CRYPTO4A

State of the HSM Industry

March 11th 2026

Company Background

Fast growing & Experienced Team

- 41 skilled professionals
- Founded by the engineering & product management of Chrysalis-ITS (SafeNet, Gemalto, and Thales Luna HSM)

Proven Innovation in Cybersecurity

- 44% annual growth since 2017
- Deep expertise in secure military-grade communications
- Long-term investor support from day one

Trusted Global Leaders

- Supporting Fortune 100 enterprises with quantum-safe HSM solutions
- Critical infrastructure protection for a post-quantum world

Industry First

- The ONLY company with a quantum-safe HSM deployed in production today
- Customer-centric by design
  - No vendor lock-in
  - Full control of cryptographic assets

Products & Services

- QxVault | QxHSM | QxEDGE | QxCompute | QxEmulator
- Expert-led Professional Services

Crypto4A's Team

Decades of cryptographic leadership, one mission: secure the digital future.

Bruno Couillard
Co-Founder | CEO

Dr. Jim Goodman
Co-Founder | CTO

Jean Pierre Fiset
Co-Founder | CESO

John O'Connor
VP, Product Management

Ron Vandergeest
VP, Engineering

Robert Grapes
VP, Business Development

Meaghan Green
Director, Marketing

CRYPTO4A

HSM Vendors

Main HSM Vendors

- Crypto4A (QASM/QxHSM)
- Entrust (nShield5)
- Fortanix (DSM Appliance)
- Futurex (GSP4000)
- i4p (Trident HSM)
- IBM (4770-001 CCA)
- Kryptus (ASI-HSM)
- Marvell (LS2 HSM)
- Securosys (Primus HSM)
- Thales TCT (Luna HSM - K7)
- Utimaco (u.Trust Anchor CSe)

