CYBERSEC 2024
臺灣資安大會

5/14 Tue – 5/16 Thu
臺北南港展覽二館

Generative
Future

Brand Day

Practices and Challenges of Quantum-Safe Cryptography in Software Information System Development

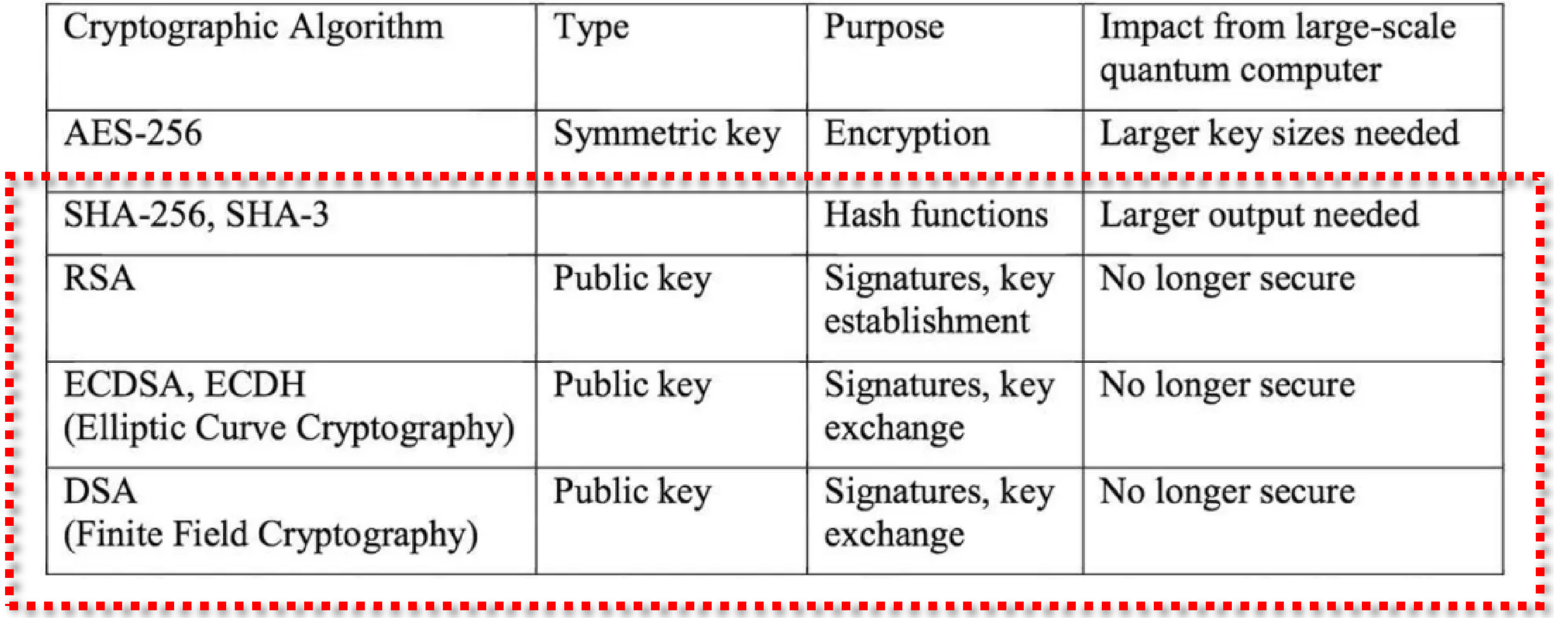
Ivan Liao

CEO of Openfind

ivan@openfind.com

Quantum Computing Threats

NIST estimates that a quantum computer breaking RSA-2048 in a matter of hours could be built by 2030 for about a billion dollars.



Cryptographic Algorithm	Type	Purpose	Impact from large-scale quantum computer
AES-256	Symmetric key	Encryption	Larger key sizes needed
SHA-256, SHA-3		Hash functions	Larger output needed
RSA	Public key	Signatures, key establishment	No longer secure
ECDSA, ECDH (Elliptic Curve Cryptography)	Public key	Signatures, key exchange	No longer secure
DSA (Finite Field Cryptography)	Public key	Signatures, key exchange	No longer secure

RSA/ECC are used in public-private key encryption/signature systems, such as: IC Cards (Credit Cards, Citizen Digital Certificates, Health Insurance Cards), Certificates (Electronic Transaction Certificates), Bitcoin, DRM, WiFi, OTA Updates, and TLS, etc.

