How I Met Your Algorithm

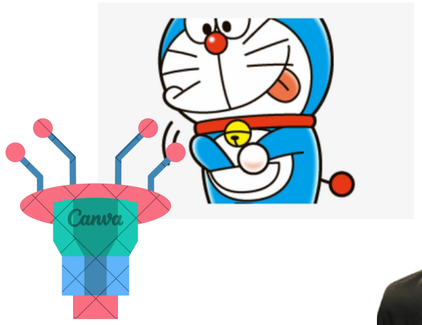
A Post Quantum Love Story

Who Am I

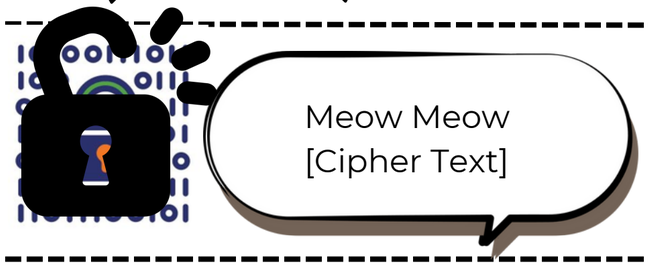

Just another soul in a random corner of the world, living in quiet fear and paying taxes.

Encrypted Meow Meow

Very Powerful Quantum Computer



Let’s use Post Quantum Cryptography



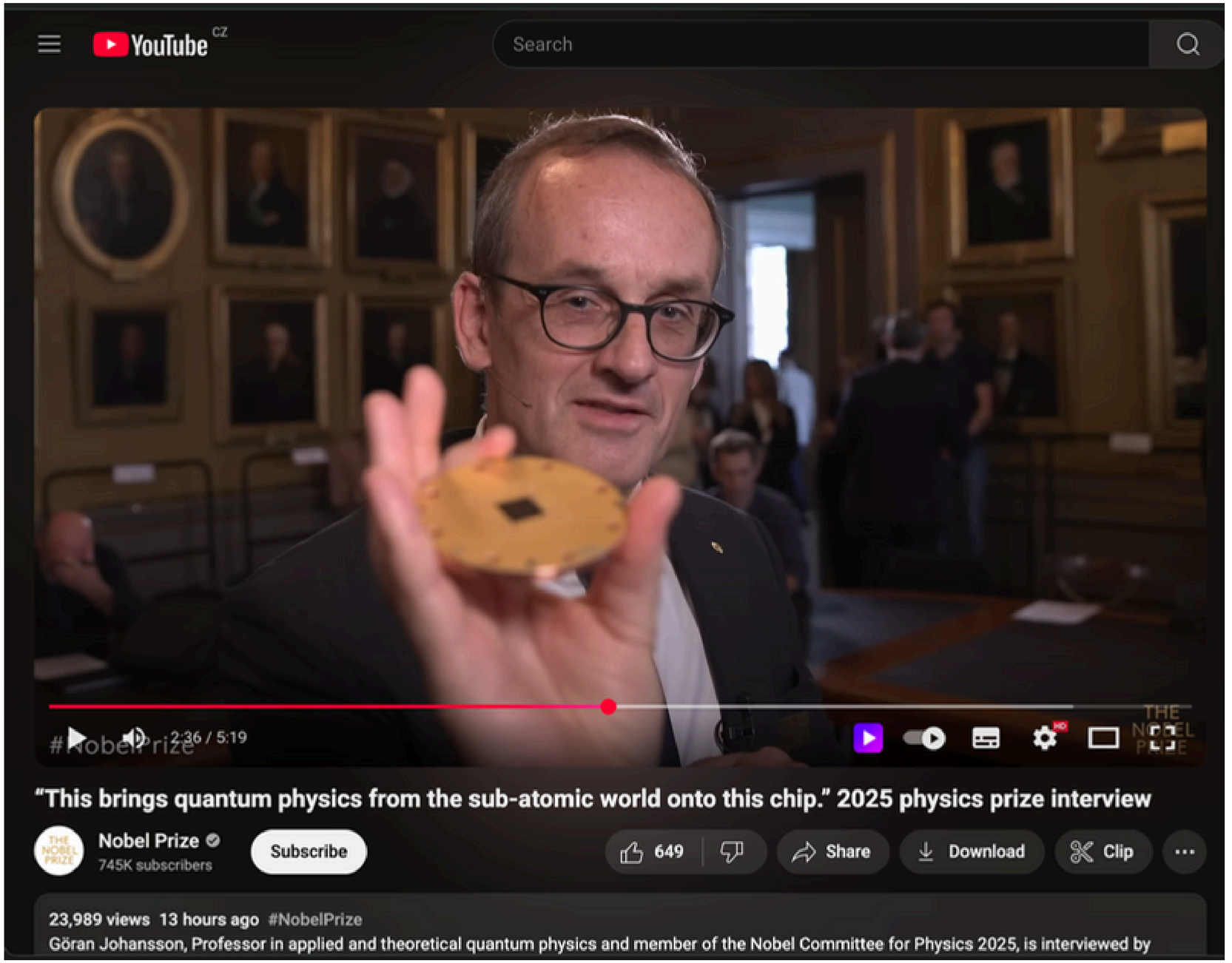
Alice (My cat)

