Press Release

CryptoNext Security and ProvenRun Strengthen Their Strategic Alliance with Post-Quantum Integration into ProvenRun's New Hardware Security Module, ProvenHSM

CryptoNext Security and ProvenRun integrate post-quantum cryptography into ProvenHSM, delivering a crypto-agile, high-assurance hardware security module built for the quantum era.

Paris, France - April 2026

ProvenRun and CryptoNext Security are taking a significant step forward in their collaboration. The two companies announced the integration of CryptoNext Security's post-quantum cryptography (PQC) components into ProvenRun's next-generation Hardware Security Module, ProvenHSM, delivering unparalleled levels of protection for the most demanding environments.
This milestone marks an acceleration of the partnership initiated in 2025, confirming the shared ambition to provide the market with a fully integrated, high-assurance, end-to-end security stack built for the post-quantum era.

ProvenHSM: a crypto-agile HSM designed for the post-quantum transition
ProvenHSM builds on ProvenRun's established expertise in Trusted Execution Environments (TEEs) and formally verified operating systems. With the integration of CryptoNext Security's PQC technology, ProvenHSM demonstrates its capability to support post-quantum cryptography while maintaining strong operational security, providing:

- full crypto-agility,
- secure algorithm updates,
- end-to-end protection of cryptographic operations,
- and enhanced resilience against threats emerging from quantum computing.

Together, these capabilities provide a strong security foundation for industries where systems must remain secure for decades, including aerospace and defense, automotive, industry, semiconductors, and IoT.

A practical response to the quantum threat
As quantum computing capabilities advance, systems deployed today must remain secure for decades. CryptoNext Security's PQC technologies, rooted in over twenty-five years of academic research, enable organizations to prepare and transition smoothly toward

quantum-resilient cryptography. Their native integration into ProvenRun's HSM ensures customers benefit from:

- immediate protection,
- a gradual and controlled transition,
- and long-term cryptographic durability for embedded infrastructures.

Supporting the quantum transition with a flexible ecosystem

As quantum computing progresses, systems deployed today must remain secure throughout long operational lifetimes. Post-quantum cryptography provides mechanisms to prepare for this transition while maintaining compatibility with existing infrastructures. Integrating CryptoNext Security's PQC technology within ProvenHSM allows organizations to test, adopt, and deploy quantum-resilient cryptography within a secure, flexible, and crypto-agile architecture.

Quotes

"ProvenRun is the right partner to bring our vision of crypto-agility to critical embedded systems. Embedding our technologies within their new ProvenHSM delivers a post-quantum-ready security foundation that industries can rely on for the long term."
- Jean-Charles Faugère, Founder, CryptoNext Security

"After a productive first year of collaboration, we are entering a decisive new stage. Integrating CryptoNext Security's PQC technologies into our ProvenHSM creates a fully-trusted, end-to-end security solution tailored to the most demanding embedded environments."
- Thierry Chesnais, CEO, ProvenRun

About CryptoNext Security

Founded in 2019 and built on over 25 years of academic research, CryptoNext Security is a software vendor which helps organizations transition to quantum-resilient cybersecurity by managing cryptographic risks and long-term compliance. Its solutions enable organizations to inventory, migrate to Post-Quantum Cryptography (PQC), and manage cryptography in a fast-evolving security landscape. CryptoNext Security serves major players in finance, defense, industry, and government, where long-term cryptographic security is mission-critical.

For more information, please visit https://www.cryptonext-security.com

About ProvenRun

ProvenRun is a security software company specializing in high-assurance embedded systems and trusted computing. For over 15 years, it has delivered secure-by-design solutions for mission-critical environments across defense, avionics, automotive, and industrial markets. Building on its expertise in formally verified operating systems and isolation mechanisms, ProvenRun extends its high-assurance approach with ProvenHSM, enabling hardware-rooted trust and strong cryptographic guarantees for modern and regulated digital services.

For more information, visit https://www.provenrun.com

Media Contacts

CryptoNext Security
Nicolas Drouault – Head of Marketing & Communication
nicolas.drouault@cryptonext-security.com

ProvenRun
Vinicius Malta – Head of Marketing
vinicius.malta@provenrun.com