Post-Quantum

Cryptography Conference

From Inventory to Action: Navigating the Next Phase of PQC Transition

Bruno Couillard

Co-Founder & CEO at Crypto4A

KEYFACTOR CRYPTO4A SSL.com ENTRUST HID

October 28 - 30, 2025 - Kuala Lumpur, Malaysia

PKI Consortium

CRYPTO4A

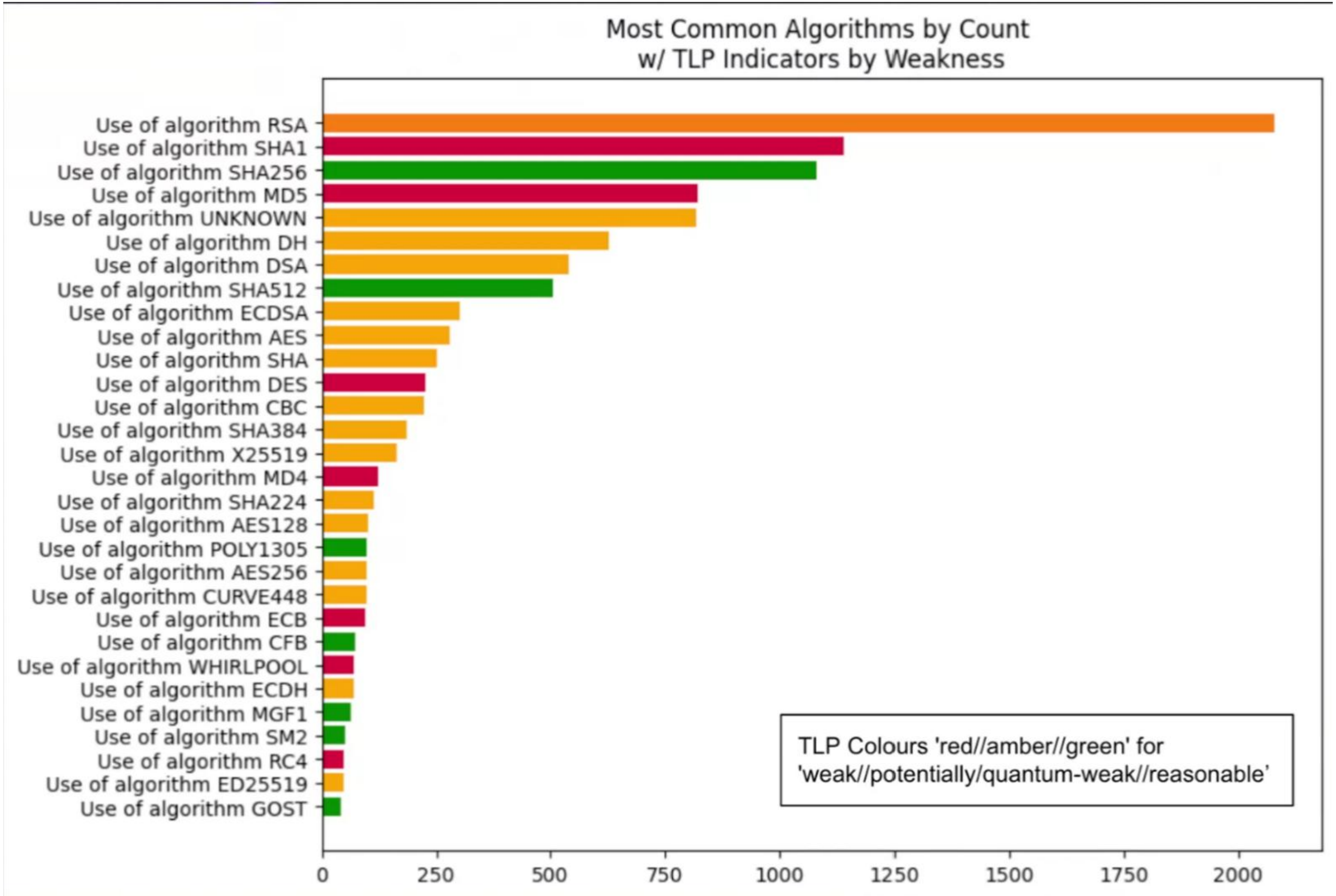
From Inventory to Action: Navigating the Next Phase of PQC Transition