Bob (My other cat)

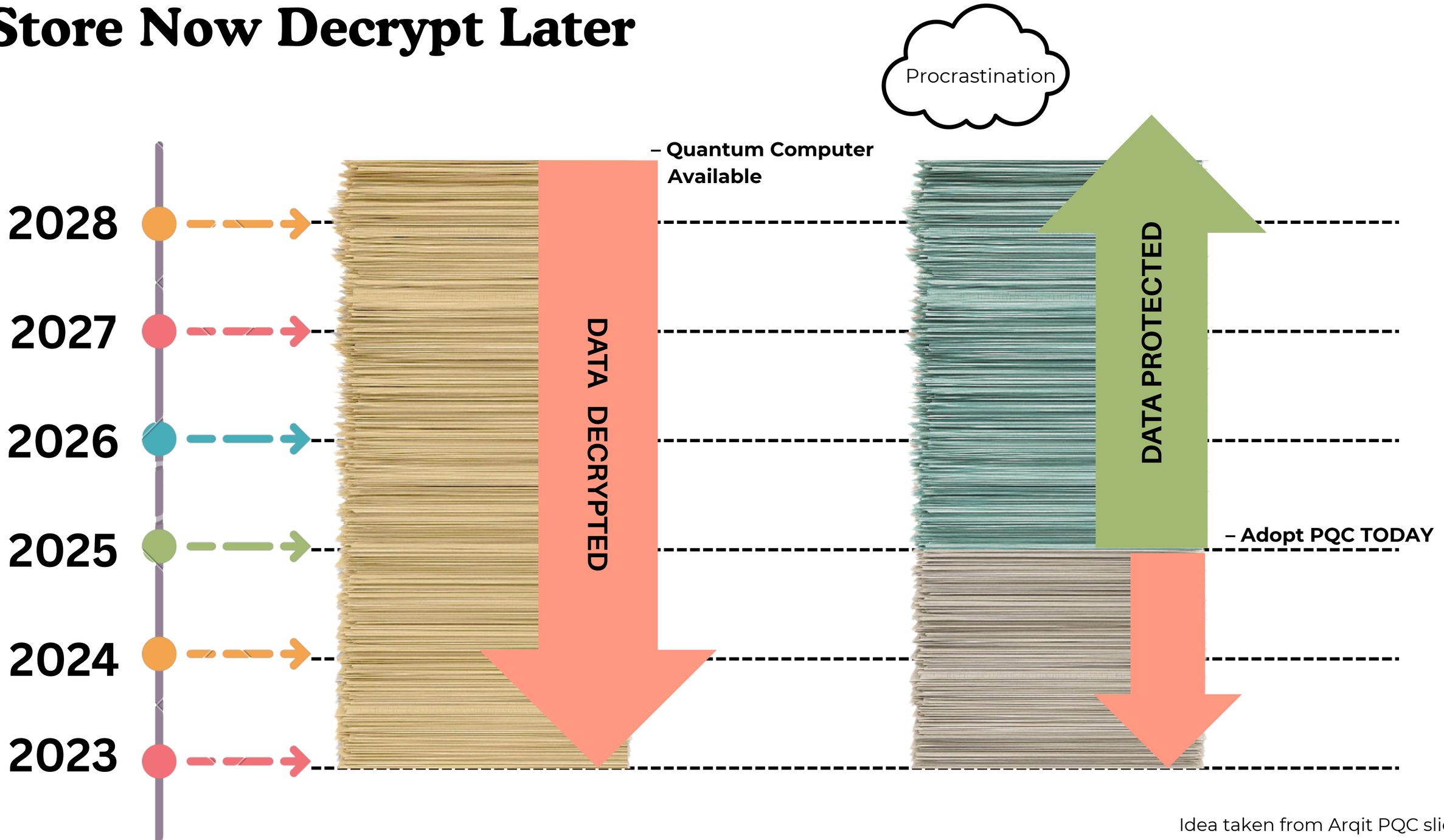
Securely communicating over the Internet using classical cryptography

PQ public key

PQ private key


YouTube CZ
Search
#NobelPrize
2:36 / 5:19
THE NOBEL PRIZE
"This brings quantum physics from the sub-atomic world onto this chip." 2025 physics prize interview
Nobel Prize
745K subscribers
Subscribe
649
Share
Download
Clip
23,989 views 13 hours ago #NobelPrize
Göran Johansson, Professor in applied and theoretical quantum physics and member of the Nobel Committee for Physics 2025, is interviewed by

