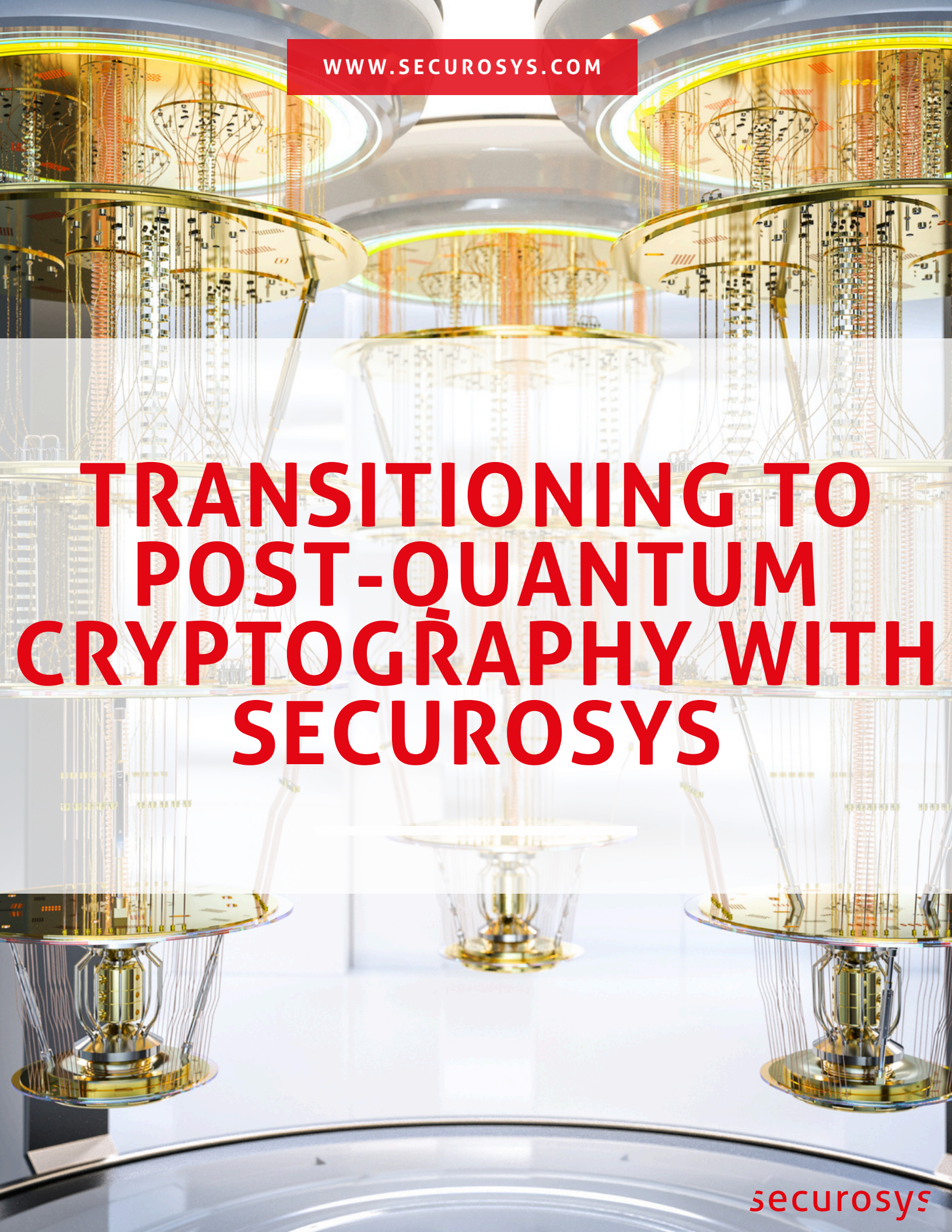


WWW.SECUROSYS.COM

TRANSITIONING TO POST-QUANTUM CRYPTOGRAPHY WITH SECUROSYS

securosys

EXECUTIVE SUMMARY

The arrival of NIST's official Post-Quantum Cryptography (PQC) standards marked a significant milestone in the global effort to safeguard digital infrastructure against future quantum computing threats. Quantum computers are now a fast-approaching reality , and they will be capable of breaking classical cryptographic systems such as RSA and ECC within the decade. As industries prepare for this seismic shift, Securosys is already delivering the tools needed to transition confidently.

