframe



Source:
GlobalRiskInsitute.org

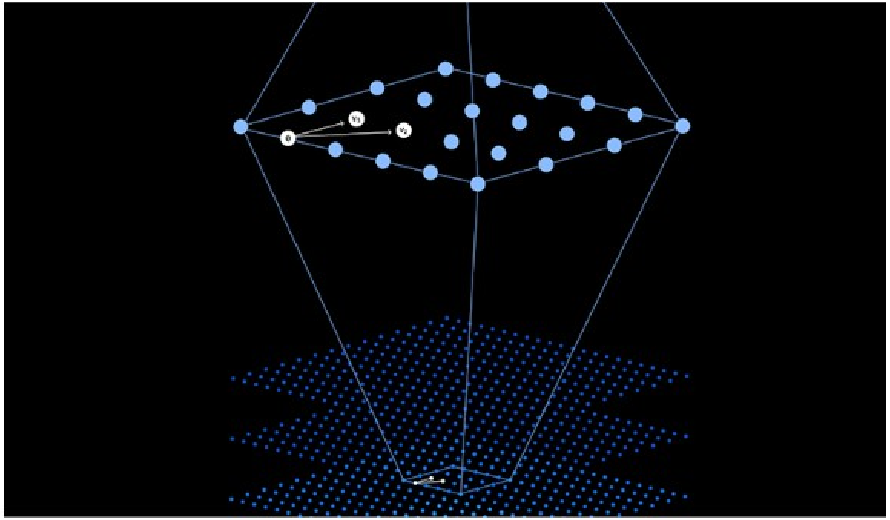
1. Understand the Risk
2. Becoming Quantum Safe
3. Protecting Applications
4. Next Steps

Quantum Safe Cryptography

a.k.a. Post Quantum Cryptography or Quantum Resistant Cryptography

Traditional public-key cryptography relies upon mathematical problems that are difficult to solve on classical computers.

Quantum-safe cryptography includes **a suite of algorithms and systems that are resistant to attacks by both classical and quantum computers.**



Post-Quantum Cryptography PQC

Overview

Short URL: https://www.nist.gov/pqcrypto

FIPS 203, FIPS 204 and FIPS 205, which specify algorithms derived from CRYSTALS-Dilithium, CRYSTALS-KYBER and SPHINCS+, were published August 13, 2024.

4th Round KEMs

Additional Digital Signature Schemes - Round 1 Submissions

PQC License Summary & Excerpts

For a plain-language introduction to post-quantum cryptography, go to: What Is Post-Quantum Cryptography?

Background

NIST initiated a process to solicit, evaluate, and standardize one or more quantum-resistant public-key cryptographic algorithms. **Full details can be found in the Post-Quantum Cryptography Standardization page.**

In recent years, there has been a substantial amount of research on quantum computers – machines that exploit quantum mechanical phenomena to solve mathematical problems that are difficult or intractable for conventional computers. If large-scale quantum computers are ever built, they will be able to break many of the public-key cryptosystems currently in use. This would seriously compromise the confidentiality and integrity of digital communications on the Internet and elsewhere. The goal of *post-*

PROJECT LINKS
Overview
FAQs
News & Updates
Events
Publications
Presentations
ADDITIONAL PAGES
Post-Quantum Cryptography Standardization
Call for Proposals
Example Files
Round 1 Submissions
Round 2 Submissions
Round 3 Submissions
Round 3 Seminars
Round 4 Submissions
Selected Algorithms 2022
Workshops and Timeline
PQC Seminars

Open Source

Post-Quantum Cryptography Alliance

https://pqca.org

To advance the adoption of post-quantum cryptography, by producing high-assurance software implementations of standardized algorithms, and supporting the continued development and standardization of new post-quantum algorithms with software for evaluation and prototyping.

Initial Projects Overview

Open Quantum Safe project

liboqs

Library of many PQ algorithms

- Main profile: standards-track algorithms
- Experimental profile: new algorithms, NIST signatures on-ramp etc.

OQS demos

Prototype integrations of PQ into protocols and applications to support experiments, standardization, interoperability

OQS OpenSSL 3 Provider

Integration of PQ + hybrid algorithms from liboqs into OpenSSL 3 via OpenSSL provider interface

- TLS key exchange, authentication
- X.509
- S/MIME, CMS, CMP

PQ Code Package

“Kyber” code package

High-assurance production source-code implementations of Kyber

- C, x86_64, ARMv8, …
- Rust, Go, …
- audited/certified/formally verified

Plus appropriate wrappers / providers, e.g. Kyber OpenSSL 3 provider

Potential Phase 2 projects

- Dilithium
- XMSS, LMS
- SPHINCS+
- Falcon (-> Phase 3?)