Crypto4A – QASM/QxHSM

CRYPTO4A

Entrust – nShield5

CRYPTO4A

Fortanix – DSM Appliar

CRYPTO4A

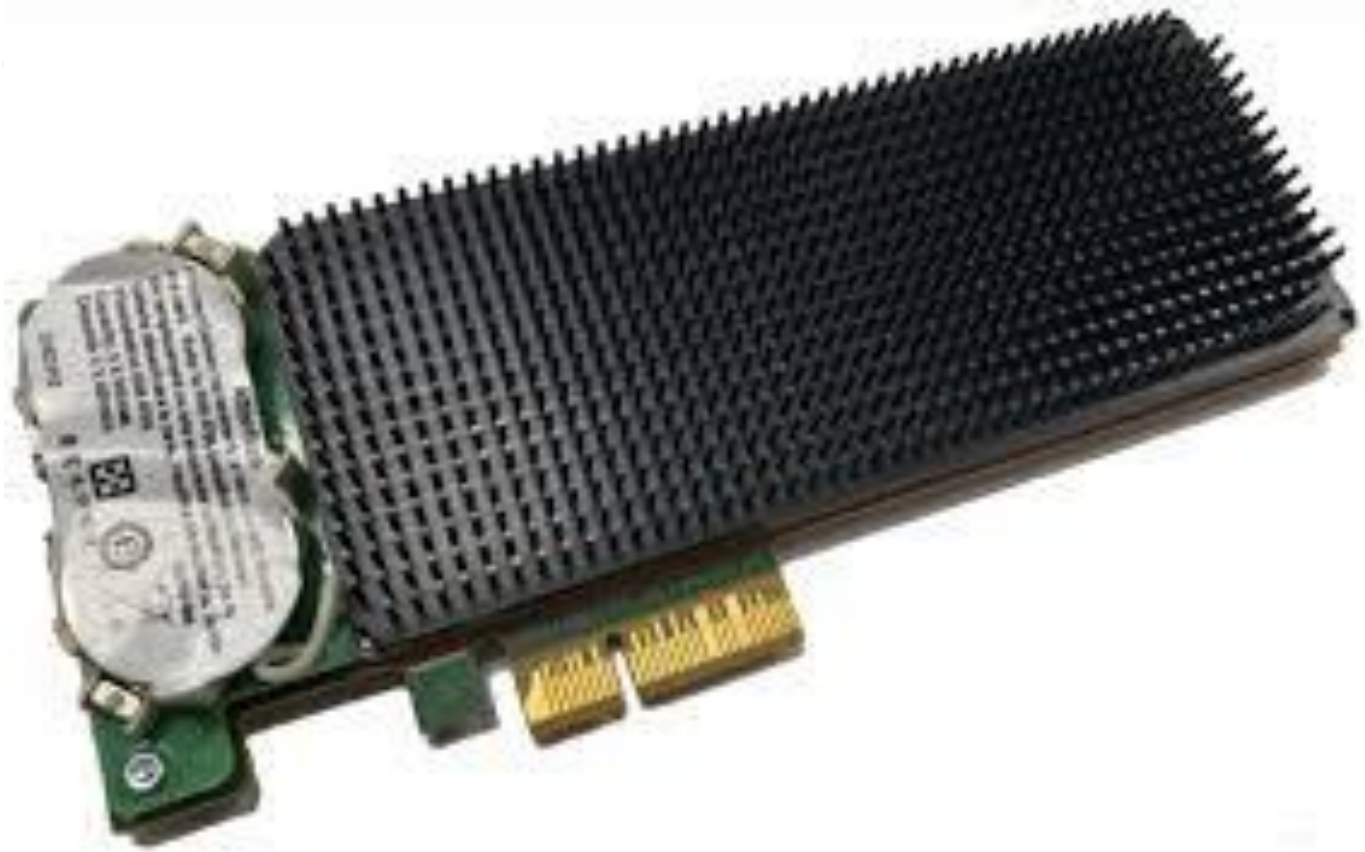
Futurex – GSP4000

CRYPTO4A

I4p – Trident HSM

CRYPTO4A

IBM – 4770-01 CCA

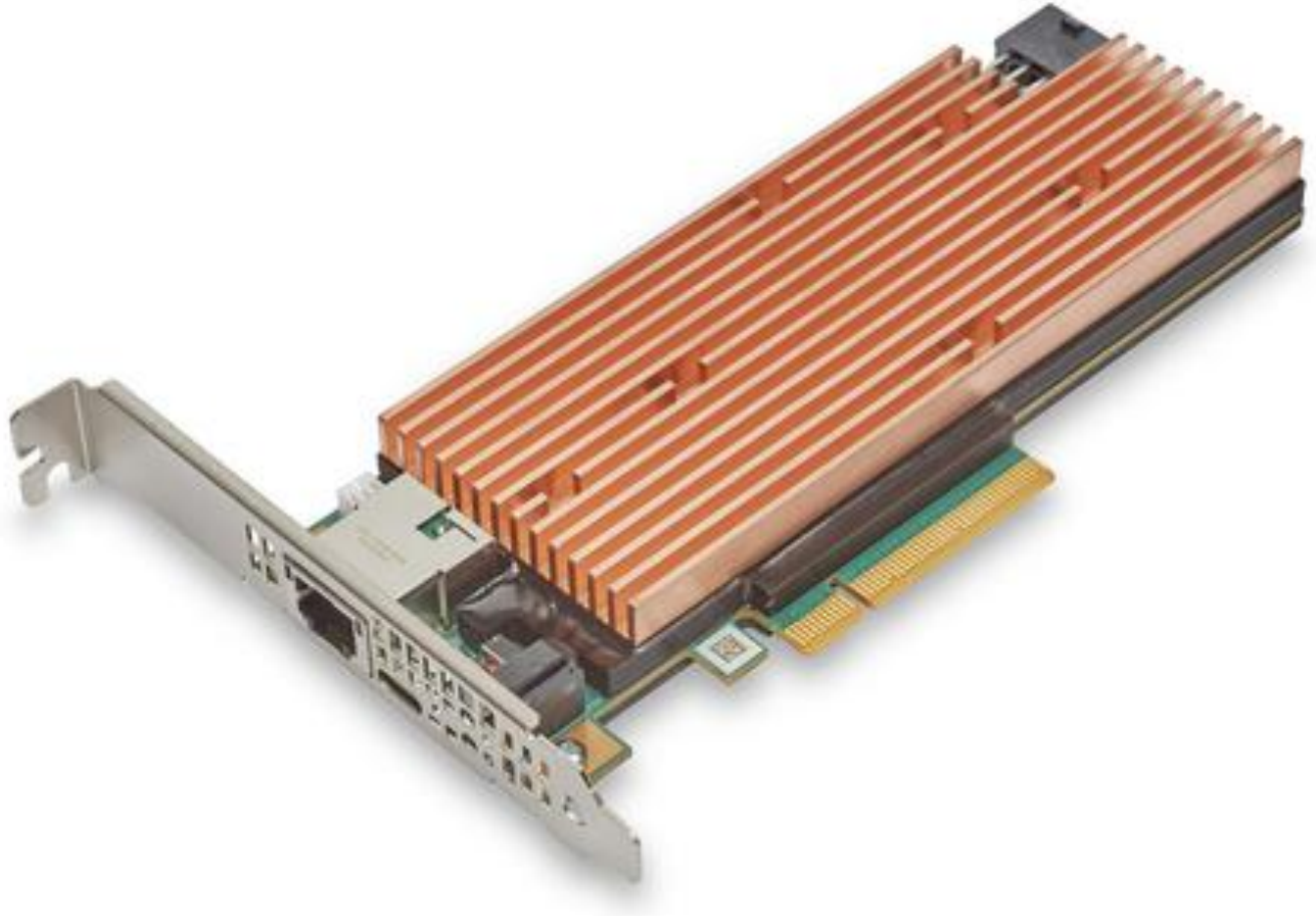


CRYPTO4A

Kryptus – ASI-HSM

CRYPTO4A

Marvell – LS2 HSM



CRYPTO4A

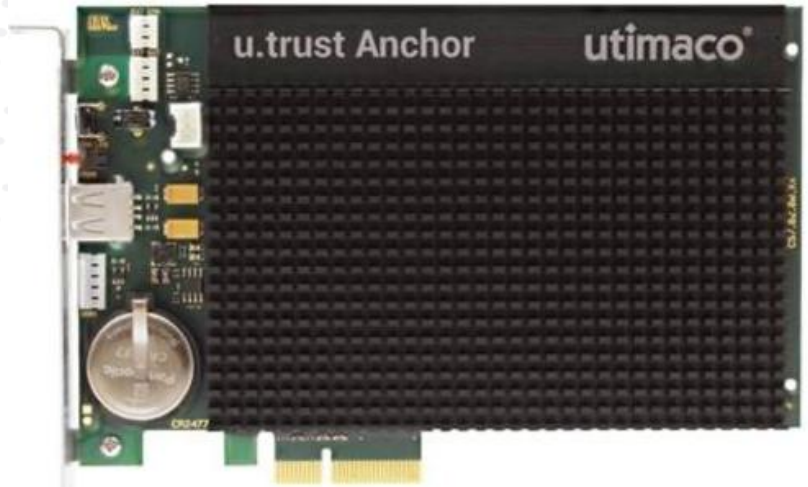
Securosys – Primus HS

CRYPTO4A

Thales – LunaHSM (K7)

CRYPTO4A

Utimaco – u.Trust Anchor CSe



CRYPTO4A

Vendor	PCIe Module	Network Appliance	Module (network+backplane)
Crypto4A (QxHSM/QxHSM)	X	X	✓
Entrust (nShield5)	✓	✓	X
Fortanix (DSM Appliance)	X	✓	X
i4P (Trident HSM)	X	✓	X
IBM (4770-001 CCA)	✓	X	X
Kryptus (ASI-HSM)	X	✓	X
Marvell (LS2 HSM)	✓	X	X
Securosys (Primus HSM)	X	✓	X
Thales (Luna HSM – K7)	✓	✓	X
Utimaco (u.Trust Anchor Cse)	✓	✓	X