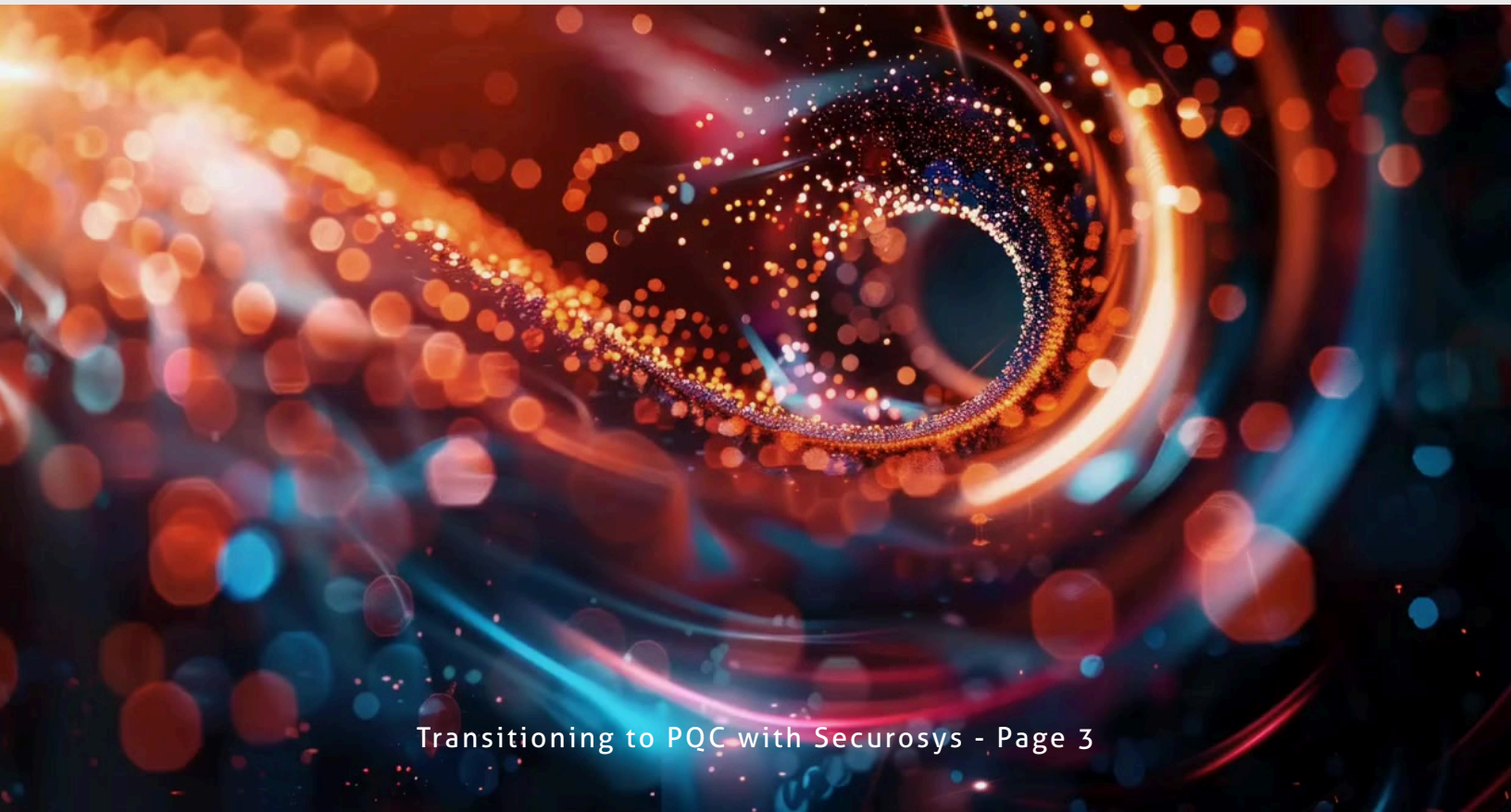
This white paper explores how Securosys Primus HSMs, including the advanced Primus HSM CyberVault and CloudHSM services, are enabling organizations to adopt quantum-safe cryptography today. Featuring hybrid cryptographic operations, high-speed performance, and flexible testing environments, Securosys' PQC-ready infrastructure ensures you can future-proof your security while maintaining operational continuity. With collaborative research from HSLU validating real-world PQC integration, this paper provides a roadmap and practical guidance for embracing the post-quantum era.

INTRODUCTION

Quantum computing represents a paradigm shift in data security. Once capable enough, these machines will render today's encryption schemes vulnerable, threatening everything from financial transactions to state secrets. Compounding this risk is the growing concern of "harvest now, decrypt later" attacks—where encrypted data is stolen today with the intent of decrypting it once quantum capabilities emerge.

In July 2024, NIST released its finalized PQC algorithms — ML-KEM (Kyber), ML-DSA (Dilithium), and SLH-DSA (SPHINCS+), along with other important schemes like HSS-LMS and XMSS — setting a global standard for quantum-safe cryptography.

This shift highlights the need for timely action. Cryptographic transitions are complex and take time, often years. Organizations that manage sensitive data or long-term confidentiality requirements must begin adopting PQC mechanisms now.



SECUROSYS: AHEAD OF THE CURVE

In the face of this quantum challenge, Securosys stands out as a leader in preparing for the next era of cryptographic security. Recognizing the need for quantum-resistant solutions, Securosys has been proactively developing products designed to make the transition to the Quantum era as smooth as possible. In 2024, we launched the Primus HSM CyberVault, our most advanced Hardware Security Module (HSM), which incorporates built-in quantum-threat resistance.