Kuala Lumpur, Malaysia

October 30th, 2025

Discovery Projects

CRYPTO4A


Most Common Algorithms by Count
w/ TLP Indicators by Weakness
Use of algorithm RSA
Use of algorithm SHA1
Use of algorithm SHA256
Use of algorithm MD5
Use of algorithm UNKNOWN
Use of algorithm DH
Use of algorithm DSA
Use of algorithm SHA512
Use of algorithm ECDSA
Use of algorithm AES
Use of algorithm SHA
Use of algorithm DES
Use of algorithm CBC
Use of algorithm SHA384
Use of algorithm X25519
Use of algorithm MD4
Use of algorithm SHA224
Use of algorithm AES128
Use of algorithm POLY1305
Use of algorithm AES256
Use of algorithm CURVE448
Use of algorithm ECB
Use of algorithm CFB
Use of algorithm WHIRLPOOL
Use of algorithm ECDH
Use of algorithm MGF1
Use of algorithm SM2
Use of algorithm RC4
Use of algorithm ED25519
Use of algorithm GOST
0
250
500
750
1000
1250
1500
1750
2000
TLP Colours 'red//amber//green' for
'weak//potentially/quantum-weak//reasonable'

Attack techniques:

- Harvest Now Decrypt Later (HNDL)

- **Trust Now, Forge Later (TNFL)**

“… systems that cannot be retrofitted with quantum-safe signatures are ticking time bombs of trust.”

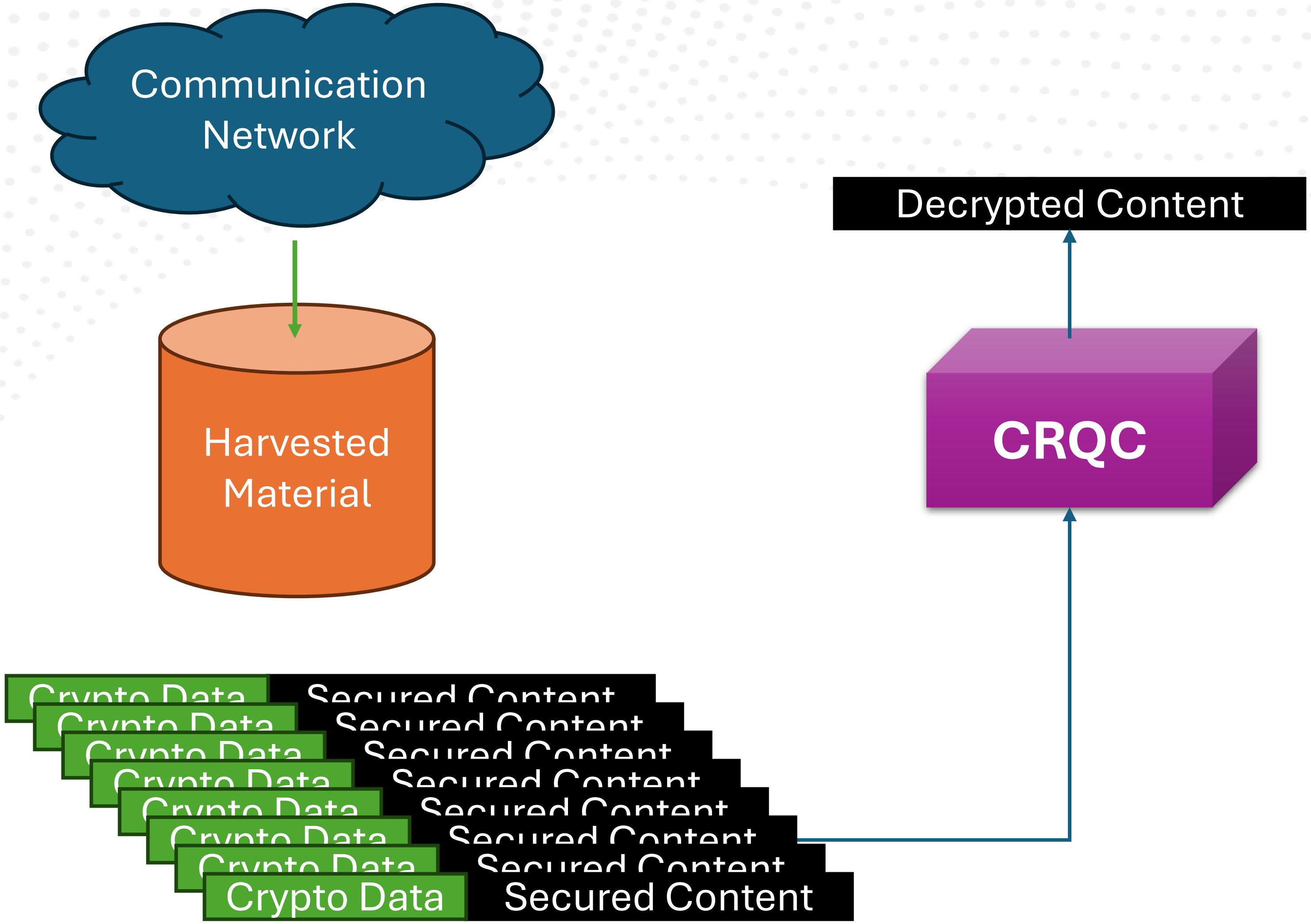
Marin Ivezic’s article, October 10th, 2025, “Trust Now, Forge Later (TNFL) – The Overlooked Quantum Threat ”