FIPS 140-3 Validation

FIPS 140-3 Validation

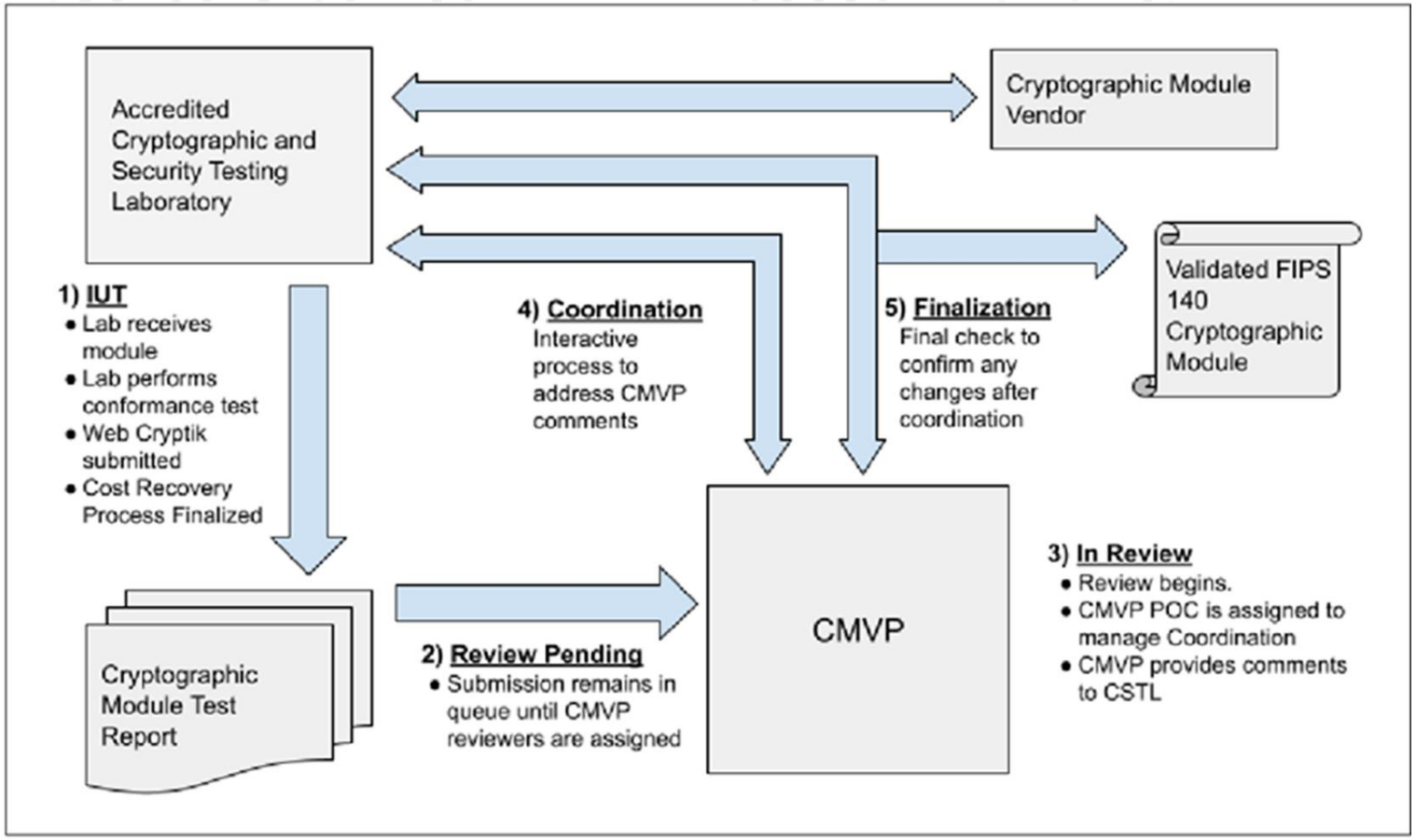
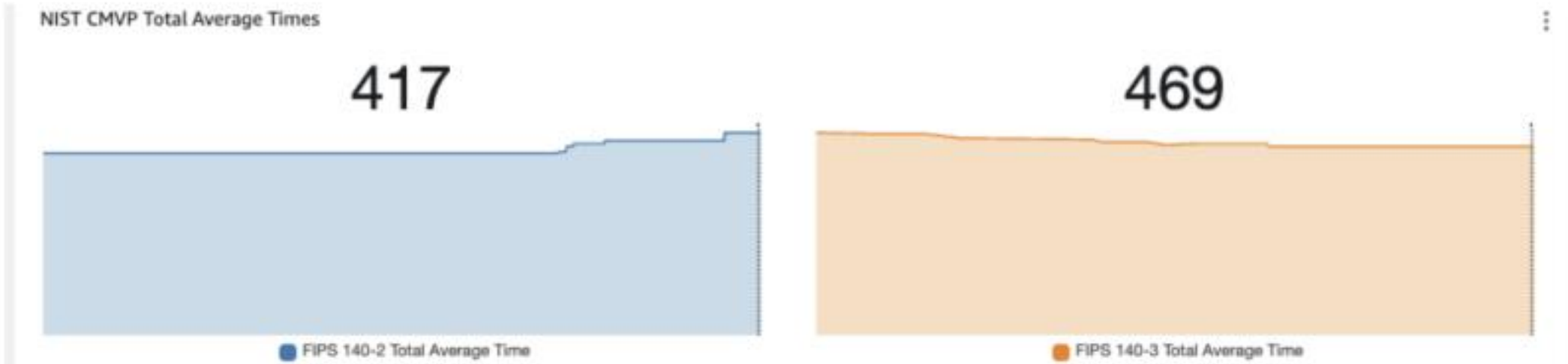