Store Now Decrypt Later



Idea taken from Arqit PQC slide

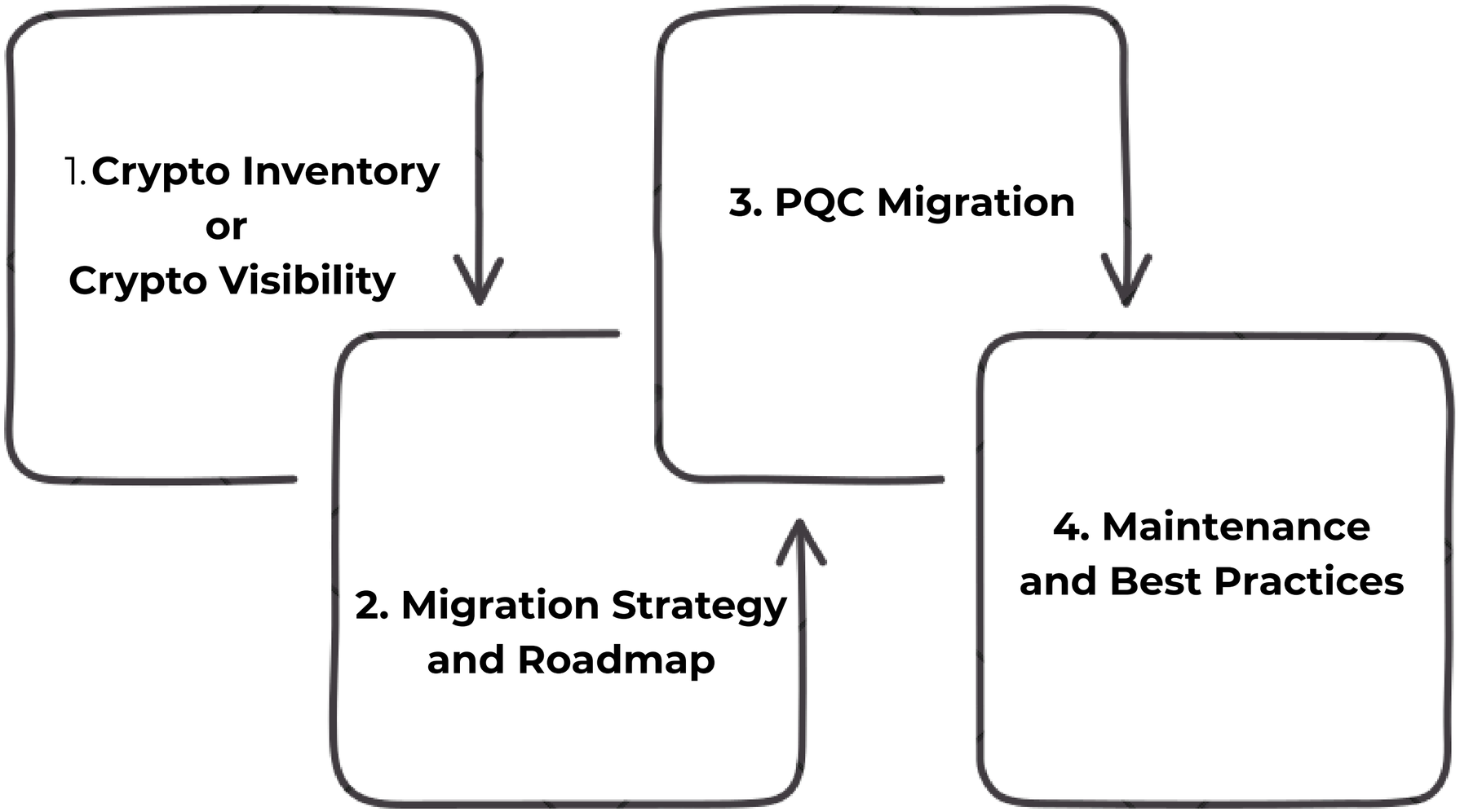
Monkey Sees Monkey Does

OpenSSL	PQClean	Tink	go crypto	pqcrystals
liboqs	wolfSSL	qrc-opensource-rs	mbedTLS	PQCrypto
PQ Code Package	Libcrux	Bouncy Castle	gnuTLS	leancrypto
CIRCL	rustls	libjade	Botan	s2n-tls
SymCrypt	AWS-LC	cuPQC	Crypto++	Sphincs+
oqs-provider	BoringSSL	NSS	pqm4	Intel Crypto Primitives

