ETSI/IQC Quantum Safe Cryptography Conference 2026

Quantum-Safe HSM Design

Presented by: Dr. Jim Goodman, CTO

CRYPTO4A

18/06/2026

Quantum-Safe HSM Design

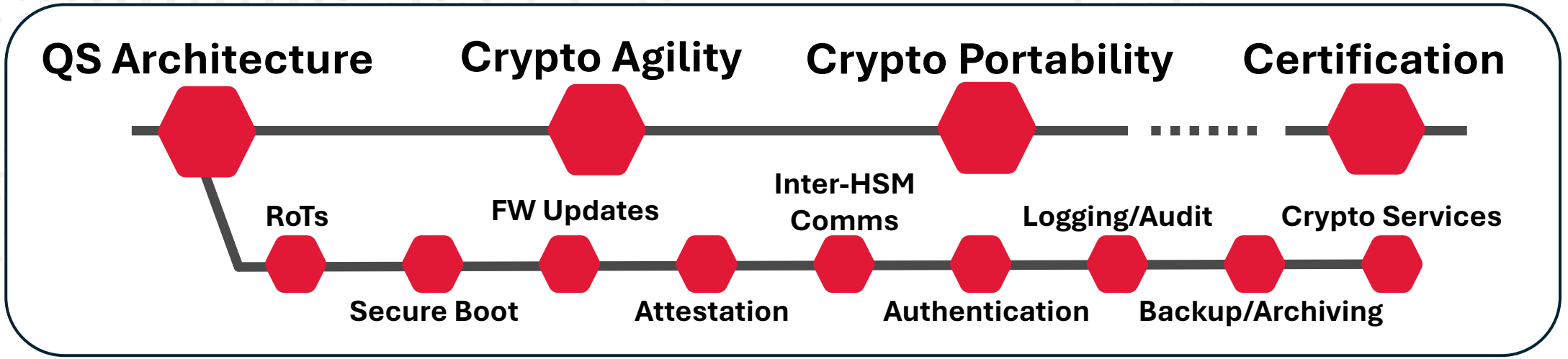
Dr. Jim Goodman, CTO

June 18th ,2026

A Unique Opportunity

- The PQC migration is the perfect opportunity to fix the sins of the past as we transition to a (hopefully!) quantum safe future
- HSMs are both the providers and **CONSUMERS** of cryptography
  - Most people tend to focus on the former and overlook the latter
- Develop next generation **MODERN** quantum-safe HSMs
  - Quantum-safe foundation and architecture with PQC services/capabilities
  - Crypto agility
  - Crypto portability
- Update certifications to **REQUIRE** quantum-safe elements

Designing for the Future



- HSMs utilize cryptography to protect a number of core capabilities that provide their security foundations
  - Root-of-Trust Lifecyle Management
  - FW Updating & Secure Boot
  - Attestation
  - Inter-HSM Comms
  - Authentication
  - Logging & Auditing
  - Backup & Archiving
  - Cryptographic Services

Protect core HSM functions using QUANTUM-SAFE (QS) approaches

Quantum-Safe Roots-of-Trust (RoT)

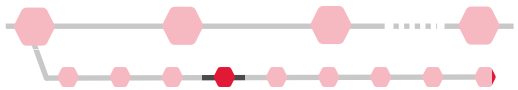
- Step (minus) one: **install QS Roots-of-Trust**
- Complication: updating/replacing roots-of-trust
  - Transition to different algorithm or parameter set for RoT
  - Recover from compromised RoT
  - Lose access to private key associated with RoT
  - Transition control to another authority and its RoT
- Leverage standardized techniques such as Trust Anchor Management Protocol (TAMP – RFC 5934)
  - Deploy TAMP artifacts inside devices for potential future use
  - Better to have it and not need it, then to need it and not have it!

Quantum-Safe Booting & FW Updates

- Can’t rely on classic cryptographic algorithms to validate and protect secure boot process and FW upgrades
  - Can’t update your way out of this at some point in the future due to lack of trust in update that transitions to a QS alternative
- Use quantum-safe FW signing infrastructure from the start
  - Validate updates using conservative QS algorithms (e.g., HBS)
  - Upgrade underlying hardware components as they become available, but in the mean time rely on AES-GCM for QS integrity/confidentiality