Figure 4- Cryptographic Module Testing and Validation Process

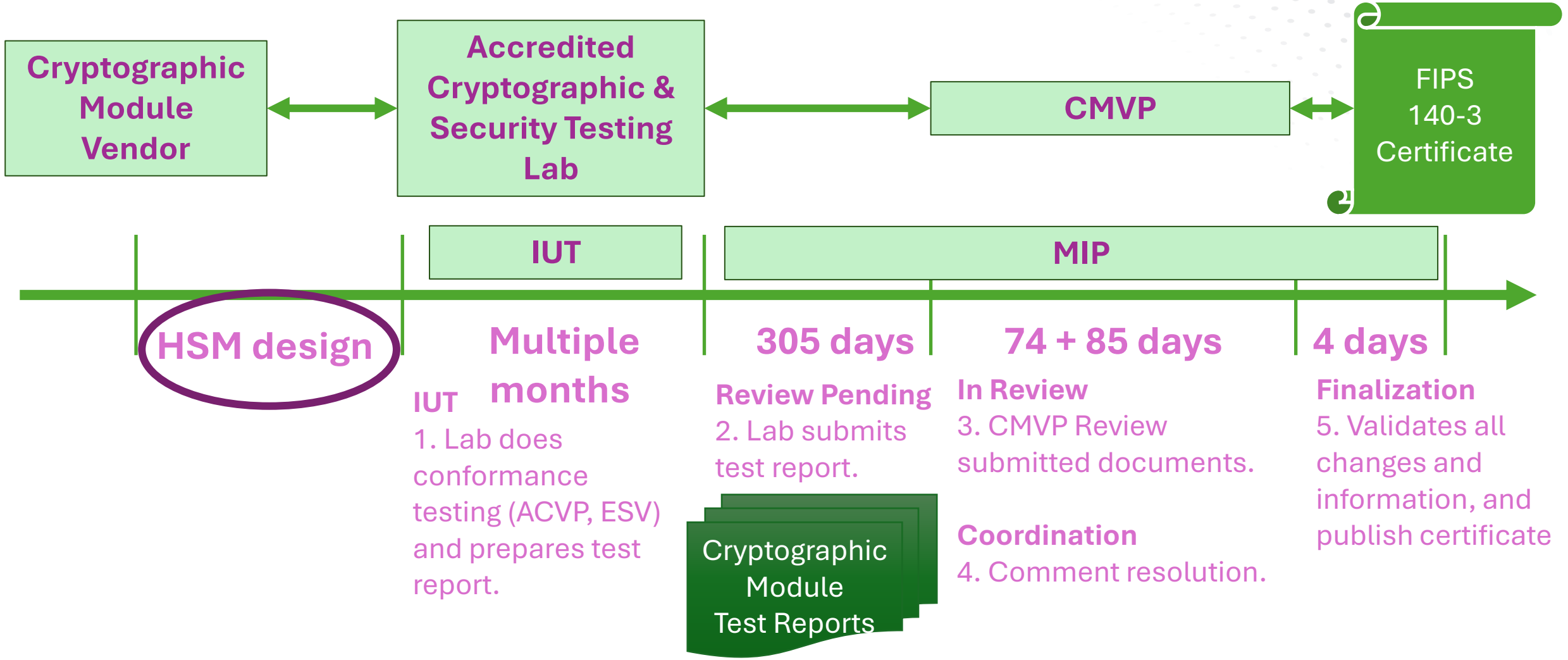
From the FIPS 140-3 Management Manual

FIPS Queue Times Statistics as of 03/03/2026

Comments | Subscribers (711) | Documents | Overview



FIPS 140-3 Certification Timeline



CRYPTO4A

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

HSM & PQC

Vendor	CAVP with PQC algorithms												
	LMS			ML-DSA (FIPS 204)			ML-KEM (FIPS 203)		SLH-DSA (FIPS 205)			Certificate #	Cert date
	KeyGen	SigGen	SigVer	KeyGen	SigGen	SigVer	KeyGen	EncapDecap	KeyGen	SigGen	SigVer		
Crypto4A (QASM)	x	x	x	x	x	x	x	x	x	x	x	A4204, A5631	14 Aug 2024
Entrust (nShield5)				x	x	x	x	x	x	x	x	A7285	30 July 2025
Fortanix (DSM Appliance)	x	x	x									A5344	22 May 2024
Futurex (GSP4000)				x	x	x	x	x				A7998	2 Feb 2026
i4p (Trident HSM)													
IBM (4770-001 CCA)													
Kryptus (ASI-HSM)				x	x	x	x	x				A6066	4 Nov 2024
Marvell (LS2 HSM)				x	x	x	x	x				A6877	1 May 2025
Securosys (Primus HSM)	x	x	x	x	x	x	x	x	x	x	x	A6129, A6130, A6131	7 Nov 2024
Thales TCT (Luna HSM - K7)	x	x	x	x	x	x	x	x				A7358	9 Feb 2025
Utimaco (u.Trust Anchor CSe)	x	x	x	x	x	x	x	x				A7400 A7401	17 Sep 2025

CRYPTO4A

HSM & FIPS

	ESV Certificate		CMVP Process			
Vendor	Certificate #	Date	IUT	MIP		Average days left
Crypto4A (QASM)	E96	11/27/2023		Comment Resolution	27 Feb 2026	15
Entrust (nShield5)	E38	4/11/2023	13 Jun 2025			
Fortanix (DSM Appliance)	E232	3/14/2025	28 Nov 2025			
Futurex (GSP4000)			27 Sep 2024			
i4p (Trident HSM)			7 Oct 2025			
IBM (4770-001 CCA)	multiple		14 Jan 2025			
Kryptus (ASI-HSM)				Review	26 Jan 2026	123
Marvell (LS2 HSM)	E231	3/3/2025	18 Mar 2024	Pending Review	29 Jan 2026	431
Securosys (Primus HSM)	E285	10/10/2025	17 Dec 2024	Cost Recovery	20 Feb 2026	469
Thales TCT (Luna HSM - K7)	E252	5/8/2025	28 Jan 2025			
Utimaco (u.Trust Anchor CSe)	E108	1/23/2024		Pending Review	13 Jan 2026	409