Relationship status with OpenSSL

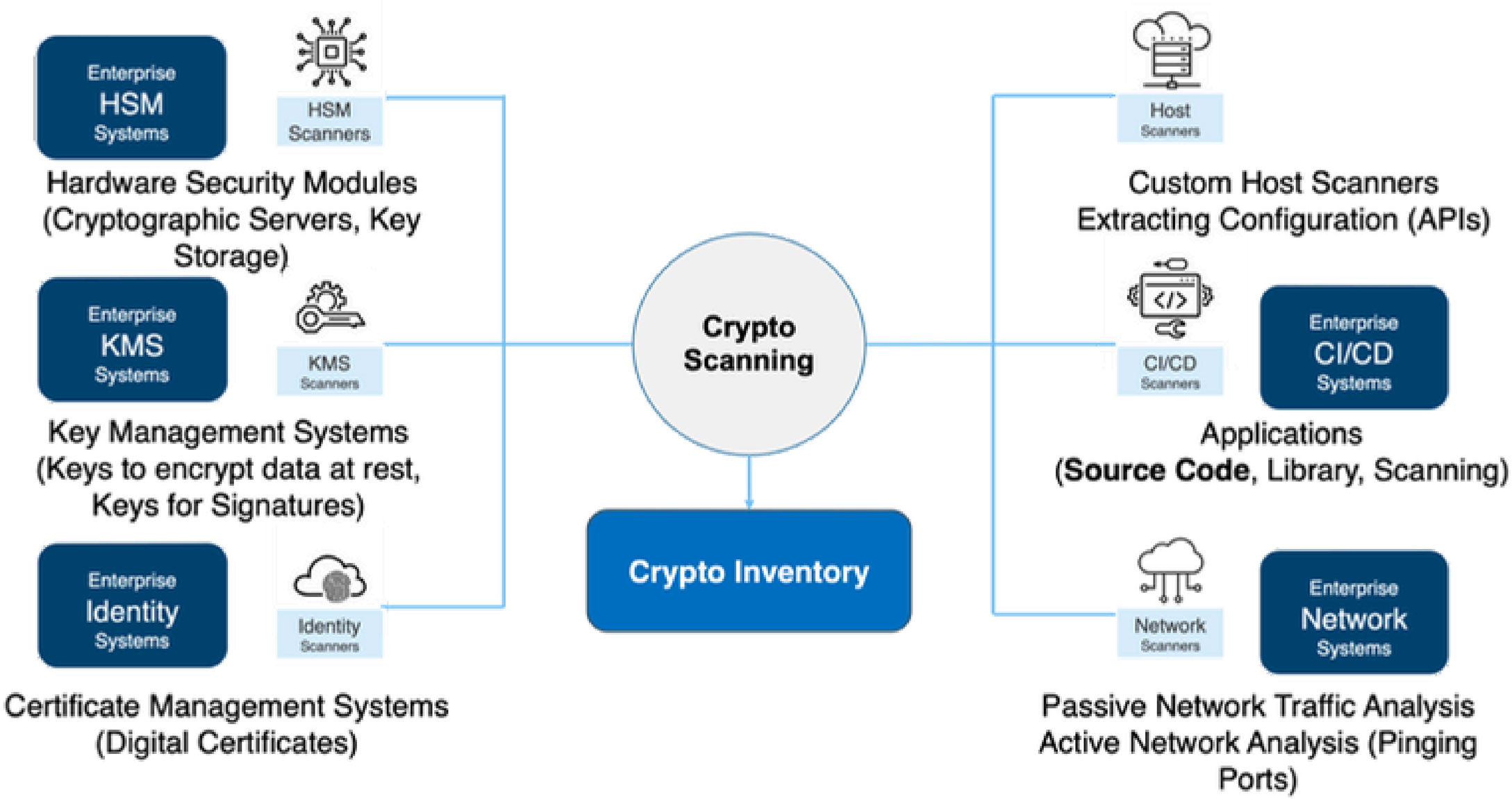
OpenSSL	PQClean	Tink	go crypto	pqcrystals
liboqs	wolfSSL	qrc-opensource-rs	mbedTLS	PQCrypto
PQ Code Package	Libcrux	Bouncy Castle	gnuTLS	leancrypto
CIRCL	rustls	libjade	Botan	s2n-tls
SymCrypt	AWS-LC	cuPQC	Crypto++	Tink
oqs-provider	BoringSSL	NSS	pqm4	Intel Crypto Primitives