Quantum Computing Threats

Data Confidentiality

Harvest Now & Decrypt Later (HNDL)

Attackers steal and store the data now, and decrypt the data when quantum computer matures in the near future.

Impact Industry:

Government、National Defense、BFSI、HealthCare

Impact Range：

Personal data, secret data, Email data, banking data, medical data..etc

URGENT !!

Authenticity

Identity Spoofing

Hackers exploit digital signatures used for network transmission, impersonating legitimate users or systems to gain access to data and subsequently undermine data authenticity."

Impact Industry:

Government、National Defense、BFSI、HealthCare、Payment…etc

Impact Range：

Secret data、medical data、bank transaction…etc

After 2030 !

Global Progress in PQC

- NIST began soliciting PQC algorithms in December 2016 and started the selection process
- July 2022 (Third-round) selected algorithms 2022
    - Key-Encapsulation Mechanism: CRYSTALS-Kyber
    - Digital Signature: CRYSTALS-Dilithium, FALCON, SPHINCS+
- February 2022: IBM Cloud's Key Protect service began supporting PQC
- August 2022: AWS KMS/ACM/Secrets Manager services started providing support
- August 2023: Google Chrome 116 began testing support, with official support expected in version 119
- August 2023: CloudFlare officially supported PQC across all services
- AWS announced that in 2024 it will expand support to a variety of services

Openfind Proactively Aligns with Global

CLOUDFLARE

- Oct 2022: Cloudflare Research release Post-Quantum Key Agreement
- All domains served through Cloudflare, have enabled hybrid post-quantum key agreement.

Google

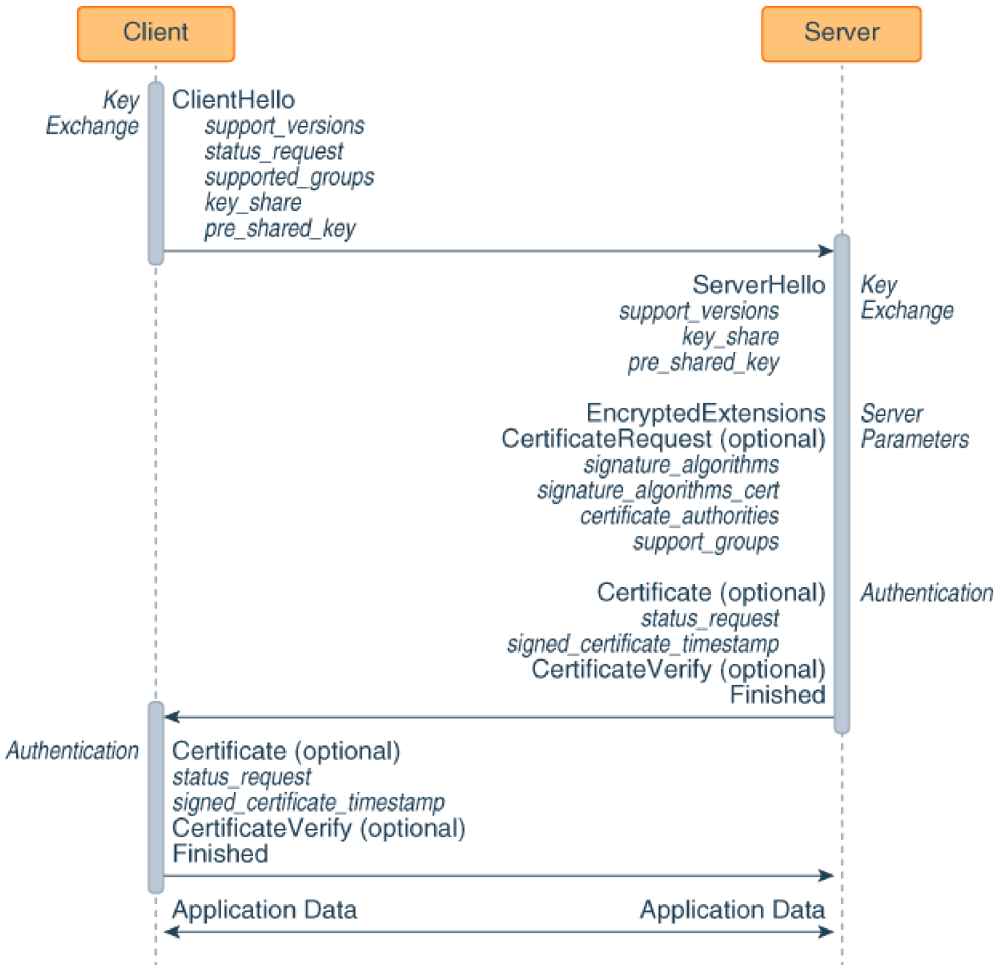
- August 2023: Google announce Protecting Chrome Traffic with Hybrid Kyber KEM
- Chrome begin supporting X25519Kyber768 for establishing symmetric secrets in TLS, starting in Chrome 116