The complete picture

Vendor	CAVP with PQC algorithms													ESV Certificate		CMVP Process			
	LMS			ML-DSA (FIPS 204)			ML-KEM (FIPS 203)		SLH-DSA (FIPS 205)			Certificate #	Cert date	Certificate #	Date	IUT	MIP		Average days left
	KeyGen	SigGen	SigVer	KeyGen	SigGen	SigVer	KeyGen	EncapDecap	KeyGen	SigGen	SigVer								
Crypto4A (QASM)	x	x	x	x	x	x	x	x	x	x	x	A4204, A5631	14 Aug 2024	E96	11/27/2023		Comment Resolution	27 Feb 2026	15
Entrust (nShield5)				x	x	x	x	x	x	x	x	A7285	30 July 2025	E38	4/11/2023	13 Jun 2025			
Fortanix (DSM Appliance)	x	x	x									A5344	22 May 2024	E232	3/14/2025	28 Nov 2025			
Futurex (GSP4000)				x	x	x	x	x				A7998	2 Feb 2026			27 Sep 2024			
i4p (Trident HSM)																7 Oct 2025			
IBM (4770-001 CCA)														multiple		14 Jan 2025			
Kryptus (ASI-HSM)				x	x	x	x	x				A6066	4 Nov 2024				Review	26 Jan 2026	123
Marvell (LS2 HSM)				x	x	x	x	x				A6877	1 May 2025	E231	3/3/2025	18 Mar 2024	Pending Review	29 Jan 2026	431
Securosys (Primus HSM)	x	x	x	x	x	x	x	x	x	x	x	A6129, A6130, A6131	7 Nov 2024	E285	10/10/2025	17 Dec 2024	Cost Recovery	20 Feb 2026	469
Thales TCT (Luna HSM - K7)	x	x	x	x	x	x	x	x				A7358	9 Feb 2025	E252	5/8/2025	28 Jan 2025			
Utimaco (u.Trust Anchor CSe)	x	x	x	x	x	x	x	x				A7400 A7401	17 Sep 2025	E108	1/23/2024		Pending Review	13 Jan 2026	409

CRYPTO4A

References

- ESV https://csrc.nist.gov/projects/cryptographic-module-validation-program/entropy-validations/search?Vendor=crypto4a&ipp=25
- CAVP https://csrc.nist.gov/projects/cryptographic-algorithm-validation-program/validation-search?searchMode=validation&productType=-1&algorithm=176&ipp=25
- IUT: https://csrc.nist.gov/Projects/cryptographic-module-validation-program/modules-in-process/iut-list
- MIP:https://csrc.nist.gov/Projects/cryptographic-module-validation-program/modules-in-process/modules-in-process-list
- CMVP: https://csrc.nist.gov/Projects/cryptographic-module-validation-program/validated-modules/search

Cryptographic Module Validation Program CMVP

Entropy Source Validation Search

Certificate Number: E

Vendor: crypto4a

Implementation Name:

Description:

Noise Source Classification: All

Reuse Status: All

Validation Date / / to / /

Items Per Page 25

Search Reset

Showing **1** matching records.

Vendor	Implementation	Certificate Number	Validation Date
Crypto4A Technologies Inc.	Crypto4A QASM Entropy Source	E96	11/27/2023

Cryptographic Algorithm Validation Program CAVP

Search By ◉ Validation ○ Implementation

Validation Number Prefix | Number

Includes Algorithm(s)

- KMAC-128
- KMAC-256
- KTS-IFC
- LMS KeyGen

Validation Date / / — / /

Items Per Page 25

Search Reset

Showing **23** matching records.

Vendor	Implementation	Validation Number	Validation Date
Beijing JN TASS Technology Co., Ltd.	TASS CloudHSM SJJ1528	A7183	7/17/2025
Beijing JN TASS Technology Co., Ltd.	TASS Crypto Engine (LMS)	A6960	5/27/2025
Crypto4A Technologies, Inc.	QASM	A4204	7/14/2023
Crypto4A Technologies, Inc.	QASM Cryptographic Module	A5631	8/14/2024
Entrust Corporation	PQSDK	A7990	1/30/2026
Fortanix, Inc.	Fortanix Crypto Algorithm Library	A5344	5/22/2024
IDEMIA Secure Transactions	IDEMIA Sphere Cryptographic Library	A6961	5/28/2025
PQSecure Technologies, LLC	libpqsecure	A6936	5/20/2025
PQSecure Technologies, LLC	Libpqsecure-rs	A7616	10/29/2025
PUFsecurity Corporation	PUFpqc – PUF-based post quantum cryptography	A7029	6/11/2025
Securosys SA	Primus HSM firmware implementation	A7792	12/15/2025
Securosys SA	Primus HSM LMS aarch32 firmware implementation	A5703	9/4/2024
Securosys SA	Primus HSM LMS aarch64 firmware implementation	A5702	9/4/2024
Thales	Thales Luna K7 Cryptographic Library	A7358	9/2/2025
Thales Trusted Cyber Technologies	Luna M7 Firmware Cryptographic Library	A5021	1/30/2024

Cryptographic Module Validation Program CMVP

Implementation Under Test List

The IUT list is provided as a marketing service for vendors who have a viable contract with an accredited laboratory for the testing of a cryptographic module, and the module and required documentation is resident at the laboratory. The CMVP does not have detailed information about the specific cryptographic module or when the test report will be submitted to the CMVP for validation. When the lab submits the test report to the CMVP, the module will transition from the IUT list to the MIP list. If you would like more information about a specific cryptographic module or its schedule, please contact the vendor.