CRYPTO4A

Potential RSA usages:

- Key Transport (HNDL):
  - Capture the session establishment data and decrypt later
- Document signing (TNFL):
  - one signature, multiple verifications over time
- Code Signing (TNFL):
  - Multiple signature over time, hard-coded verification key
- Attestation (TNFL):
  - Multiple signatures over the life of a product line under a single certificate chain

HNDL - System



Communication Network

Harvested Material

Decrypted Content

CRQC

Crypto Data | Secured Content

Crypto Data | Secured Content

Crypto Data | Secured Content

Crypto Data | Secured Content

Crypto Data | Secured Content

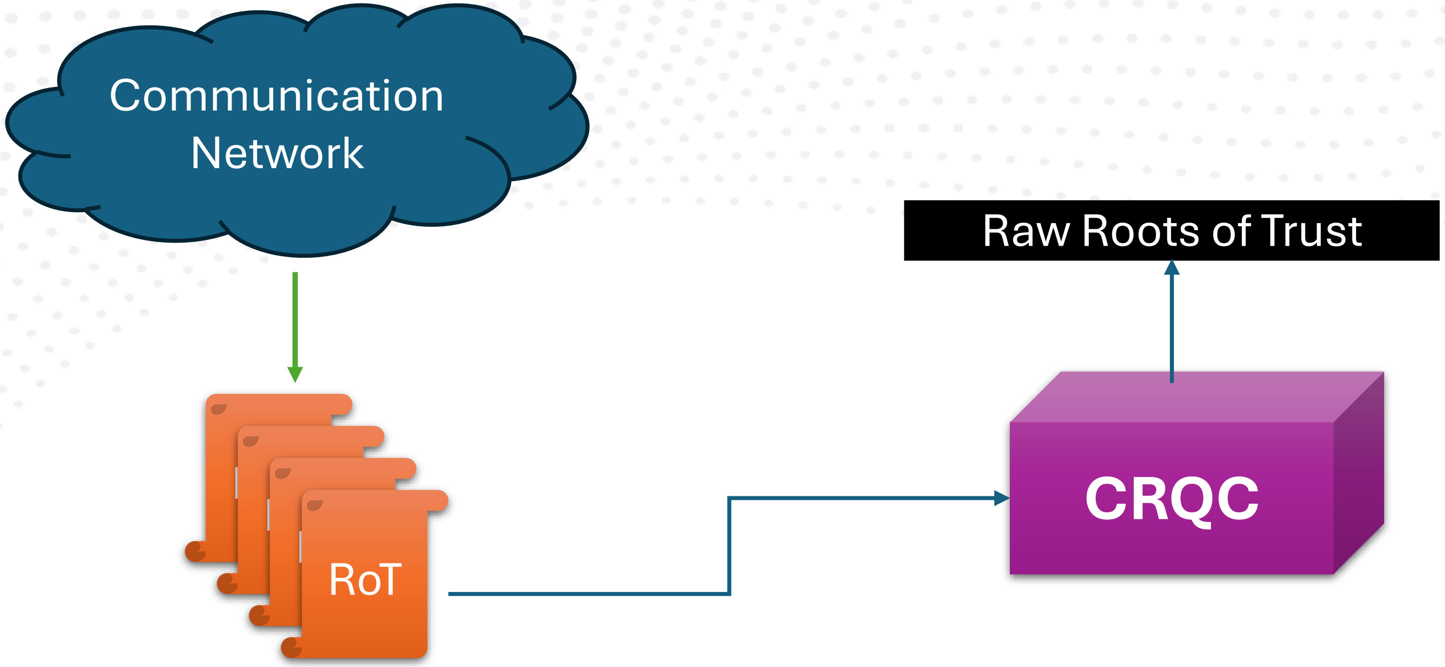
