Quantum Computing Is Reshaping Cybersecurity — SpecterAI Urges Vietnam Enterprises to Prepare Now

SpecterAI Calls on Vietnam Businesses to Accelerate Quantum-Ready Digital Signature Security

SpecterAI

VIETNAM, May 7, 2026 /EINPresswire.com/ -- SpecterAI Quantum Security, a post-quantum cryptography (PQC) compliance testing and certification company operating across Vietnam and the Asia-Pacific region, has released the second instalment of its three-part intelligence brief series examining Vietnam's readiness for the post-quantum transition. Part 2 addresses the vulnerability of digital signature infrastructure to quantum-enabled attacks and outlines the steps Vietnamese enterprises must take to migrate to ML-DSA, standardized by the U.S. NIST as FIPS 204 in August 2024.

Digital signatures are the cryptographic mechanism that establishes the legal validity of electronic contracts, authorizes inter-bank settlement instructions, and authenticates regulatory filings submitted to Vietnamese government agencies. Current digital signature systems rely on RSA and ECDSA—algorithms that a sufficiently powerful quantum computer running Shor's algorithm could defeat, enabling an adversary to forge signatures or derive private signing keys from publicly available information. Unlike threats to encrypted data, where the harm is disclosure, a quantum attack on digital signatures introduces the risk of retroactive falsification: an adversary could manufacture signed documents or contest the validity of genuine ones. For enterprises with long-horizon contractual and regulatory records — financial institutions, insurers, infrastructure operators — this represents a systemic liability.

> The organizations that complete ML-DSA migration now will not merely be compliant — they will hold a verified cryptographic credential that positions them ahead of regional peers.”
>
> *Dr. Huynh*

The urgency for Vietnamese organizations is heightened by converging regulatory deadlines. Vietnam's Cybersecurity Law No. 116/2025/QH15, effective July 1, 2026, establishes binding

cryptographic requirements for operators of critical information infrastructure. Separately, State Bank of Vietnam Circulars 17 and 18/2024/TT-NHNN, which took effect July 01, 2024, require biometric authentication for digital banking transactions and control, and payment of recurring expenditures through the state treasury— an enforcement action that resulted in over 86 million bank accounts being deactivated for non-compliance, according to State Bank of Vietnam data reported in October 2025. At the international level, NIST IR 8547 sets 2030 as the target deadline for deprecating RSA and elliptic curve algorithms and 2035 as the absolute cutoff.

SpecterAI Quantum Security

The threat is not limited to Vietnam. Across the ASEAN region, post-quantum cryptography readiness varies significantly. Singapore has deployed Southeast Asia's first quantum-safe network infrastructure. Malaysia's National Cyber Security Agency (NACSA) issued a National PQC Readiness Roadmap in November 2025, explicitly targeting quantum-secure financial systems across ASEAN. The Lowy Institute noted in November 2025 that the ASEAN Digital Masterplan 2025 contains no reference to quantum security, leaving compliance to individual nations and enterprises. SpecterAI's analysis indicates that Vietnamese organizations completing ML-DSA migration within the next 12 to 18 months will carry a verifiable compliance credential that the majority of regional peers cannot yet claim — a differentiator relevant to correspondent banking relationships, foreign direct investment due diligence, and cross-border trade frameworks.

NIST FIPS 204 specifies ML-DSA in three parameter sets. ML-DSA-65, offering security equivalent to 192-bit classical encryption, is recommended for most enterprise and financial applications. Migration requires four structured phases: a cryptographic inventory to identify every location where digital signatures are generated or verified (including PKI certificates, API authentication tokens, document signing workflows, and hardware security modules); risk-based prioritization focused on high-value, long-retention signed records; library updates and parameter selection mapped to applicable Vietnamese and international standards; and independent third-party validation confirming mathematical correctness against FIPS 204 requirements. SpecterAI's SPECTER PQC Validation Platform, a proprietary compliance testing engine covered under multiple pending patents, evaluates ML-DSA implementations across 23 structured validation checks, including polynomial arithmetic, key generation, signature generation and verification,

and adversarial edge cases. When tested against FIPS 204, the platform achieved a 100 percent pass rate with a security margin exceeding NIST Category 3 requirements.

SpecterAI's Q1 2026 compliance scans of enterprise and financial sector infrastructure in Vietnam found that the majority of organizations continue to rely on RSA-2048 or elliptic curve signature variants, with several running cryptographic libraries that have not been updated in over 24 months, and none with a documented post-quantum migration roadmap.

Vietnam has been publicly identified as a target of nation-state advanced persistent threat (APT) groups including APT31, APT41, Mustang Panda, and SharpPanda, as reported by Vietnam's national cybersecurity authorities and confirmed by independent analysis from the University of Washington and the Australian Institute of International Affairs.

"Vietnam's enterprises are building one of the most ambitious digital identity and authentication infrastructures in Southeast Asia. The question is whether that infrastructure will be quantum-resistant or will require costly reconstruction within the decade,"

said Dr. Huynh Vinh Phuc, Chairman, APAC, SpecterAI Quantum Security.
"The organizations that complete ML-DSA migration now will not merely be compliant — they will hold a verified cryptographic credential that positions them ahead of regional peers in correspondent banking, investment due diligence, and cross-border digital trade,"
Dr. Huynh added.

About SpecterAI Quantum Security
SpecterAI Quantum Security is a post-quantum cryptography compliance testing and certification company operating across Vietnam and the Asia-Pacific region. The company's SPECTER PQC Validation Platform — covered under multiple pending patents across all six NIST-standardized PQC algorithm families — provides independent validation of ML-KEM, ML-DSA, SLH-DSA, and related post-quantum implementations against FIPS 203, FIPS 204, FIPS 205. SpecterAI operates in partnership with internationally accredited evaluation laboratories to provide compliance certification recognized across ASEAN, European, and U.S. regulatory frameworks.

Media Contact:
Dr. Huynh Vinh Phuc
Chairman, APAC, SpecterAI Quantum Security
www.specterai.ai | www.specterai.vn
Level 3, Cobi Tower II, No. 2-4 Street No. 8, Tan My Ward, District 7, Ho Chi Minh City, Vietnam

Huynh Vinh Phuc
Specter AI Quantum Security
+84 90 390 90 01
peter.huynh@specterai.vn

Visit us on social media:
LinkedIn
Facebook
YouTube