Last Updated: 3/9/2026

Module Name	Vendor Name	Standard	IUT Date
AMD Versal ACAP	Advanced Micro Devices (AMD)	FIPS 140-3	8/19/2025
Alibaba Cloud Crypto	Alibaba Cloud Computing Ltd.	FIPS 140-3	8/18/2025
Schlage Wireless Cryptographic Module	Allegion PLC	FIPS 140-3	7/23/2024
Alphawave Co-Wave AW400-O DSP	Alphawave Semi	FIPS 140-3	10/15/2025
AWS-LC 4 Cryptographic Module (Dynamic)	Amazon Web Services Inc.	FIPS 140-3	2/24/2026
AWS-LC 4 Cryptographic Module (Static)	Amazon Web Services Inc.	FIPS 140-3	2/24/2026
Amazon Linux 2023 Kernel Cryptographic API	Amazon Web Services, Inc.	FIPS 140-3	7/18/2025
AWS Key Management Service HSM	Amazon Web Services, Inc.	FIPS 140-3	11/8/2024
AWS Key Management Service HSM (2.2.0, h3.0)	Amazon Web Services, Inc.	FIPS 140-3	4/15/2025
AWS Key Management Service HSM (2.3.0, h3.0)	Amazon Web Services, Inc.	FIPS 140-3	4/15/2025
AWS Key Management Service HSM (2.3.0, h4.0)	Amazon Web Services, Inc.	FIPS 140-3	4/15/2025
AWS Nitro Ethernet Storage Encryption (ESE) Engine	Amazon Web Services, Inc.	FIPS 140-3	1/26/2026

PROJECT LINKS

Overview
FAQs
News & Updates
Publications

ADDITIONAL PAGES

Validated Modules
- Search
- Caveats

Modules In Process
- Modules In Process List
- Implementation Under Test List

Entropy Validations
- Entropy Source Validation Search
- Entropy Validation Announcements
- ESV
- Entropy Source Validation Workshop
- Entropy Validation Documents

Programmatic Transitions
CMVP FIPS 140-2 Management Manual
CMVP FIPS 140-2 Related References
CMVP FIPS 140-3 Management Manual
CMVP FIPS 140-3 Related References
FIPS 140-2 IG Announcements

Cryptographic Module Validation Program CMVP

Modules In Process List

The MIP list contains cryptographic modules on which the CMVP is actively working on. For a module to transition from Review Pending to In Review, the lab must first pay the NIST Cost Recovery fee, and then the report will be assigned as resources become available. The validation process is a joint effort between the CMVP, the laboratory and the vendor and therefore, for any given module, the action to respond could reside with the CMVP, the lab or the vendor. This list does not provide granularity into which entity has the action. The various circumstances that can trigger "On Hold" are stated in the FIPS 140-3 Management Manual, Section 4.3.4. For each submission, the status and the date it went into that state is listed. If you would like more information for a specific cryptographic module or its schedule, please contact the vendor.

Last Updated: 3/9/2026

Module Name	Vendor Name	Standard	Status
Samsung NVMe TCG Opal SSC SEDs PM9D3a Series	Samsung Electronics Co., Ltd.	FIPS 140-3	Pending Review (12/31/2025)
Samsung NVMe TCG Opal SSC SEDs PM9D3a Series	Samsung Electronics Co., Ltd.	FIPS 140-3	Pending Review (1/7/2026)
AMD ASP Cryptographic CoProcessor ("Strix 1" and "Krackan 1")	Advanced Micro Devices (AMD)	FIPS 140-3	Review (1/23/2026)
AMD ASP Cryptographic CoProcessor ("Strix Halo")	Advanced Micro Devices (AMD)	FIPS 140-3	Review (1/8/2026)
MESH SDR Cryptography Module	Codan | DTC	FIPS 140-3	Pending Review (9/6/2025)
Code Siren Post-Quantum Cryptographic (PQC) Library for Desktop	Code Siren, LLC	FIPS 140-3	Pending Review (2/13/2026)
Code Siren Post-Quantum Cryptographic (PQC) Library for Mobile	Code Siren, LLC	FIPS 140-3	Pending Review (2/19/2026)
Port Authority Series	Communication Devices Inc.	FIPS 140-3	Pending Review (1/15/2026)
CorSSL	Corsec Security, Inc.	FIPS 140-3	Pending Review (1/13/2026)
QASM Cryptographic Module	Crypto4A Technologies Inc.	FIPS 140-3	Comment Resolution - CMVP (2/27/2026)
Rocky Linux 8 and 9 GnuTLS Cryptographic Module	Ctrl IQ, Inc.	FIPS 140-3	Comment Resolution - Lab (1/20/2026)
Rocky Linux 8 and 9 NSS Cryptographic Module	Ctrl IQ, Inc.	FIPS 140-3	Comment Resolution - CMVP (3/5/2026)
Rocky Linux 8 OpenSSL Cryptographic Module	Ctrl IQ, Inc.	FIPS 140-3	Comment Resolution - CMVP (3/6/2026)
Rocky Linux 9 GnuTLS Cryptographic Module	Ctrl IQ, Inc.	FIPS 140-3	Pending Review (11/25/2025)

PROJECTS | CRYPTOGRAPHIC MODULE VALIDATION PROGRAM | VALIDATED MODULES

Cryptographic Module Validation Program CMVP

Search

All questions regarding the implementation and/or use of any validated cryptographic module should first be directed to the appropriate VENDOR point of contact (listed for each entry). General CMVP questions should be directed to cmvp@nist.gov.