Openfind

- September 2023: Openfind pioneered the introduction of PQC technology in the Mail2000 email system
- Accessing emails through the latest Chrome browser, or between two Mail2000 systems that have implemented PQC, provides protection against quantum attacks

X25519Kyber768 Post-Quantum Key Exchange for HTTPS

Generative Future



Client

Server

Key Exchange

ClientHello
support_versions
status_request
supported_groups
key_share
pre_shared_key

ServerHello
support_versions
key_share
pre_shared_key

Key Exchange

EncryptedExtensions
CertificateRequest (optional)
signature_algorithms
signature_algorithms_cert
certificate_authorities
support_groups

Server Parameters

Certificate (optional)
status_request
signed_certificate_timestamp
CertificateVerify (optional)
Finished

Authentication

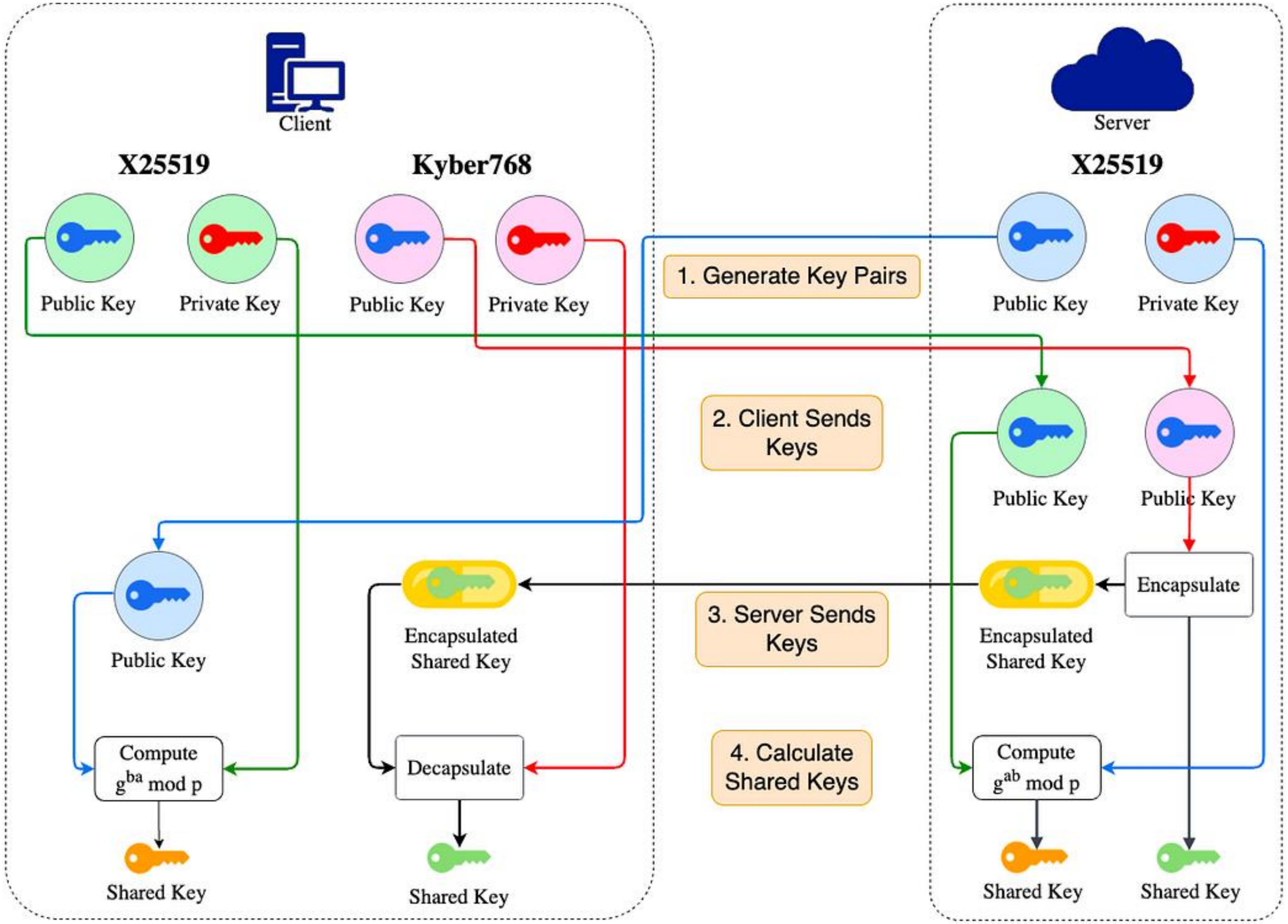
Authentication

Certificate (optional)
status_request
signed_certificate_timestamp
CertificateVerify (optional)
Finished