It’s not a race. It’s a marathon

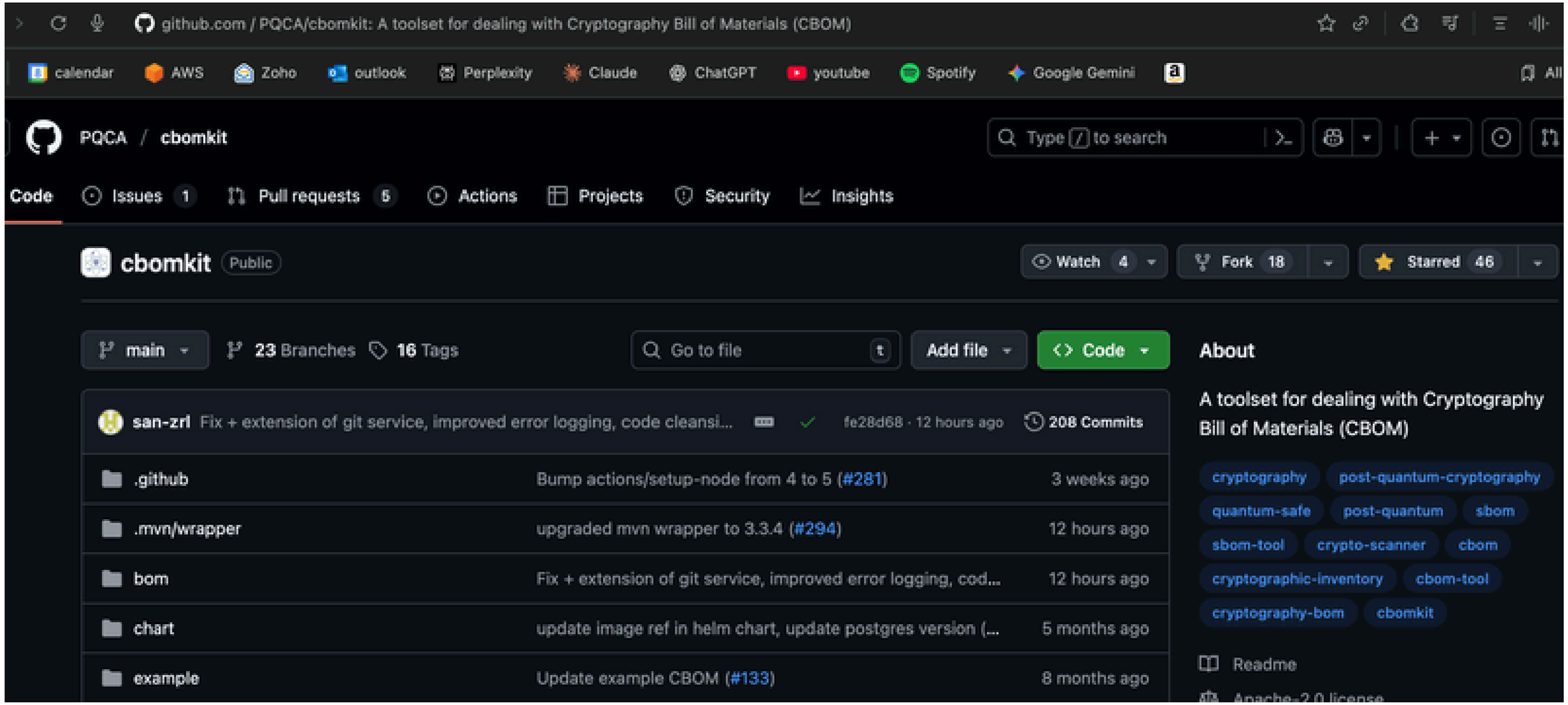



I solemnly swear that I am up to no good.

Chambers of Secrets



Chambers of Secrets: PQCA CBOMkit

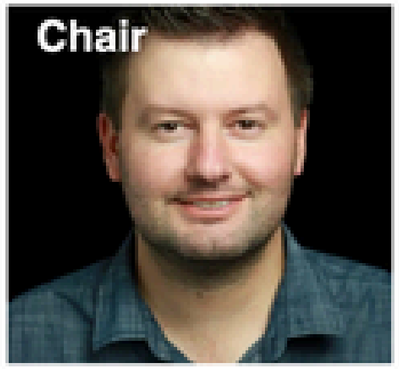


Technical Advisory Council (TAC)

Post-Quantum Cryptography Alliance

Norm Ashley
Cisco

Yarkin Doroz
NVIDIA

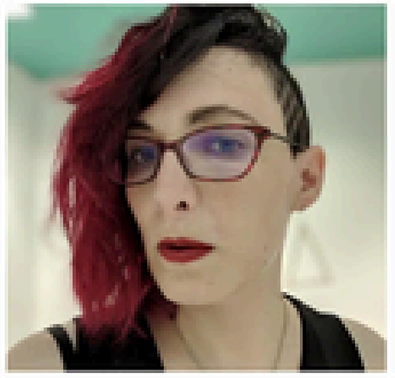


Brian Jarvis
Amazon Web Services

Matthias Kannwischer

Aditya Koranga
PQStation

Michael Maximilien
IBM



Sophie Schmieg
Google

The Technical Advisory Council (TAC) provides oversight of the Post-Quantum Cryptography Alliance technical communities. Its functions include:

- Admitting new projects
- Approving new proposals for project lifecycle changes, defining how “production ready” projects are
- Establishing community norms, workflows, or policies that are not within the scope of any single project
- Resolving technical matters that affect multiple projects
- Coordinating cross-project opportunities