Use this form to search for information on validated cryptographic modules.

Select the basic search type to search modules on the active validation list. Select the advanced search type to to search modules on the historical and revoked module lists.

Search Type: (•) Basic ( ) Advanced — Search | Reset | Show All

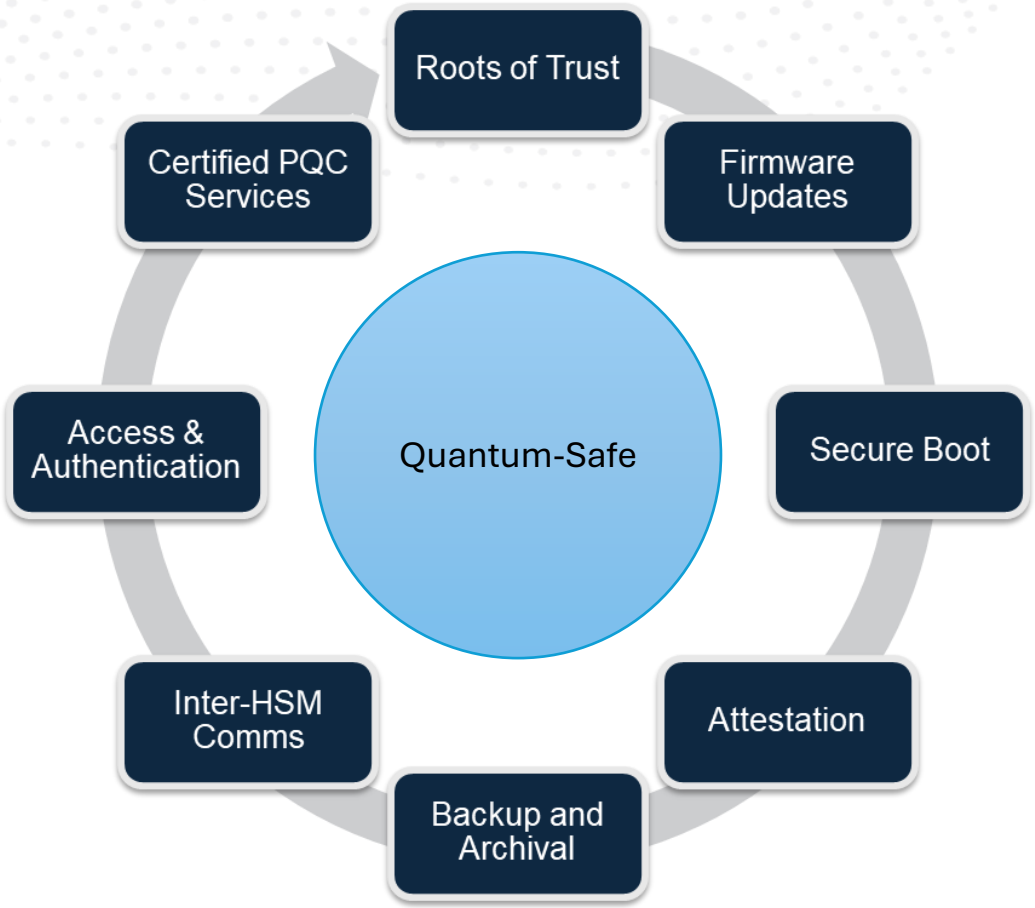
Certificate Number:

Vendor:

Module Name:

More Cool Things

What Makes an HSM Quantum Safe by Design?



CRYPTO4A

https://crypto4a.com/resources/docs/2026-01-08-what-makes-an-hsm-quantum-safe-by-design

Other Important characteristics

- Cryptographic Agility
- Crypto-Mobility
- Cloud, on-prem, off-line deployments
  - Design scalability
  - Attestation
- API: P#11, KSP, REST, GRPC…
- Work-flow automation

Standards Involvement

- NIST's NCCoE
  - Chaired the HSM interoperability working group
- NIST PQC standardization:
  - SP-800-208 (LMS & XMSS), FIPS 203, 204 & 205
- IETF:
  - Algorithms Composite (hackathons) – strong contributors
    - ML-DSA+RSA; ML-DSA + ECDSA; ML-DSA + Brainpool
    - ML-KEM + RSA; ML-KEM + ECDH*
  - RATS:
    - HSM definitions (authors)
  - PLANTS (contributors)
    - Merkle Tree, inclusion proof
  - SCITT (following)
- PKIC – Crypto Module Working Group
- PKCS#11

Crypto4A - QASM

CRYPTO4A

CRYPTO4A

Thank you

For more information please contact:

Bruno Couillard
CEO & Co-founder

bruno@crypto4A.com
www.crypto4A.com