Application Data

Application Data

Key Exchange in TLS 1.3



Client

X25519

Kyber768

Public Key

Private Key

Public Key

Private Key

Server

X25519

Public Key

Private Key

1. Generate Key Pairs

2. Client Sends Keys

Public Key

Public Key

Encapsulate

Encapsulated Shared Key

3. Server Sends Keys

Public Key

Encapsulated Shared Key

Compute g^{ba} mod p

Decapsulate

4. Calculate Shared Keys

Compute g^{ab} mod p

Shared Key

Shared Key

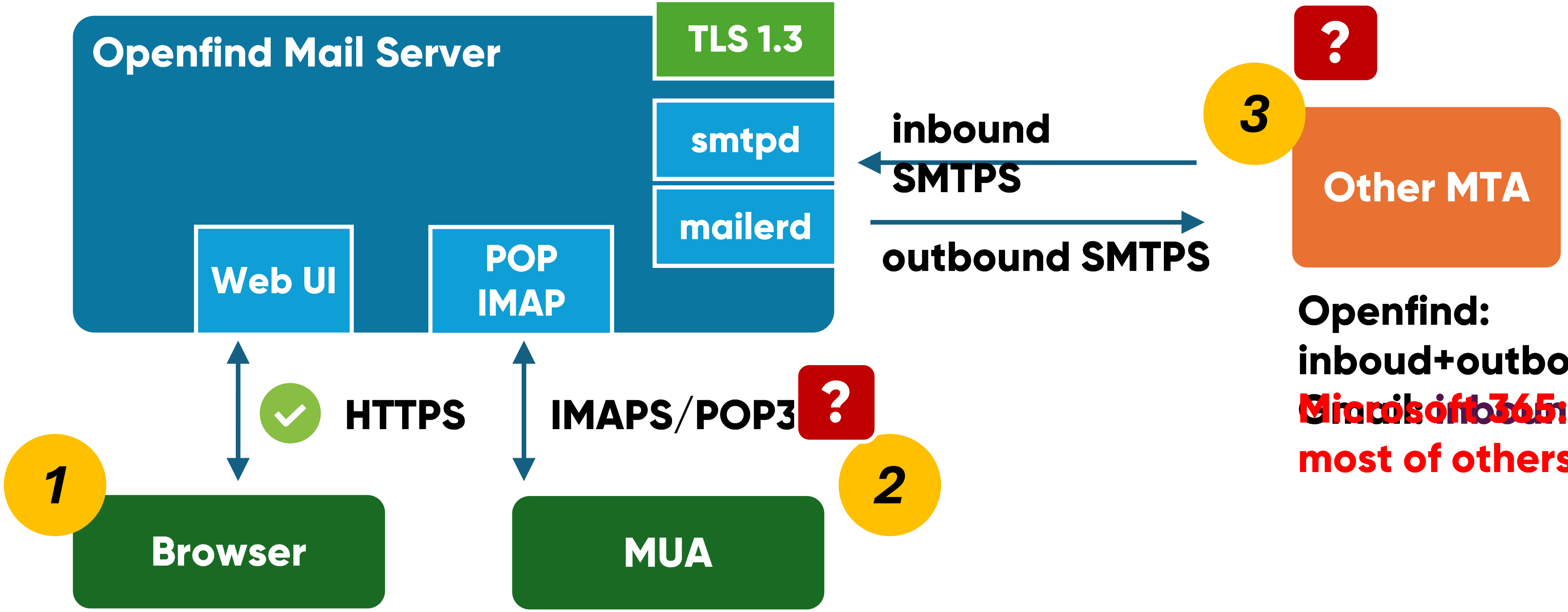
Shared Key

Shared Key

How X25519Kyber768 works

Source: https://medium.com/@hwupathum/using-crystals-kyber-kem-for-hybrid-encryption-with-java-0ab6c70d41fc

