EINPRESSWIRE

Kiteworks Achieves FIPS 140-3 Validation, Expanding Comprehensive Compliance Portfolio

Enhanced cryptographic security addresses critical requirements for government agencies and regulated industries

SAN MATEO, CA, UNITED STATES, March 19, 2025 /EINPresswire.com/ -- Kiteworks, which empowers organizations to effectively manage risk in every send, share, receive, and use of private data, announced today that it has achieved Federal Information Processing Standard (FIPS) 140-3 validation for its cryptographic module, building upon its previous FIPS 140-2 certification. This milestone reinforces Kiteworks' commitment to providing the highest level of security for organizations that handle sensitive information, particularly those in regulated industries such as finance, pharmaceutical and life sciences, the defense industrial base, healthcare, and government.

> Achieving FIPS 140-3 validation represents a significant advancement in our security capabilities and demonstrates our unwavering commitment to protecting our customers' most sensitive data.”
>
> *Frank Balonis, CISO and SVP of Operations at Kiteworks*

The validation demonstrates Kiteworks has achieved FIPS 140-3 Level 1 compliance (excluding those sections that are not applicable) with Level 3 compliance in Life-Cycle Assurance. This validation ensures that Kiteworks' cryptographic implementation meets rigorous federal standards required for protecting sensitive information in U.S. federal agencies and Designated Information in Canada. For clients, this means their sensitive data receives protection that is officially recognized and validated by federal security authorities—a critical requirement for organizations subject to regulatory compliance.

"Achieving FIPS 140-3 validation represents a significant advancement in our security capabilities and demonstrates our unwavering commitment to protecting our customers' most sensitive data," said Frank Balonis, CISO and SVP of Operations at Kiteworks. "For our clients in government, healthcare, financial services, and defense sectors, this validation eliminates compliance barriers and provides assurance that their critical data is protected by cryptography that's recognized as effective by federal authorities. Without validated cryptography, sensitive information is considered by NIST to be essentially in plaintext form—completely vulnerable to compromise."

Kiteworks safeguards sensitive data through a multilayered protection framework featuring double encryption where files are encrypted at both the file level and the disk level using separate encryption keys. This approach requires attackers to breach multiple security layers and decrypt content using two different keys to access protected information.

Kiteworks' FIPS 140-3 validated cryptographic module operates exclusively in Approved mode, supporting a comprehensive suite of algorithms including AES (CBC, GCM, CCM, KW), SHA (1, 2, 3), HMAC, RSA, DSA, ECDSA, EDDSA, and various key derivation functions—all CAVP certified. Key generation follows SP 800-133 Rev. 2 guidelines, with random values produced by an internal Counter DRBG offering a minimum-security strength of 128 bits.

For encryption at rest, Kiteworks employs AES-256 encryption by default and supports FIPS 140-3 validated encryption. For encryption in transit, Kiteworks utilizes TLS 1.3 protocols. At the same time, Kiteworks Email Protection Gateway (EPG) extends this protection with S/MIME and OpenPGP encryption for email messages and attachments.

FIPS 140-3, published on March 22, 2019, supersedes FIPS 140-2 and aligns with the international ISO/IEC 19790:2012(E) standard. The standard establishes security requirements for cryptographic modules used within security systems that protect sensitive but unclassified information. Non-validated cryptography is viewed by NIST and the Canadian Centre for Cyber Security as providing no protection to information—equivalent to plaintext.

The FIPS 140-3 validation adds to Kiteworks' already impressive portfolio of compliance certifications, including FedRAMP High, IRAP (Australia), ISO 27001, ISO 27017, ISO 27018, SOC 2 Type II, and more. This comprehensive compliance coverage enables clients to satisfy multiple regulatory requirements with a single platform, significantly reducing the complexity and cost of maintaining separate solutions for different compliance mandates.

The achievement is particularly significant for Kiteworks' customers in the Defense Industrial Base (DIB) who must comply with the Cybersecurity Maturity Model Certification (CMMC) 2.0 requirements, as strong cryptographic controls are essential components of these regulations.

"This validation reinforces our position as a trusted security partner for organizations in highly regulated industries," added Balonis. "By implementing FIPS 140-3 validated cryptography within our Private Content Network, we're providing our customers with a solution that delivers tangible business benefits—streamlined procurement processes for government contractors, simplified compliance reporting, reduced audit scope, and fundamentally strengthened security against advanced threats targeting sensitive communications."

For more information about Kiteworks' FIPS 140-3 validation and its comprehensive approach to securing sensitive communications, visit kiteworks.com.

About Kiteworks
Kiteworks’ mission is to empower organizations to effectively manage risk in every send, share, receive, and save of sensitive content. The Kiteworks platform provides customers with a Private Content Network that unifies, tracks, controls, and secures sensitive content moving within, into, and out of their organization, significantly improving risk management and ensuring regulatory compliance on all sensitive content communications. Headquartered in Silicon Valley, Kiteworks protects over 100 million end users for over 35,000 global enterprises and government agencies.

David Schutzman
Kiteworks
+14083165255 ext.
email us here
Visit us on social media:
Facebook
X
LinkedIn
YouTube

This press release can be viewed online at: https://www.einpresswire.com/article/795036328