Happy Adoption

AWS Security Blog

ML-KEM post-quantum TLS now supported in AWS KMS, ACM, and Secrets Manager

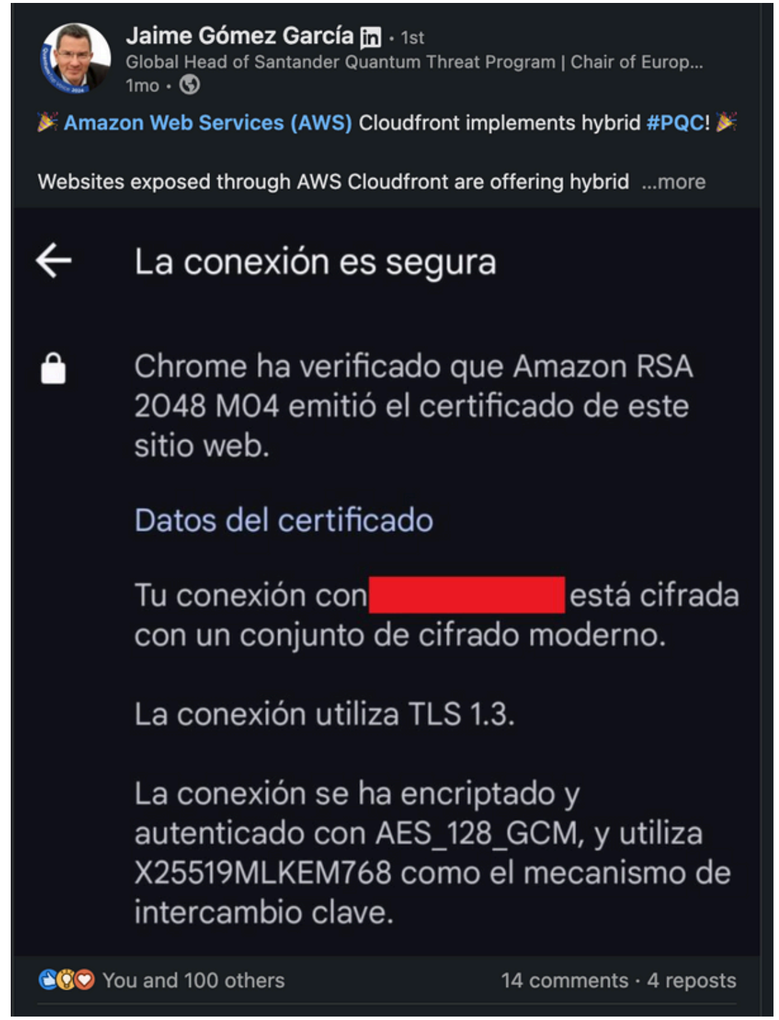
by Alex Weibel | on 07 APR 2025 | in Announcements, AWS Certificate Manager, AWS Key Management Service, AWS Secrets Manager, Intermediate (200), Security, Identity, & Compliance | Permalink | Comments | Share

Amazon Web Services (AWS) is excited to announce that the latest hybrid post-quantum key agreement standards for TLS have been deployed to three AWS services. Today, AWS Key Management Service (AWS KMS), AWS Certificate Manager (ACM), and AWS Secrets Manager endpoints now support Module-Lattice-Based Key-Encapsulation Mechanism (ML-KEM) for hybrid post-quantum key agreement in non-FIPS endpoints in all AWS Regions in the `aws` partition. The AWS Secrets Manager Agent, built on AWS SDK for Rust now also has opt-in support for hybrid post-quantum key