Crypto Data | Secured Content

Crypto Data | Secured Content

Crypto Data | Secured Content

- **Total cost:**
- Collection system: $
- Storage system: $
- CRQC costs:
  - Build: $$$
  - Per use: $

TNFL - System



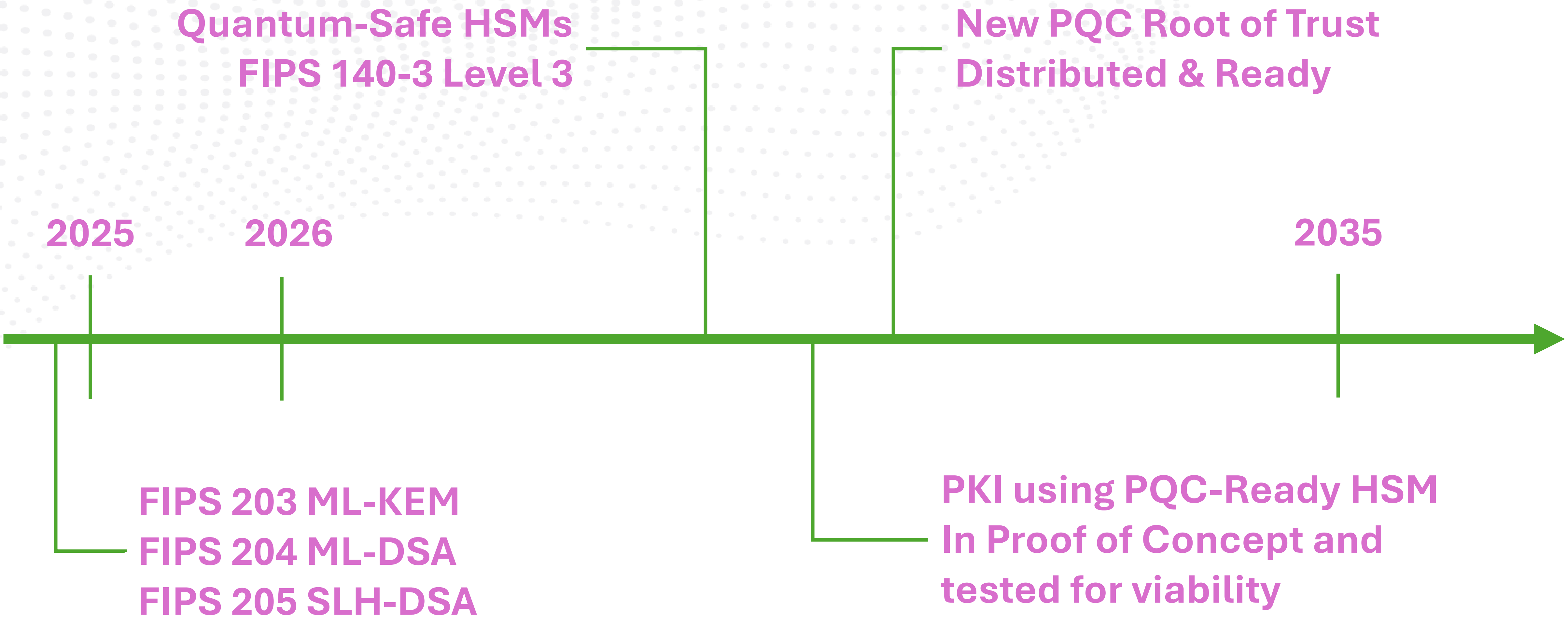
- **Total cost:**
- Collection system: 0
- Storage system: 0
- CRQC costs:
  - Build: $$$
  - Per use: $

TNFL vs HNDL costs

Items	HNDL	TNFL
Collection System	$	0
Storage System	$	0
CRQC	$$$	$$$
Cost per use	$	$
Cost of breaking 1 message:	$+$+$$$+$	$$$+$
Cost of breaking 100 messages:	$+$+$$$+**100$**	$$$+**$**
Cost of breaking 1,000,000 messages:	$+$+$$$+**1,000,000$**	$$$+**$**

