

Proposed response to the IAB PQWS workshop invitation

Subject: PQWS Workshop Submission – Keys, Hardware, and Software/Firmware Signing

Dear PQWS Workshop Program Committee,

I would like to express my interest in participating in the IAB Workshop on Accelerating the Deployment of Post-Quantum Authentication.

I am the CEO and co-founder of Crypto4A Technologies, a Canadian developer of hardware security and cryptographic infrastructure. I have been involved in the design and deployment of HSM technology and cryptographic systems for more than three decades, including contributing to PKCS#11 and working on cryptographic modernization within the Canadian government.

I would particularly like to contribute to two of the workshop topics:

1. Keys and hardware

HSMs, FIPS 140-3, PKCS#11 readiness, stateful hash-based key management, and constrained/IoT devices

There is an important gap between defining PQC algorithms and making them operationally feasible usable within the hardware and key-management infrastructure on which today's PKI and trusted computing depends.

I would like to discuss practical experience from the HSM perspective, including:

- What it means for an HSM to be genuinely **PQC-ready and crypto-agile**, rather than simply adding PQC algorithms to an existing cryptographic interface.
- The implications of **FIPS 140-3 validation** for PQC-enabled HSMs and the practical challenges of bringing new PQC algorithms and key-management mechanisms through a validated cryptographic module.
- **PKCS#11 readiness for PQC**, including the challenges associated with representing new key types, mechanisms, attributes and lifecycle operations while maintaining interoperability with existing applications and PKI infrastructure.
- The operational challenges of managing **stateful hash-based signatures such as LMS/HSS**, particularly the requirement to preserve and advance signing state without ever reusing a one-time signing key.
- The implications of stateful signatures for HSM backup, cloning, high availability, disaster recovery, key migration and audit.

I believe there is considerable value in discussing these issues from the perspective of actually deploying PQC-capable hardware rather than considering PQC solely at the algorithm or protocol layer.

2. Software and firmware signing

Package, container and firmware size limitations, offline verification, and long-lived or archival validation

If I'm allowed the time, I would also like to contribute practical experience concerning the use of PQC signatures for software and firmware authentication.

In particular, I would be interested in discussing:

- The distinction between the relatively modest impact of PQC signatures on a large software package and their potentially significant impact on **small firmware images and constrained devices**.
- The implications of signature size and verification cost for **secure boot and remote firmware update architectures**.
- The use of **stateful hash-based signatures for firmware signing**, including the operational advantages and risks associated with maintaining signing state over the lifetime of a product.
- **Offline verification**, particularly for devices that may be disconnected for long periods or operate in environments where access to online certificate status or trust services cannot be assumed.
- The problem of **long-lived devices and system's software and firmware**: how do we maintain the ability to validate a signature for decades after a device was originally deployed, particularly when the original trust anchor or signing infrastructure is "burned-in" for the life of a device? What are the requirements to ensure that the signing algorithm, certificate chain and cryptographic materials are maintained over the device's operational lifetime?
- The relationship between PQC migration and **secure update mechanisms**, where the update mechanism itself may have a lifetime comparable to or greater than the cryptographic algorithms being used today.

I believe this last point deserves particular attention. For long-lived systems, the objective should not simply be to make today's firmware signing PQC-capable. We need to consider whether the **entire trust and update mechanism remains recoverable, verifiable and cryptographically trustworthy throughout the operational lifetime of the device**.

Perspective I would bring to the workshop

My primary interest would therefore be in discussing the **deployment and lifecycle implications of PQC**, rather than the design of the underlying algorithms.

In my experience, the difficult part of PQC migration is increasingly not:

"Can we implement the algorithm?"

but rather:

"Can we deploy, validate, manage, update, recover and eventually retire the cryptographic keys and trust infrastructure over the lifetime of the system?"

This becomes particularly important for HSMs, PKI infrastructure, firmware signing systems, IoT devices and other systems expected to remain operational for many years.

I would be pleased to contribute to a discussion focused on these practical deployment challenges and on identifying areas where additional standards work or interoperability guidance would help accelerate PQC adoption.

Best regards,

Bruno Couillard

CEO & Co-founder

Crypto4A Technologies Inc.

Canada