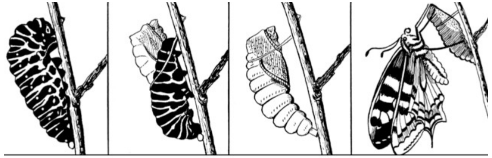
Production track: safe for use in production environments, with external audits or certification

Experimental track: primarily for prototyping and experiments, mindful of potential production use

Becoming Quantum Safe

<u>Discover</u>: Scan source and object code to locate cryptographic assets, dependencies, and vulnerabilities. Build a cryptography bill of materials (CBOM).

<u>Observe</u>: Create a dynamic cryptographic inventory to guide remediation. Analyze cryptographic posture and compliance to prioritize risks.



<u>Transform</u>: Learn and apply quantum-safe remediation patterns in a development environment. Prepare to deploy quantum-safe solutions to your stack.

1. Understand the Risk

2. Becoming Quantum Safe

3. Protecting Applications

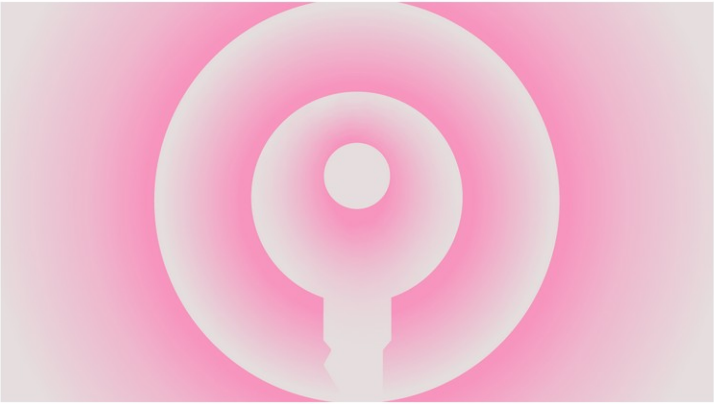
4. Next Steps

IBM Quantum Technology Qiskit Research Pricing Blog Community Resources Sign in to Platform

Quantum Research
↳ Blog

Bringing quantum-safe security to IBM Quantum Platform, and the world

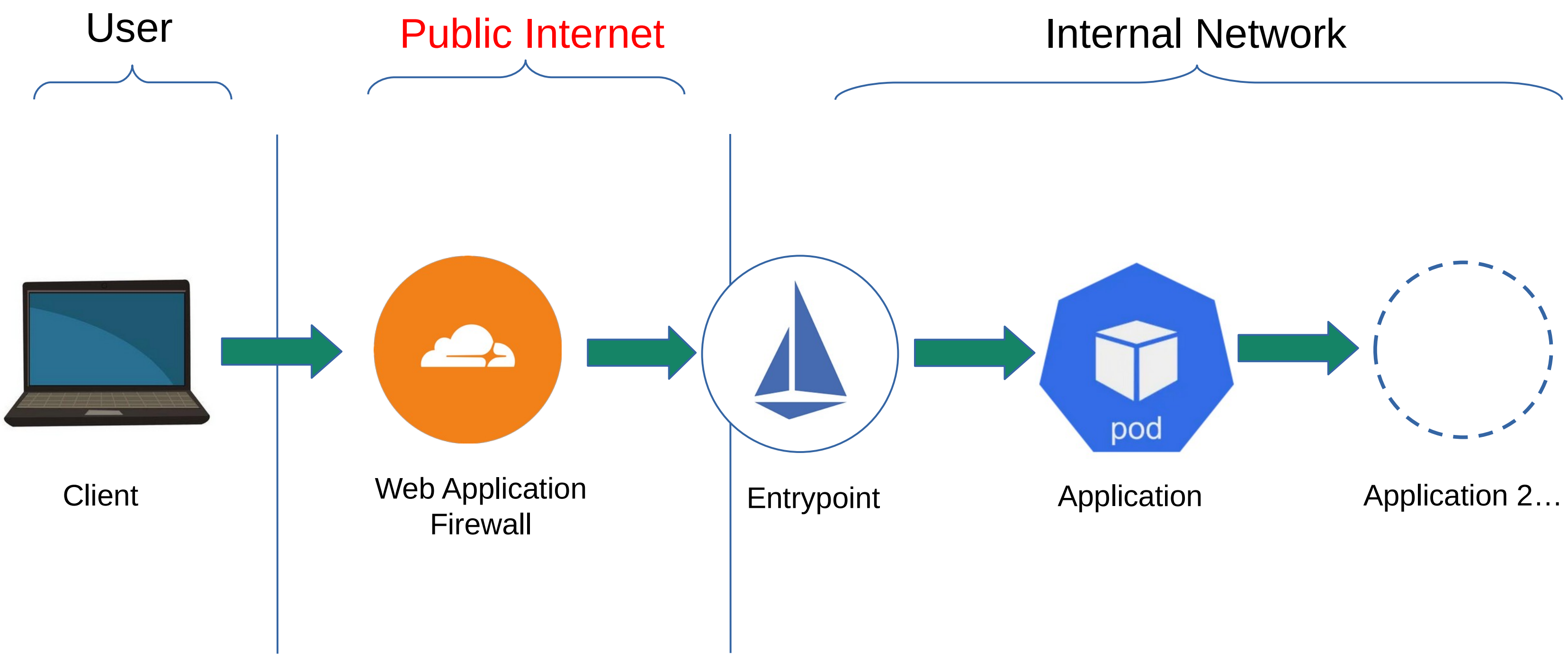
How IBM® is working to make itself, the open source community, and the world quantum safe.



