enQase Receives FIPS 140-3 Validation for Cryptographic Module

CMVP Certificate #5346 validates enQase's standards-based cryptographic module for networks, servers, appliances, edge devices, IoT, and enterprise applications

AUSTIN, TX, UNITED STATES, July 14, 2026 /EINPresswire.com/ -- enQase, a pioneer in quantum security and crypto-agility, today announced that the Cryptographic Module Validation Program (CMVP) has issued FIPS 140-3 Certificate #5346 for the enQase FIPS 140-3 Cryptographic Module.

enQase Cryptographic Module is FIPS 140-3 Validated, Certificate #5346

The certificate, issued under the Federal Information Processing Standard 140-3, confirms that the enQase FIPS 140-3 Cryptographic Module has completed the NIST (National Institute of Standards & Technology) CMVP validation process. The module is listed by CMVP as an active FIPS 140-3 validated software cryptographic module, with an Overall Level 1 validation.

> FIPS 140-3 validation is an important milestone for enQase and for organizations that require independently validated cryptographic capabilities"
>
> *Rajesh Patil, CEO, enQase*

The enQase FIPS 140-3 Cryptographic Module is a standards-based cryptographic engine for networks, servers, appliances, edge devices, IoT, and enterprise applications. The module delivers FIPS 140-3 cryptographic functions that can support secure implementation across supported platforms.

"FIPS 140-3 validation is an important milestone for enQase and for organizations that require independently validated cryptographic capabilities," said Rajesh Patil, CEO of enQase. "As enterprises, government agencies, and critical infrastructure providers prepare for a quantum-safe future, validated cryptographic modules are a foundational element of trust, compliance, and long-term security readiness."

FIPS 140-3 is the current U.S. government standard for security requirements for cryptographic modules. Validation under the CMVP provides organizations with a recognized basis for evaluating cryptographic modules used to protect sensitive information.

“Together with enQase’s portfolio of 15 U.S. and international patents, this certificate reinforces enQase’s commitment to both innovation and practical, standards-aligned quantum security solutions,” Patil added. “As customers work to modernize cryptographic infrastructure and prepare for post-quantum requirements, FIPS 140-3 validation gives them added confidence that enQase is building on a trusted and verifiable foundation.”

The enQase FIPS 140-3 Cryptographic Module was validated by DEKRA Cybersecurity Certification Laboratory, and is now fully activated.

To view the certificate, visit the NIST Computer Security Resource Center listing for Certificate #5346.

About enQase
enQase is a U.S.-based, full-stack quantum-safe security platform that unifies proven cryptography, physics-based quantum hardware, and a powerful software integration layer to deliver crypto agility for the quantum era.

The enQase Platform enables enterprises, defense organizations, cloud providers, and critical infrastructure operators to adopt quantum-safe technologies with minimal disruption, while maintaining business continuity and operational resilience.

By combining quantum-grade hardware with software-defined control and broad interoperability, enQase aligns with NIST standards, accelerates compliance readiness, and reduces risk across data, network, and compute layers in an evolving cryptographic landscape.

enQase
email us here
enQase Media Relations