Quantum-Safe Attestation

- Provides cryptographic proof of identity, origin, and system integrity
  - HSM evaluates claims, generates digitally-signed response attesting to them
  - Enables high assurance remote operation
- Allow for both classical and QS options for your attestation trust anchors (crypto agility for the win!)
  - Should use **conservative cryptographic algorithms** to ensure long term resilience
- Allow the generation of user-specific attestation keys to simplify user-specific attestation validation
  - Allow transition to different attestation authorities
  - Use to update exhausted attestation authorities (e.g., S-HBS)



CRYPTO4A

Quantum-Safe Inter-HSM Comms

- Need to securely transfer keys between devices
  - Required to provide high-availability, disaster recovery and load balancing
  - **SNDL attacks are as relevant in inter-HSM comms as they are between servers on the Internet**
- Crypto agility requires variety of algorithms to ensure compatibility while providing quantum-safe options
  - Don’t forget the hybridized/composite variants
- Quantum-safe option considerations
  - Would have liked a standardized Classic McEliece but it wasn’t to be

Quantum-Safe Authentication

- Access authentication governs access to every secure operation for users/administrators
- Need to ensure the use of QS authentication mechanisms to ensure only legitimate users and systems retain control

Quantum-Safe Logging/Auditing

- Secure logging and auditing are essential for security, accountability, compliance, and incident response
  - Provide verifiable, time-stamped record of system activity
  - Enables breach detection, policy enforcement validation, and reconstruction of events to determine timeline and scope of an incident
- Need QS integrity protection mechanisms to ensure they aren’t susceptible to modification/forgery

Quantum-Safe Backup/Archiving

- Backups preserve critical key material and configuration data
- Need to securely store keying material outside the HSM security boundary
  - Running out of internal storage
  - Facilitating disaster recovery and resiliency mechanisms using resilient external storage facilities (i.e., backup and restore)
  - Storing permanent keys in an external “secure world” container
- Ensure you’re using QS cryptographic primitives to protect keys/backups outside of the HSM security boundary
  - **SNDL types of attacks are as relevant for externally stored HSM data as they are for Internet Traffic**

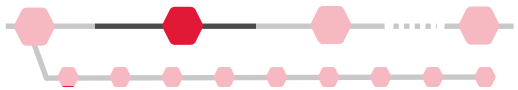
CRYPTO4A

Quantum-Safe Cryptographic Services

- HSMs exist to serve external systems by providing encryption, signing, and key management services
- Need to provide CAVP-certified PQC primitives
  - ML-KEM, ML-DSA, SLH-DSA, LMS/HSS, etc.
- Need to be able to adapt to evolving standards as we continue to transition to a (hopefully!) quantum safe reality using crypto agility
  - Requires conservative FW update process to secure the evolution

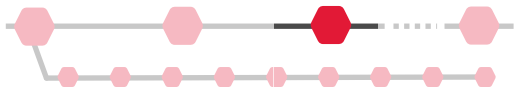
Crypto Agility

- Migration to PQC introduces a lot of churn
  - Adopt stop-gap solutions due to time constraints
  - Will solutions implemented today be supported 10+ years down the line?
- Engineer solutions that are able to **EVOLVE** over time **AND** maintain backwards compatibility over entire lifecycle
  - Robust and secure upgrade mechanisms to allow you to evolve through a range of algorithms without being the weak link
  - Reprogrammable system components allow you to deliver the necessary performance as you introduce new algorithms
- Consider overall system performance impact of hybrid approach between existing and new algorithms



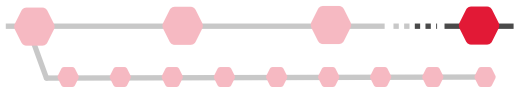
Crypto Portability

- Ability to adopt a security posture in which the user owns their keys and can ultimately decide what they want to do with them
  - Extend crypto agility to the provenance of private keying material to allow for customer migration to alternative platforms
- **Eliminates vendor lock-in** by providing mechanisms and tools to securely migrate keys to another device
  - HSM vendors **need to work together** to define mechanisms and formats to allow secure transfers (e.g., PKIC-CM PACKeM)
  - Forces HSM vendors to up their game by giving customers the ability to migrate more easily to other platforms



Certification Requirements

- Certification processes like FIPS 140-3 do **NOT** have specific requirements to ensure modules use QS mechanisms for their internal services
  - Can end up relying on mechanisms that will be deprecated in 2030 and disallowed in 2035
  - Operational lifetimes will likely take modules past these dates putting users at risk
- Use the PQC transition to start introducing requirements (or IGs) for the use of QS internal mechanisms to cover this gap



Thank you!

Dr. Jim Goodman,

CTO, Co-Founder – Crypto4A

jimg@crypto4a.com