Assessment: PQC Integration Points in Mail



Chrome 116+

Outlook: not yet

Openfind: inboud+outbound

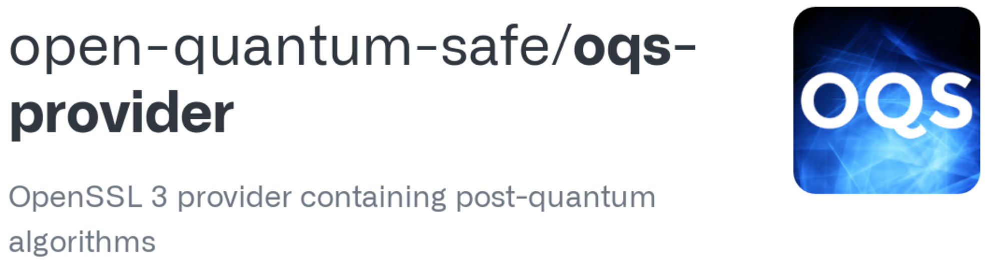
Gmail: inbound

Microsoft 365: not yet

most of others: not yet

PoC / Implement Steps

- **Build environment**
- **Integration**
- **Validation**



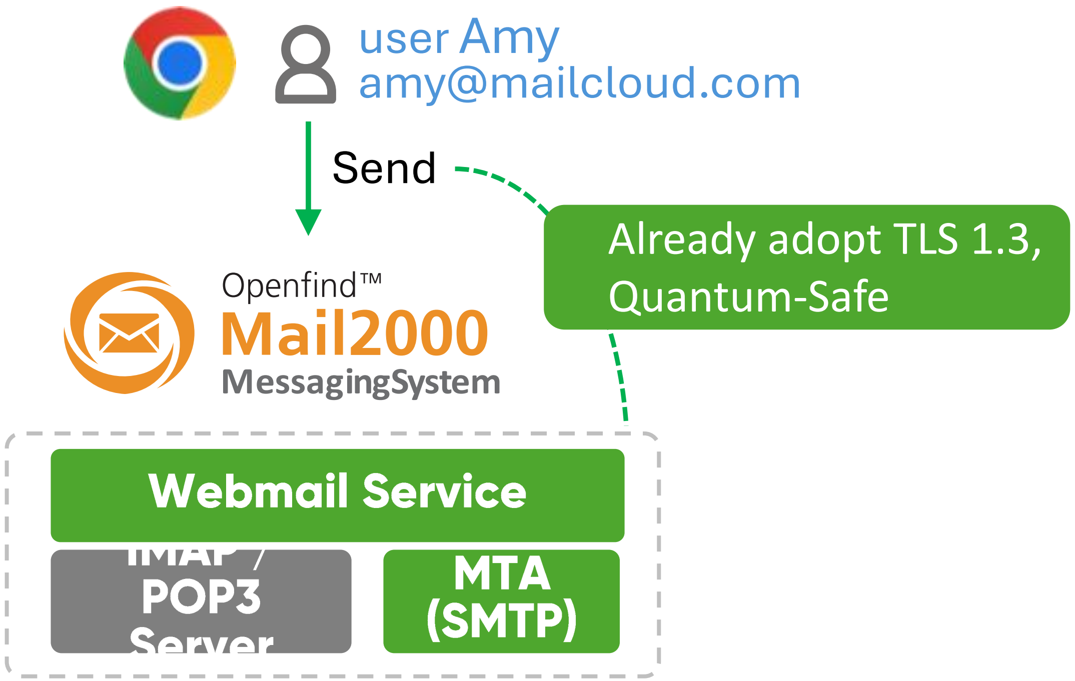
open-quantum-safe/**oqs-provider**

OpenSSL 3 provider containing post-quantum algorithms

