Crypto4A Technologies Submits PQC-Capable QASM for FIPS 140-3 Level 3 Certification

An industry first and a major milestone to securing a post-quantum future.

OTTAWA, ONTARIO, CANADA, March 20, 2025 /EINPresswire.com/ -- Crypto4A Technologies, a pioneer in quantum-safe and crypto-agile security solutions, is excited to announce that its QASM hardware cryptographic core and v5.0 firmware —powering its QxHSM™ and QxEDGE™ products—has been added to the National Institute of Standards and Technology (NIST) Cryptographic Module Validation Program (CMVP) Module In Process (MIP) list for FIPS 140-3 Level 3 certification.

Designed, manufactured and assembled in Canada

Quantum-Safe and Crypto-Agile by design

Space and power savings with QxBMC-3 chassis

This submission marks a world-first milestone: QASM is the first Hardware Security Module (HSM) to be submitted for certification that includes all NIST-certified permutations and variants of the NIST Post-Quantum Cryptography (PQC) algorithms, including FIPS 203, 204, 205, and LMS. This ensures organizations are prepared to protect critical assets now and in the future against the evolving threat posed by advancements in quantum computing.

Crypto4A's quantum-safe HSMs are already trusted by major chip manufacturers, board and device manufacturers, cloud service providers, government agencies, and enterprise customers worldwide. As new quantum-safe algorithms are introduced by NIST, Crypto4A customers will be able to gain access to them through simple firmware updates, thanks to the company's crypto-agile FPGA-based design and quantum-safe firmware update mechanism. Unlike traditional

HSMs, only those with quantum-safe Roots of Trust can ensure firmware updates remain secure against potential quantum computer attacks.

“We are excited to have submitted our QASM design to the CMVP for FIPS 140-3 Level 3 certification with full PQC algorithm support, which marks a first for the HSM industry! Our PQC-enabled QASM serves as the core component of our QxHSM and QxEDGE product offerings, providing all of our customers with a quantum-safe foundation on which to embark on the PQC migration journey.”, said Dr. Jim Goodman, CTO & Co-founder, Crypto4A. “We are also very thankful for our partnership with atsec information security. Their extensive level of knowledge and expertise proved invaluable for ensuring that our implementation of the approved algorithms, and the security of our devices, met and exceeded the NIST FIPS standard.”

“We appreciate the opportunity and the trust that Crypto4A has put in the atsec Cryptographic Security Testing (CST) Laboratory for their FIPS validation needs. Crypto4A is our first vendor to receive algorithm certificates for all available PQC algorithms. Throughout the project, we witnessed professionalism, dedication, attention to detail, and a good understanding of FIPS requirements from the entire team, making the validation process seamless. We look forward to many collaborations for future validations,” said Swapneela Unkule, the atsec CST Lab Manager.

“This marks a significant milestone for the industry”, said Spencer Frye, VP Growth Strategy & Operations, CERTINext/eMudhra. “Quantum-safe enablement begins with the hardware, and Crypto4A is leading the way in making this a reality.”

"Crypto4A’s submission of the first quantum-safe HSM for FIPS 140-3 Level 3 certification demonstrates a forward-thinking approach to securing a post-quantum future," said Tim Hollebeek, Vice President of Industry Standards at DigiCert. "DigiCert shares in this vision and is committed to helping enterprises become quantum-ready through trusted digital trust solutions, including post-quantum cryptographic support, certificate lifecycle automation, and scalable PKI solutions that adapt to evolving security landscapes. We applaud Crypto4A’s leadership in advancing quantum-ready security and look forward to continuing our collaboration to safeguard digital trust in the post-quantum world."

“HSMs are essential for robust PKI and digital signature solutions in production environments. As we face tight deadlines for transitioning to post-quantum cryptography, collaboration is crucial to support migration efforts.” said Tomas Gustavsson, Chief PKI Officer at Keyfactor. “Our partnership with Crypto4A has been instrumental in enabling quantum-safe algorithms for our customers. By providing production-ready security infrastructure, we empower organizations and vendors to seamlessly integrate comprehensive quantum-safe solutions, ensuring long-term resilience against emerging threats.”

“This is an important step in the timeline of preparation for PQC. NIST’s initial call for PQC algorithm proposals was in 2016 which led to a release of standards in 2024. As part of the PKI ecosystem, HSM vendors have a critical role,” said Jason Soroko, senior fellow at Sectigo.

“Congratulations to Crypto4A. Their continued efforts in this space help organizations better prepare for the quantum threats of today and tomorrow.”

With over seven years of delivering quantum-safe HSMs to the market, Crypto4A continues to lead the way in cryptographic security for the post-quantum era. The company extends a special thanks to the team at atsec (https://www.atsec.com/) for their extensive certification knowledge and guidance in helping bring this submission to completion.

For more information on Crypto4A’s quantum-safe solutions, visit www.crypto4a.com.

Robert Grapes
Crypto4A Technologies, Inc.
+1 6132662323
email us here
Visit us on social media:
LinkedIn