PKI
HSM
Modern Digital Trust

CRYPTO4A



Quantum-Safe HSMs
FIPS 140-3 Level 3

New PQC Root of Trust
Distributed & Ready

2025

2026

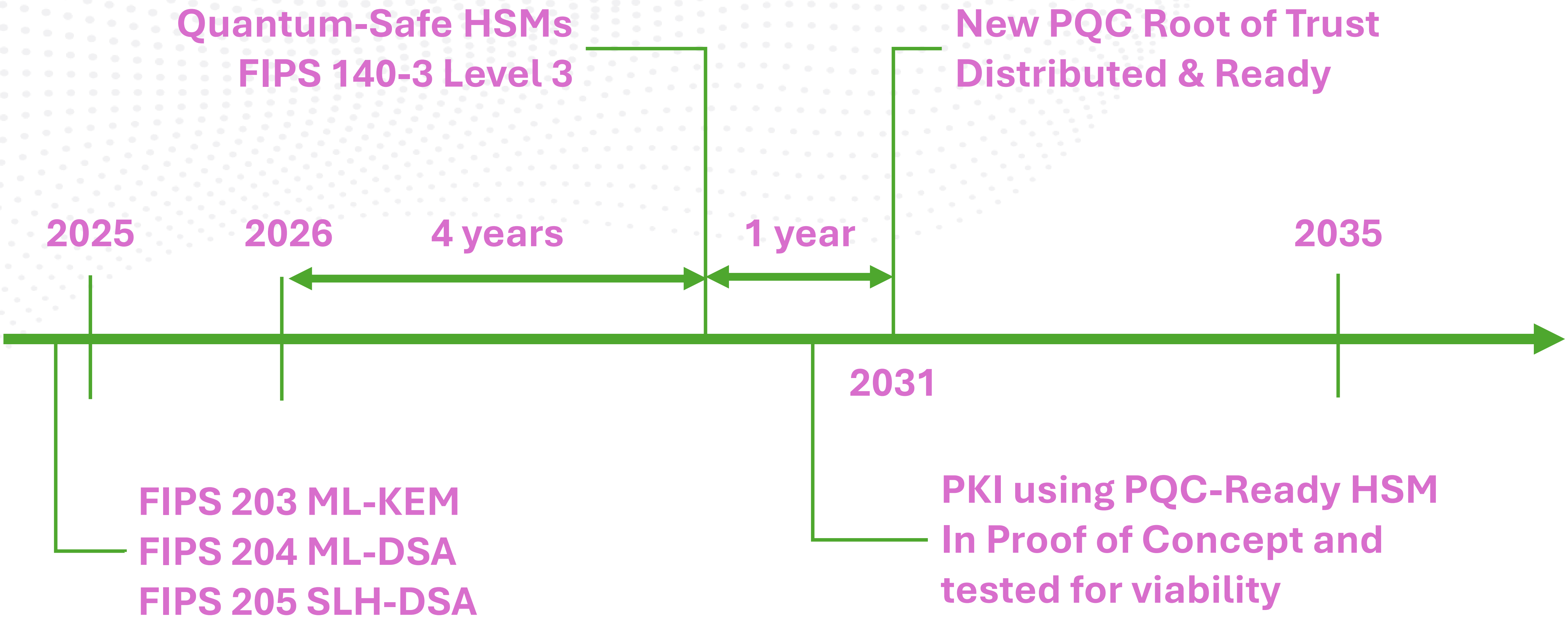
2035

FIPS 203 ML-KEM
FIPS 204 ML-DSA
FIPS 205 SLH-DSA

PKI using PQC-Ready HSM
In Proof of Concept and
tested for viability

CRYPTO4A

*Inspired by Matt Campagna’s excellent key note presentation at ICMC 2025



Quantum-Safe HSMs
FIPS 140-3 Level 3

New PQC Root of Trust
Distributed & Ready

2025

2026

4 years

1 year

2035

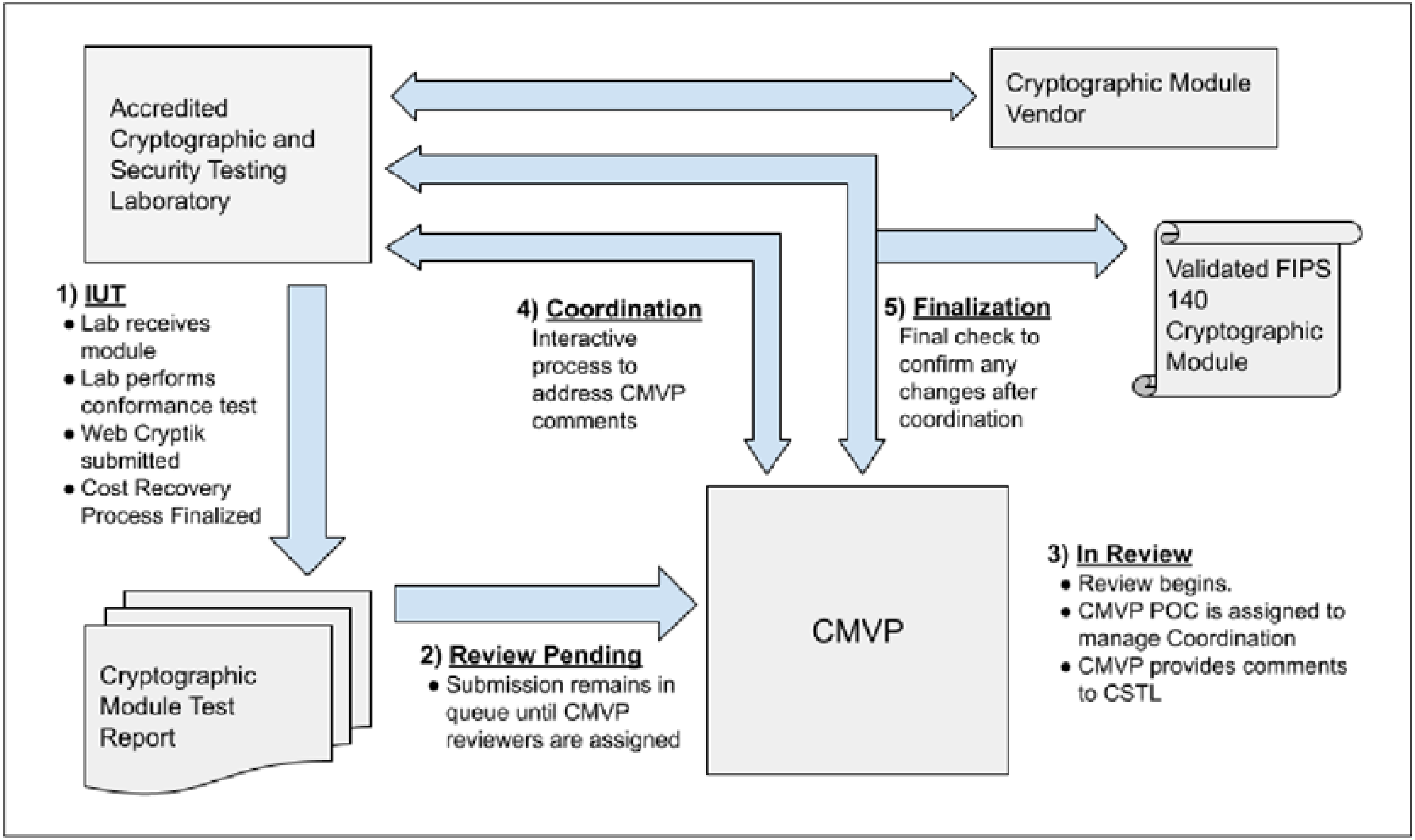
2031

FIPS 203 ML-KEM
FIPS 204 ML-DSA
FIPS 205 SLH-DSA

PKI using PQC-Ready HSM
In Proof of Concept and
tested for viability

CRYPTO4A

*Inspired by Matt Campagna’s excellent key note presentation at ICMC 2025



Accredited Cryptographic and Security Testing Laboratory

Cryptographic Module Vendor

Validated FIPS 140 Cryptographic Module

1) **IUT**

- Lab receives module
- Lab performs conformance test
- Web Cryptik submitted
- Cost Recovery Process Finalized

Cryptographic Module Test Report

2) **Review Pending**

- Submission remains in queue until CMVP reviewers are assigned

CMVP

3) **In Review**

- Review begins.
- CMVP POC is assigned to manage Coordination
- CMVP provides comments to CSTL