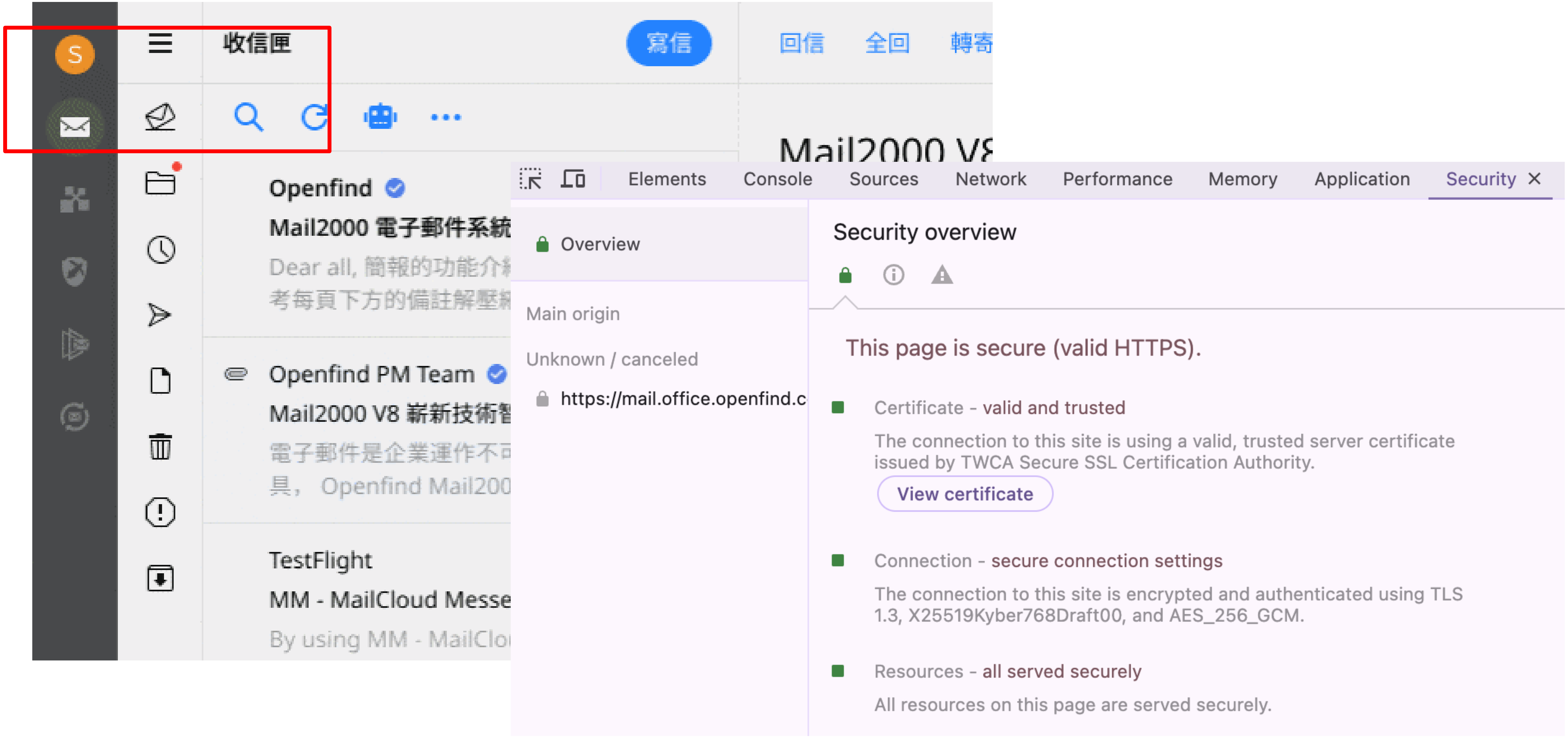
https://github.com/open-quantum-safe/oqs-provider

Chelpis

https://www.chelpis.com/



Visual design in Webmail



Openfind
Mail2000 電子郵件系統
Dear all, 簡報的功能介紹
考每頁下方的備註解壓縮

Openfind PM Team
Mail2000 V8 嶄新技術
電子郵件是企業運作不可
具，Openfind Mail200

TestFlight
MM - MailCloud Messe
By using MM - MailClo

https://mail.office.openfind.c

Security overview

This page is secure (valid HTTPS).