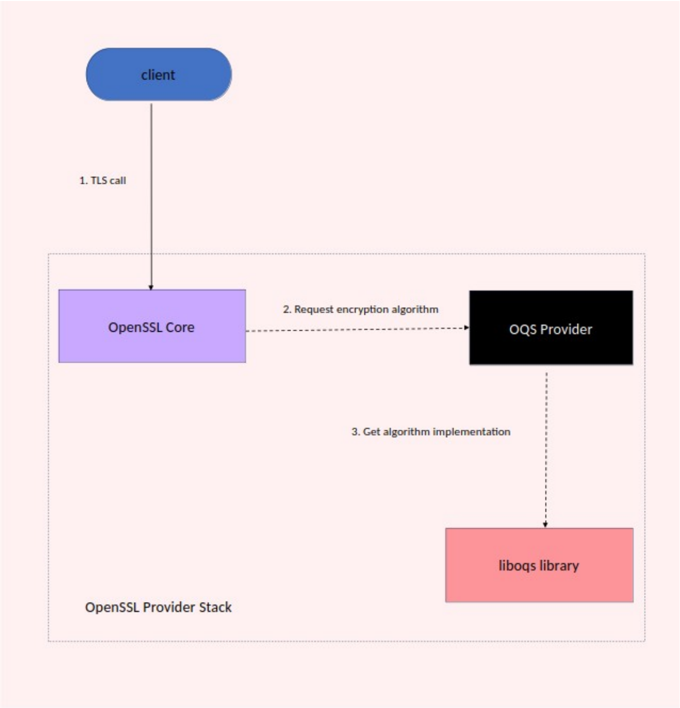
https://www.ibm.com/quantum/blog/iqp-quantum-safe

Quantum Safe Flow

High Level View



Quantum Safe Client: Configuring OpenSSL

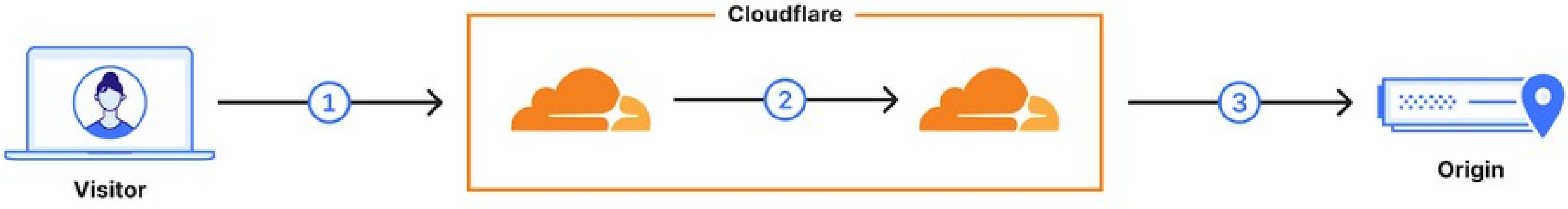


- Install liboqs & oqs-provider
  - https://github.com/open-quantum-safe/liboqs
  - https://github.com/open-quantum-safe/oqs-provider