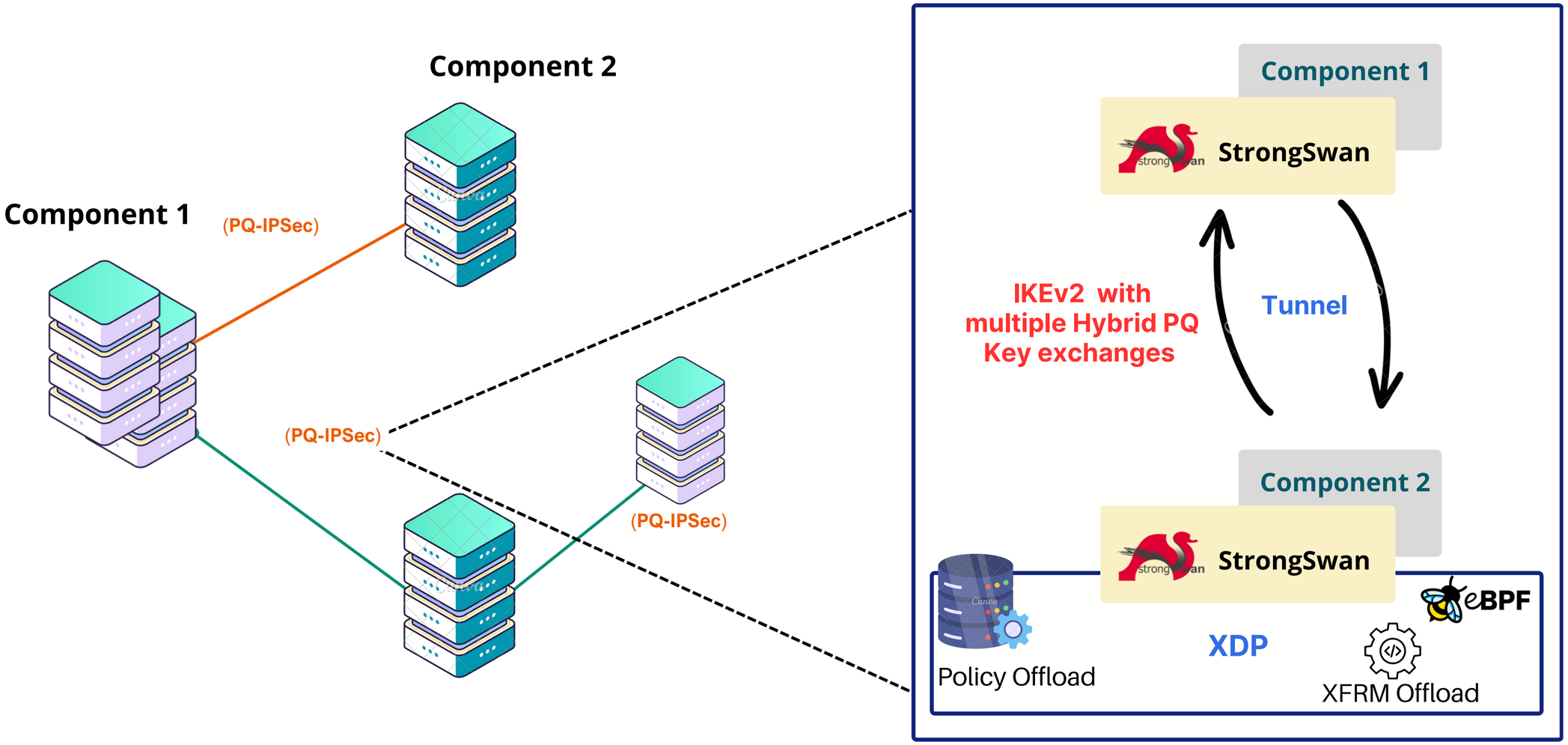
Post-Quantum Cryptography in Kubernetes

By **Fabian Kammel (ControlPlane)** | Friday, July 18, 2025

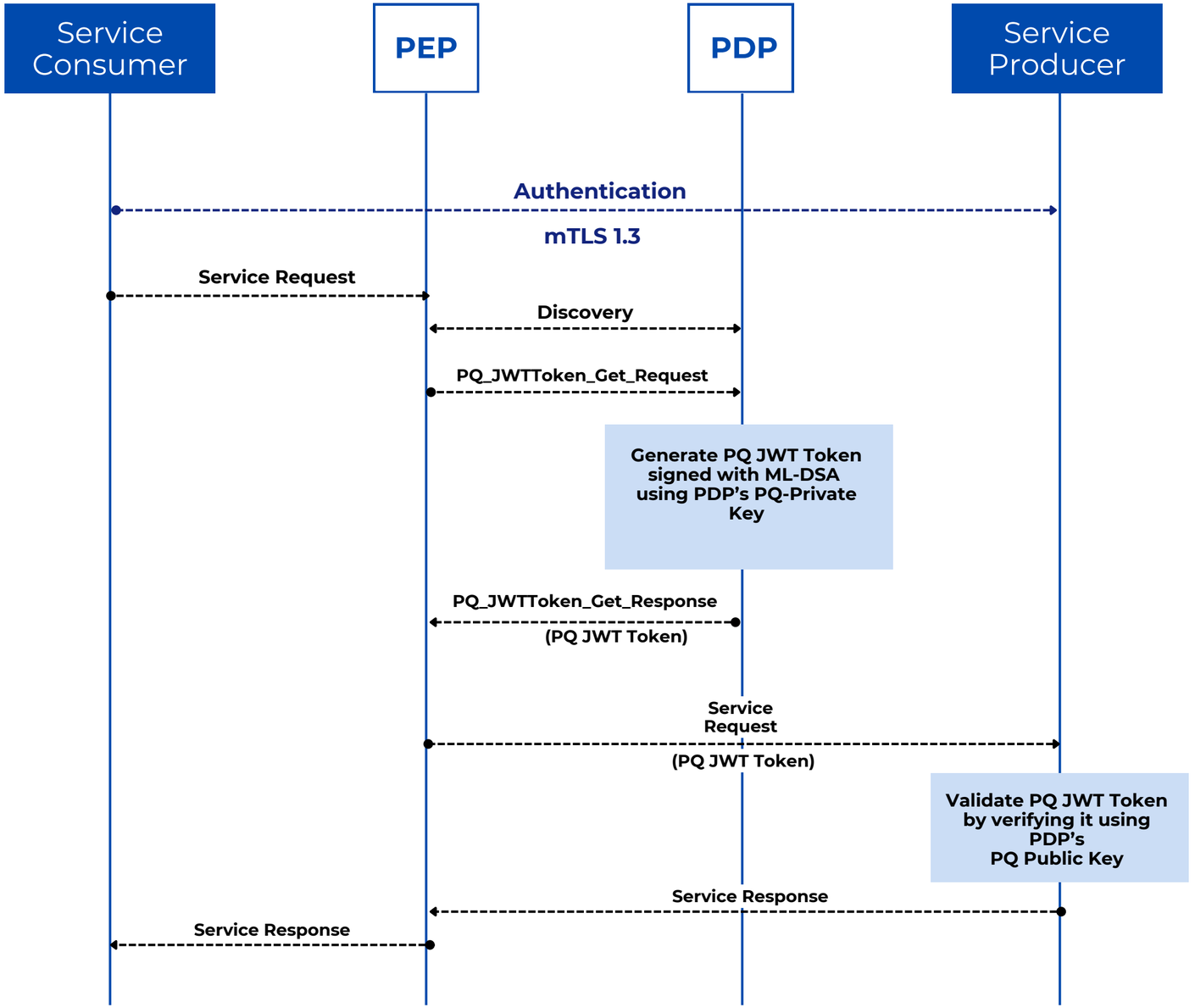
The world of cryptography is on the cusp of a major shift with the advent of quantum computing. While powerful quantum computers are still largely theoretical for many applications, their potential to break current cryptographic standards is a serious concern, especially for long-lived systems. This is where *Post-Quantum Cryptography* (PQC) comes in.