Certificate - valid and trusted

The connection to this site is using a valid, trusted server certificate issued by TWCA Secure SSL Certification Authority.

View certificate

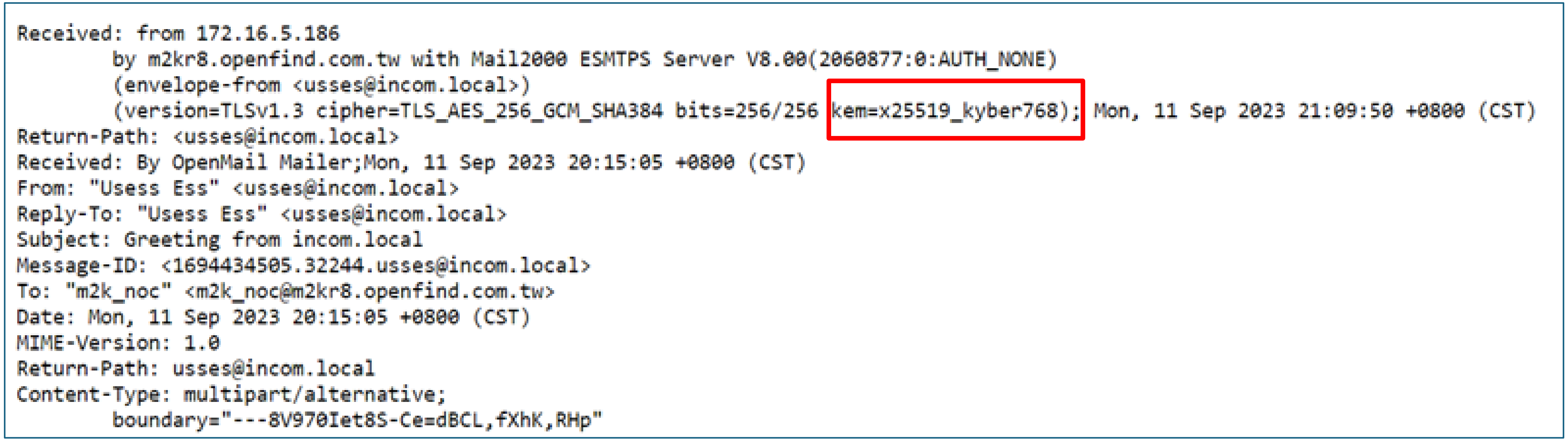
Connection - secure connection settings

The connection to this site is encrypted and authenticated using TLS 1.3, X25519Kyber768Draft00, and AES_256_GCM.

Resources - all served securely

All resources on this page are served securely.

Record KEM in Mail “Received” header



```
Received: from 172.16.5.186
        by m2kr8.openfind.com.tw with Mail2000 ESMTPS Server V8.00(2060877:0:AUTH_NONE)
        (envelope-from <usses@incom.local>)
        (version=TLSv1.3 cipher=TLS_AES_256_GCM_SHA384 bits=256/256 kem=x25519_kyber768); Mon, 11 Sep 2023 21:09:50 +0800 (CST)
Return-Path: <usses@incom.local>
Received: By OpenMail Mailer;Mon, 11 Sep 2023 20:15:05 +0800 (CST)
From: "Usess Ess" <usses@incom.local>
Reply-To: "Usess Ess" <usses@incom.local>
Subject: Greeting from incom.local
Message-ID: <1694434505.32244.usses@incom.local>
To: "m2k_noc" <m2k_noc@m2kr8.openfind.com.tw>
Date: Mon, 11 Sep 2023 20:15:05 +0800 (CST)
MIME-Version: 1.0
Return-Path: usses@incom.local
Content-Type: multipart/alternative;
        boundary="---8V970Iet8S-Ce=dBCL,fXhK,RHp"
```

Sharing of thoughts and experiences

Performance

Some may worry that PQC might impose extra burden on servers (CPU & network traffic), but in practice, the impact is minimal.

Awareness

Currently, too few people are concerned with PQC; many still underestimate the potential threats posed by quantum computers today.

Teamwork

This is a group game; playing alone yields too little benefit. We urge all MTA & MUA providers to support this promptly.