- Configure OpenSSL to use Kyber algorithm

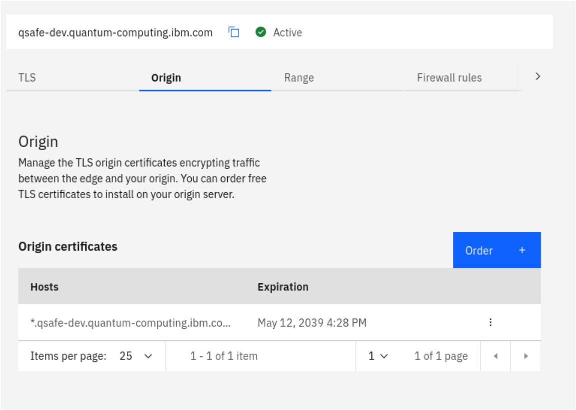
```

[oqsprovider_sect]
activate = 1
module = /opt/conda/lib/ossl-modules/oqsprovider.so

[ ssl_module ]
system_default = tls_system_default

[ tls_system_default ]
TLS.MinProtocol = TLSv1.2
TLS.MaxProtocol = TLSv1.3
DTLS.MinProtocol = DTLSv1.2
DTLS.MaxProtocol = DTLSv1.2
Groups = x25519_kyber768
Ciphersuites = TLS_AES_256_GCM_SHA384:TLS_CHACHA20_POL
CipherString = ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-RSA

#######################################################
[ ca ]
```

Quantum Safe Firewall:
Enabling PQC in Web Application Firewall

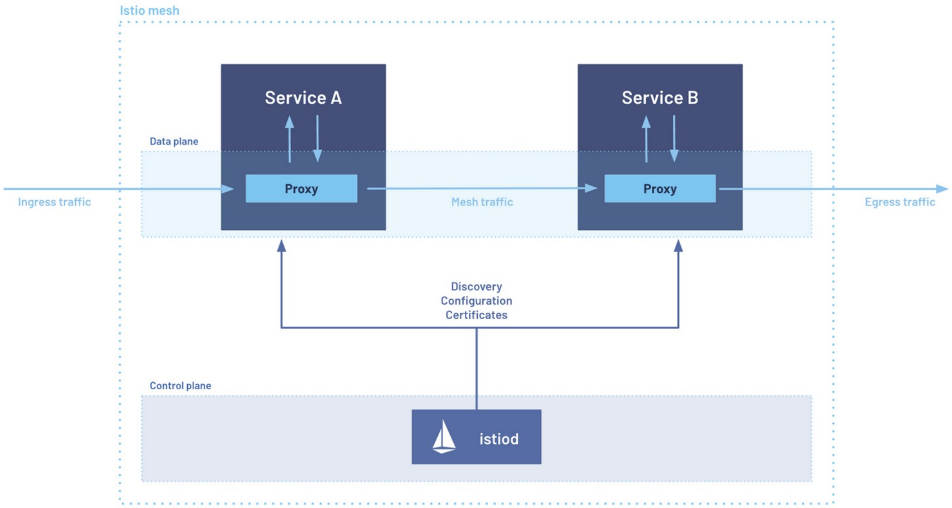


- Enable PQ encryption on IBM Cloud Internet Services
  - https://cloud.ibm.com/apidocs/cis?code=go#update-origin-post-quantum-encryption