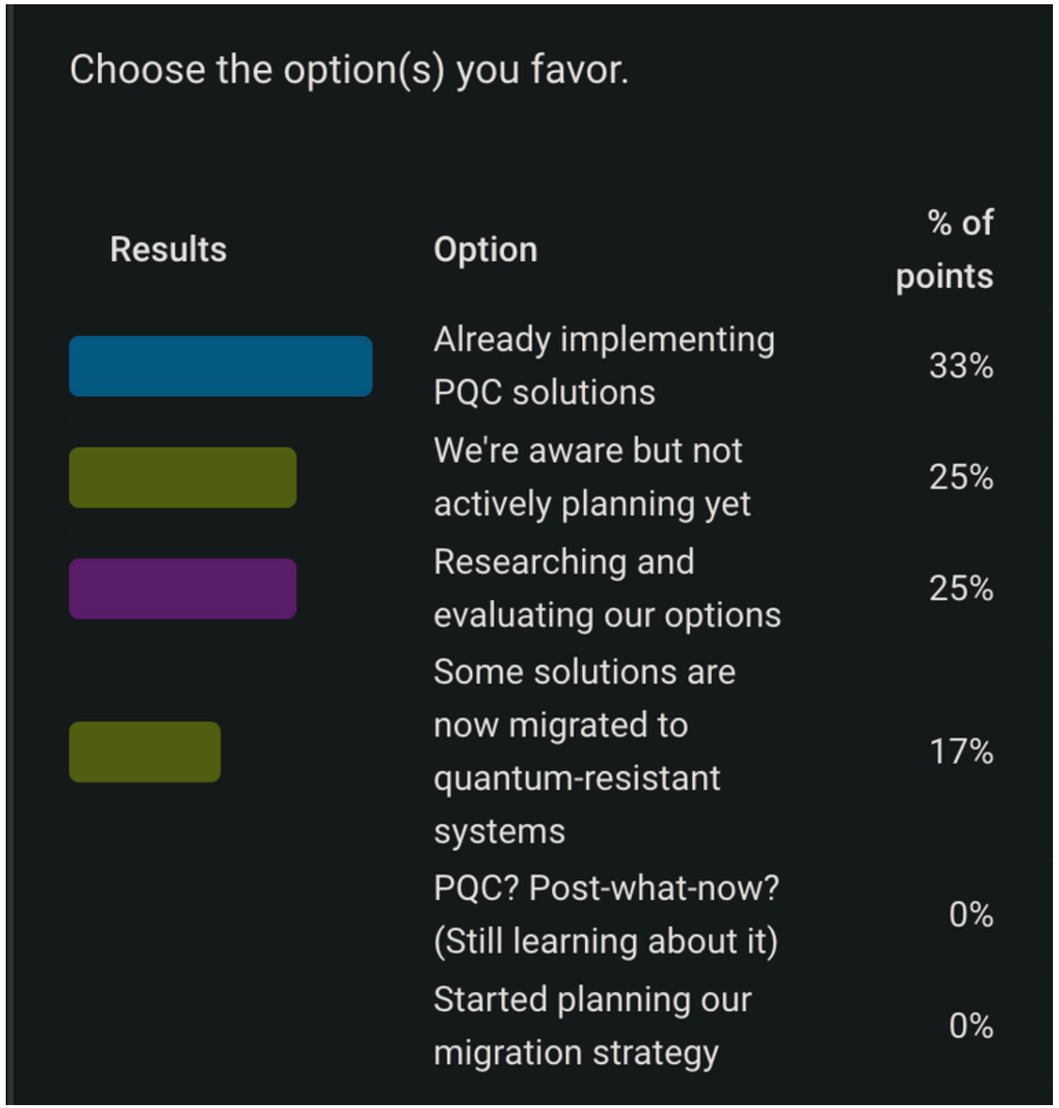
Stronger Swan



“My wife left me after reading NIST SP 800-207"



Do Small Businesses even Care?



https://openssl-communities.org/hub-businesses-small/

Post Quantamized Bye