4) **Coordination**

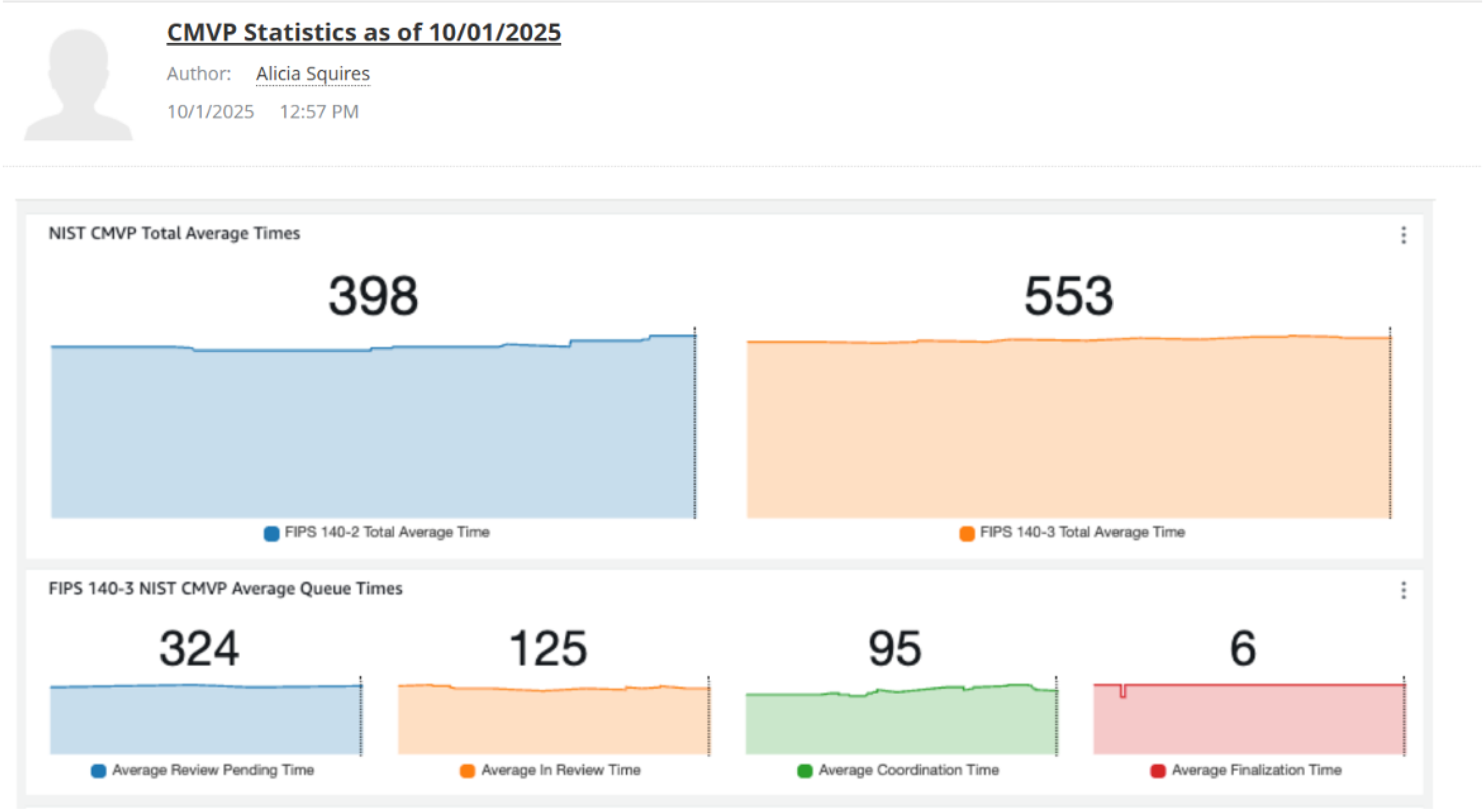
Interactive process to address CMVP comments