- Create new origin cert for Ingress / VirtualService



Quantum Safe Service Mesh: Updating Istio

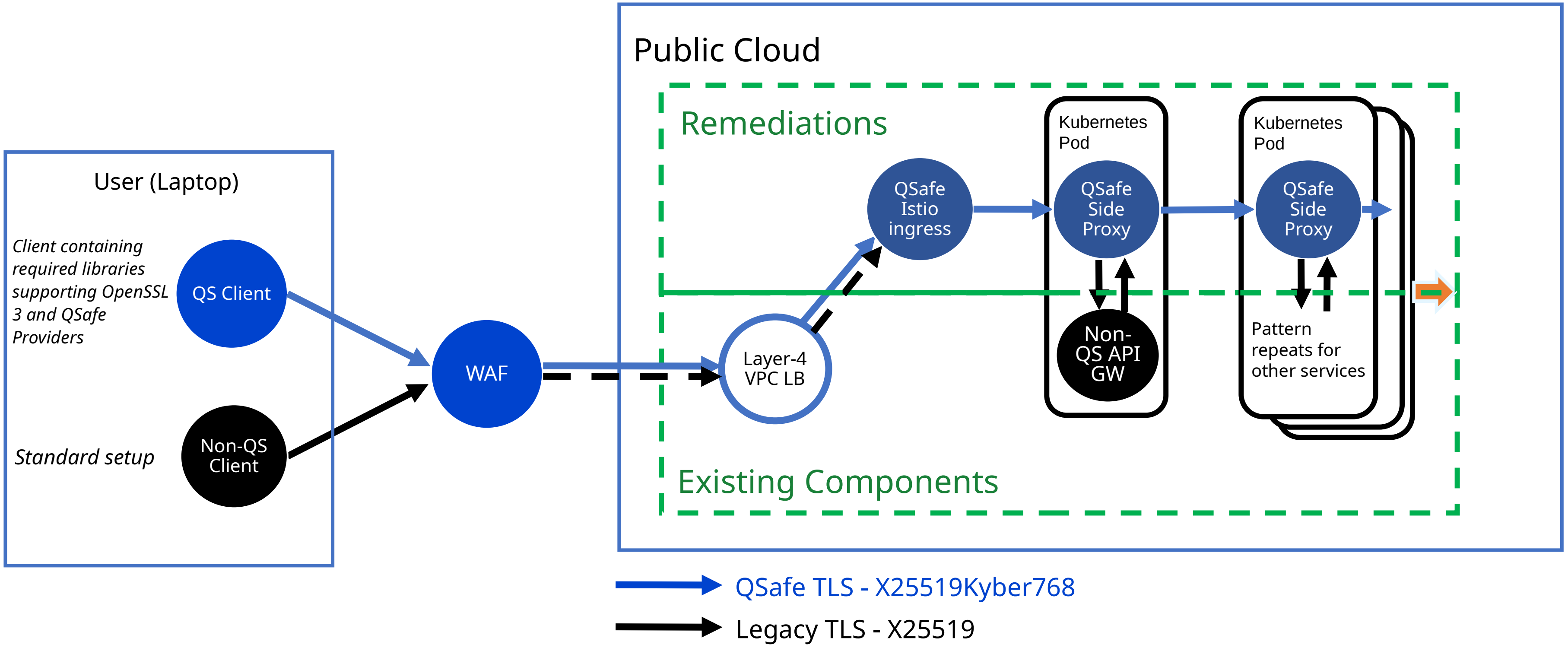


- Envoy
  - QSafe BoringSSL:

    https://github.com/google/boringssl/blob/45cf810dbdbd767f09f8cb0b0fcccd342c39041f/src/ssl/ssl_key_share.cc#L285-L293
- Istio
  - Add QSafe supported group: https://github.com/istio/istio/commit/7635f7ea50514958518eb17b631682f953e723cc
  - Secure mesh traffic: https://github.com/istio/istio/issues/52290

Quantum Safe Flow

Detail View

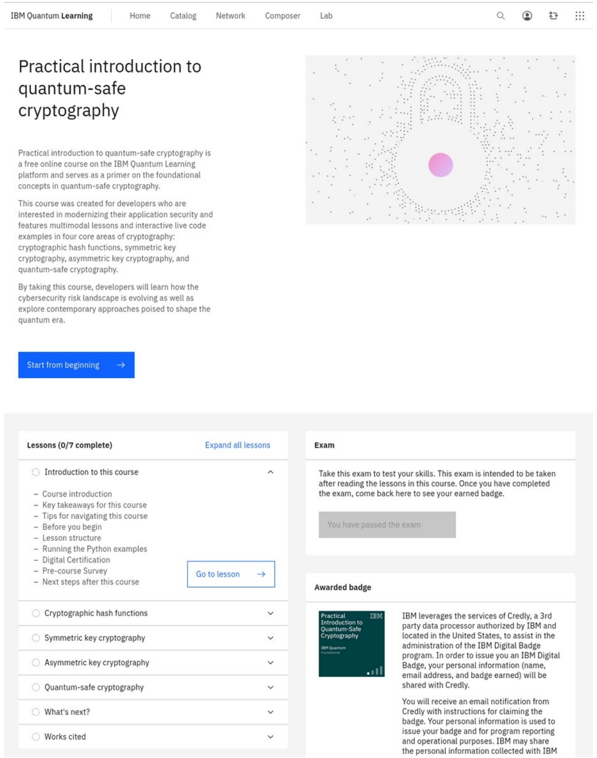


Demo

1. Understand the Risk
2. Becoming Quantum Safe
3. Protecting Applications
4. Next Steps

Next Steps

Learn about post-quantum cryptography



Start inventorying your crypto

Next Steps

Learn about post-quantum cryptography

Inventory your crypto

Rate this session

Paul Schweigert
psschwei.com
paulschw@us.ibm.com

Michael (Max)imilien
@maximilien
maxim@us.ibm.com

KubeCon | CloudNativeCon

North America 2024