The Primus HSM CyberVault is not just a response to the future — it is a solution for the present. It supports both current encryption methods and the newly introduced quantum-safe algorithms, making it ideal for hybrid use during this transitional period. This capability ensures that our customers can protect their data now while being fully prepared for the post-quantum era. The device's ability to operate over 50,000 concurrent transactions per second (tps) and over 1,000,000 concurrent tps in clustered environments, offering high availability and global geo-redundancy, underscores its readiness to meet the demands of modern, large-scale deployments.

THE TRANSITION TO QUANTUM-SAFE ENCRYPTION

We understand that the shift to quantum-safe encryption is not just about being prepared for the future — it's about ensuring continuity and security during the transition phase. The Primus HSM CyberVault is specifically designed with this challenge in mind. It enables the use of both traditional and post-quantum algorithms, providing a seamless transition path for organizations as they adapt to new standards. To support this migration journey, we also offer a dedicated test environment through our CloudHSM platform. This allows cybersecurity professionals, developers, and tech teams to explore our PQC capabilities in a risk-free setup, ideal for experimentation and planning.

Key Features of Primus CyberVault

- **Hybrid Cryptography:** Combines classical algorithms (RSA, ECC/ED) with NIST-Selected PQC algorithms for a flexible and secure transition strategy.
- **Optimized Performance for PQC:** Handles larger key sizes and signatures required by PQC while maintaining high-speed cryptographic operations.
- **High Availability & Scalability:** Supports over 50,000 transactions per second (TPS) per device, and over 1,000,000 TPS in clustered setups with global geo-redundancy.
- **Flexible Deployment:** Available as an on-premises HSM or cloud-native via our CloudHSM offering — ensuring security wherever your data resides.
- **Quantum-Safe Key Management**: Full support for ML-KEM, ML-DSA, SLH-DSA, HSS-LMS, and XMSS.

PQC IN TLS: JOINT RESEARCH WITH HSLU

To ensure practical and measurable adoption of PQC, Securosys is also working closely with academic leaders. In collaboration with Prof. Dr. Esther Hänggi and her team at the Lucerne University of Applied Sciences and Arts (HSLU), we are researching PQC performance in real-world scenarios.

Focus Areas

- **TLS Performance Under Stress**: Analyzing PQC algorithm behavior in TLS handshakes under conditions like packet loss and network latency.
- **Authentication & Key Exchange**: Exploring PQC's suitability for robust authentication in unpredictable or degraded network environments.

This research guides optimizations in our own HSM implementations and helps customers understand the operational impacts of transitioning to quantum-safe infrastructure.

Watch the video to learn more about the project.

securosys

ROADMAP TO PQC READINESS

STEP 1

ASSESS CRYPTOGRAPHIC INVENTORY

Map all cryptographic systems, certificates, and protocols in use.

STEP 2

DEFINE CONFIDENTIALITY REQUIREMENTS

If your data needs to remain secure for more than 5 years, it's time to prepare for PQC.

STEP 3

DEPLOY HYBRID CRYPTOGRAPHY

Use Securosys HSMs to run legacy and PQC algorithms concurrently to ensure backward compatibility.

STEP 4

TEST IN A CONTROLLED ENVIRONMENT

Leverage Securosys CloudHSM SBX to test TLS integrations, key exchange mechanisms, and certificate lifecycles.

STEP 5

MIGRATE AT SCALE

Confidently deploy PQC with production-grade CloudHSM or on-prem HSMs, backed by our experts and detailed documentation.

CONCLUSION

A Quantum-Safe Future Starts Now

Waiting is no longer an option. Whether you're a bank, infrastructure provider, or cloud-native business, the ability to keep your data secure in the next years depends on decisions you make now.
With Securosys, you don't just prepare for the future — you implement it. The Primus HSM CyberVault and Securosys CloudHSM are your foundation for post-quantum security.

At Securosys, we're already protecting the future of data. Are you?

WWW.SECUROSYS.COM/CONTACT

ABOUT US

Securosys SA, headquartered in Zurich, Switzerland, is a renowned industry leader specializing in cybersecurity, encryption, as well as digital identity and online keys protection. Founded in 2014, Securosys' hardware security modules (HSMs) secure transactions exceeding 100 billion euros daily on the Swiss banking system SIC (under the supervision of the Swiss National Bank) as well as the Swiss stock exchanges SIX and SDX. Over half of the world's Tier 1 banks and numerous technology companies trust the HSMs developed and manufactured by Securosys in Switzerland.

Securosys' comprehensive HSM solutions, available both on-premises and as a service in the cloud, are certified to the highest security standards, including FIPS and Common Criteria. Designed for diverse industries including finance, healthcare, and government, Securosys HSMs offer unparalleled features such as independent, cryptographically secure partitions, patented policy-based individual key protection, and cloud readiness. The devices support hybrid signatures, ensuring a seamless transition from classical to post-quantum cryptographic (PQC) algorithms.