5) **Finalization**

Final check to confirm any changes after coordination

Figure 4- Cryptographic Module Testing and Validation Process

From the FIPS 140-3 Management Manual



CMVP Statistics as of 10/01/2025

Author: Alicia Squires

10/1/2025 12:57 PM

NIST CMVP Total Average Times

398

🟦 FIPS 140-2 Total Average Time

553

🟧 FIPS 140-3 Total Average Time

FIPS 140-3 NIST CMVP Average Queue Times

324

🟦 Average Review Pending Time

125

🟧 Average In Review Time

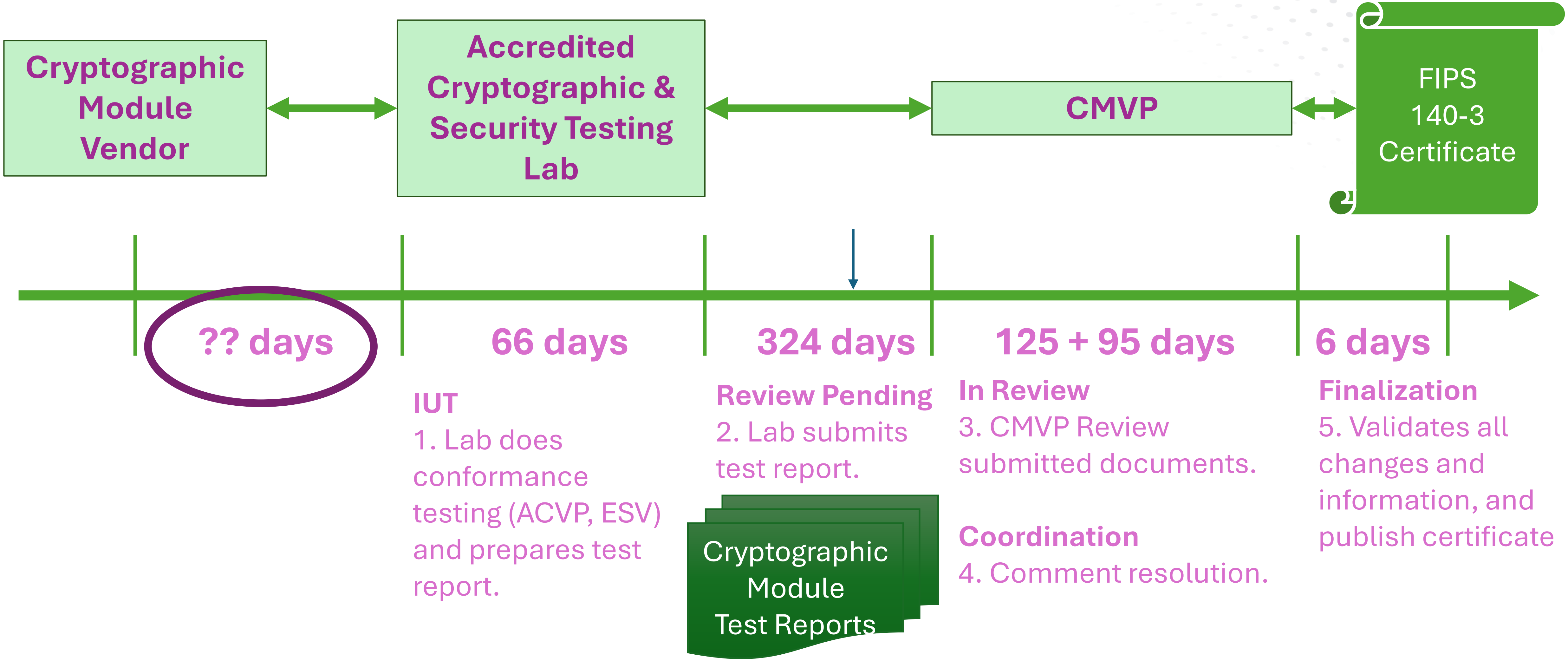
95

🟩 Average Coordination Time

6

🟥 Average Finalization Time

FIPS 140-3 Certification Timeline



Cryptographic Module Vendor

Accredited Cryptographic & Security Testing Lab

CMVP

FIPS 140-3 Certificate

?? days

66 days

IUT

1. Lab does conformance testing (ACVP, ESV) and prepares test report.

324 days

Review Pending

2. Lab submits test report.

Cryptographic Module Test Reports

125 + 95 days

In Review

3. CMVP Review submitted documents.

Coordination

4. Comment resolution.

6 days

Finalization

5. Validates all changes and information, and publish certificate

CRYPTO4A

*Inspired by Matt Campagna's excellent key note presentation at ICMC 2025

Thank you

Bruno Couillard,

CEO, Co-Founder – Crypto4A

bruno@crypto4a.com