Opportunities and Challenges

Ahead of Others

Webmail, MUA, MTA: Fully Supported

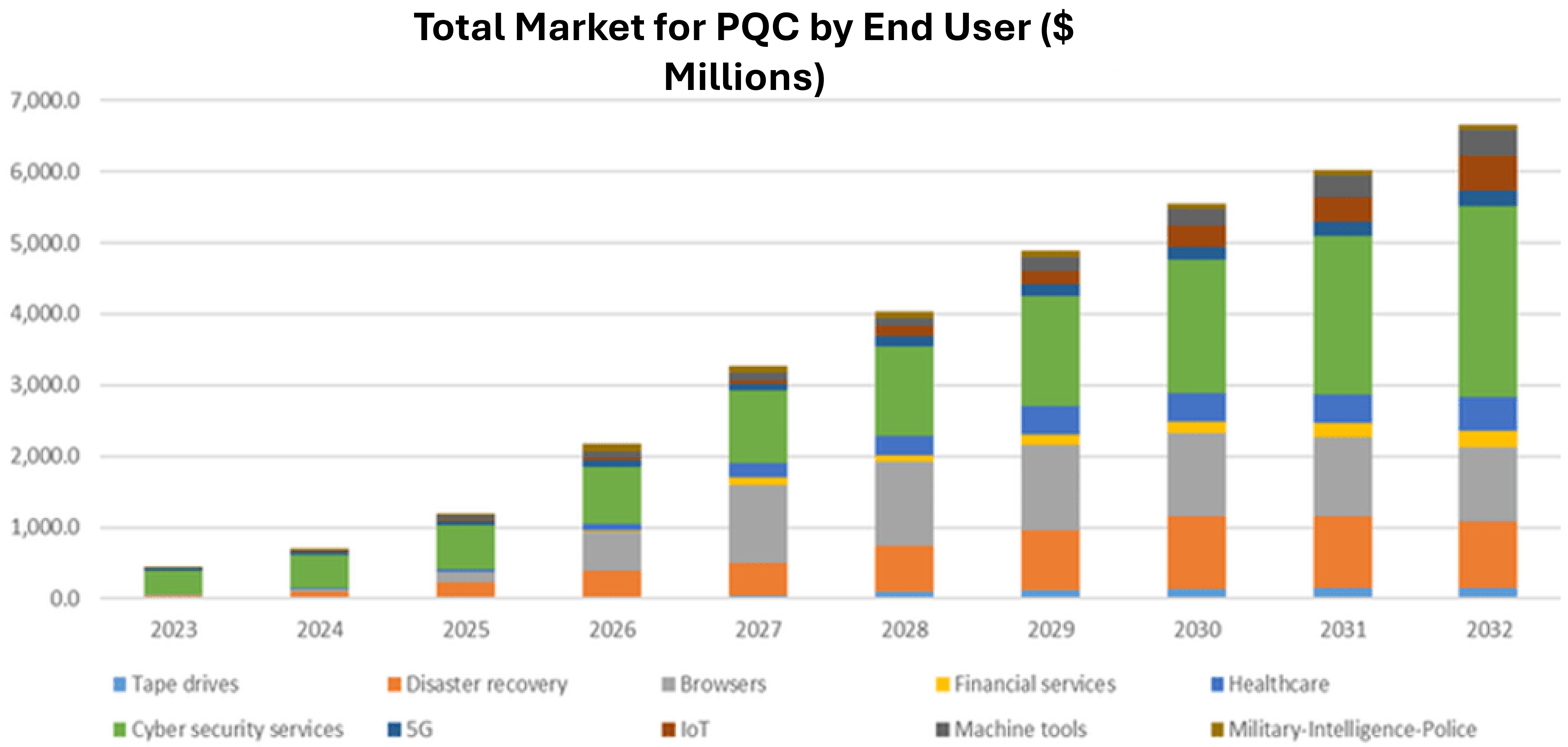
Immediate HNDL Prevention

Challenges Remain

Incomplete PQ Safety with Other MTAs

Awaiting Market Awareness of PQC

IQT Research Forecasts Revenues from Post Quantum Cryptography to Reach $6.7 Billion by 2032



Source: https://www.insidequantumtechnology.com/

Thank you!

Ivan Liao

CEO of Openfind

ivan@openfind.com