enQase

USE CASE

Revolutionize 5G Security

enQase delivers quantum-safe solution that meet the performance demands of transaction processing systems.

> ENQASE.COM

Challenge

enQase offers a quantum-safe solution for 5G networks that combines rapid deployment, cost-effectiveness, and unparalleled flexibility. enQase QRNG leverages quantum mechanics to generate truly random numbers, ensuring unpredictable, high-quality keys at rates up to XX gigabits per second, to meet high-throughput TPS demands.

enQase's Quantum Random Number Generator (QRNG) offers robust quantum-safe protection, dramatically enhancing both the security and efficiency of telecom transaction processing systems (TPS). By addressing critical vulnerabilities such as weak key generation and entropy starvation, our solution empowers telecoms to stay ahead of emerging quantum threats while optimizing network performance.

The telecommunications industry faces unprecedented challenges as quantum computing rapidly evolves, posing a significant threat to current encryption methods. This transformative technology necessitates a swift transition to quantum-resistant or a more robust, future proof quantum-safe encryption.

Key challenges

- Imminent Quantum Threats: Quantum computers are advancing rapidly and could soon break current encryption methods, putting sensitive data at risk.
- Critical Infrastructure Protection: Telecom networks, essential for national security, finance, and personal communications, are prime targets for quantum attacks.
- Harvest Now, Decrypt Later" Attacks: Adversaries are already collecting encrypted data to decrypt when quantum computers become available, threatening long-term data security.
- Regulatory Compliance: The U.S. Government has mandated quantum-safe security measures to be in place by 2030 at the latest, as per the U.S. Quantum Computing Cybersecurity Preparedness Act.

A breach of AT&T that exposed "nearly all" of the company's customers may have included records related to confidential FBI sources, potentially explaining the bureau's new embrace of end-to-end encryption.

Wire Magazine, January 16, 2025

Implementation Challenges:
Navigating the Quantum-Safe Transition

While the need for quantum-safe encryption is clear, the path to implementation is fraught with obstacles. Most products offered are standalone technologies rather than comprehensive solutions leading to several challenges:

- Security gaps: Layering technologies from different suppliers that aren't engineering to work seamlessly together risk creating interoperability issues and maintenance-driven security gaps.
- Network Performance Impacts: Quantum-safe solutions can hamper Transaction Processing Systems, impacting customer experience, and negatively impacting corporate brand and revenue.
- Legacy systems Compatibility: Ensuring interoperability between quantum-safe and legacy systems during the transition period can be challenging, especially when technologies come from different developers. This can result in compatibility issues and disruptions to existing workflows.
- Deployment and Management Complexities: A mix of technology providers adds significant complexity to management.
- Cost and Resources: Transitioning to quantum-safe systems requires investment in new technologies and expertise to manage a mix of solutions and suppliers.

Quantum-Safe Protection for 5G Networks and Transaction Processing Systems

enQase QRNG delivers quantum-safe protection, revolutionizing the security and efficiency of transaction processing systems (TPS) for telecom providers. This comprehensive solution tackles critical vulnerabilities, particularly weak key generation and entropy starvation. enQase stands out as the only quantum-safe solution with all components developed in-house, ensuring seamless interoperability and eliminating potential security gaps often associated with multi-vendor solutions. This unified approach not only enhances security but also streamlines operations, providing telecom operators with a powerful, user-friendly platform to safeguard their infrastructure against both current and future quantum threats.

enQase Improved Key Generation

QRNG Technology – A Superior Source of Randomness for Cryptographic Key Generation

- True Randomness for Unparalleled Security: This quantum phenomena ensures the generation of unpredictable and high-quality keys, forming an impenetrable foundation
- Enhanced Security: Keys generated leveraging enQase QRNG demonstrate quantum-safe resistance to attacks and vulnerabilities. The robustness surpasses the security offered by Post-Quantum Cryptography (PQC) encryption relying on conventional pseudo-random number generators.
- Future-Proof: enQase QRNG-generated keys offer comprehensive protection against both classical and quantum computing threats. This dual-threat safety ensures long-term data security, safeguarding sensitive data.

Addressing Entropy Starvation

Entropy starvation, a common issue in high-volume transaction systems, can be effectively mitigated using enQase QRNG. Ou quantum-based solution offers several key advantages:

- High-Speed Generation: enQase QRNGs can produce random numbers at rates up to XX gigabits per second, meeting the demands of even the most intensive high-throughput Transaction Processing Systems (TPS). This speed ensures that cryptographic operations never suffer from a lack of entropy, even under extreme loads.
- Continuous Entropy Supply: Unlike traditional random number generators that may experience periods of low entropy, enQase QRNGs provide a non-blocking source of entropy. This ensures a constant supply of high-quality randomness for cryptographic operations
- Scalability: QRNG technology can be easily integrated into existing systems, offering scalable solutions for entropy generation.

Enhanced TPS Security – Now Quantum Safe

Implementing enQase QRNG in TPS offers several security benefits:

- Robust Encryption: enQase QRNG enables the creation of stronger encryption keys, enhancing the overall security of transactions.
- Improved Authentication: enQase QRNGs can be used to generate one-time passwords (OTPs) and other authentication tokens with higher security.
- Secure Communication: enQase QRNGs support quantum key distribution (QKD) systems, enabling ultra-secure communication channels for sensitive transactions

enQase Unique Implementation Advantages

Telecoms can benefit from enQase QRNG implementation in several ways:

- Hardware Integration: QRNG chips can be embedded directly into devices, providing local generation of high-quality entropy.
- Cloud-Based Solutions: enQase QRNG-as-a-service offerings allow telecoms to access quantum randomness without significant infrastructure changes.
- Performance Boost: Using QRNG can improve the speed and efficiency of cryptographic operations, potentially increasing TPS throughput.
- Simplified and unified Management Console: The enQase solution, hardware and software can be managed by a simple management console, eliminating the burdensome complexities and costs from network administrators of managing multiple suppliers.

By adopting enQase QRNG-based quantum-safe protection, telecoms can significantly enhance the security and reliability of their TPS, addressing the critical issues of weak key generation and entropy starvation while preparing for future quantum computing threats.

By choosing the highest and most secure quantum-safe approach, telecoms can ensure the strongest possible protection against both current and future threats. This proactive stance not only secures critical infrastructure but also builds trust with customers and positions companies as leaders in the evolving landscape of cybersecurity.

A New Jam-Packed Biden Executive Order Tackles Cybersecurity, AI, and More

The order requires software vendors to submit proof that they follow secure development practices, building on a mandate that debuted in 2022 in response to Biden's first cyber executive order. The Cybersecurity and Infrastructure Security Agency would be tasked with double-checking these security attestations and working with vendors to fix any problems. To put some teeth behind the requirement, the White House's Office of the National Cyber Director is "encouraged to refer attestations that fail validation to the Attorney General" for potential investigation and prosecution.

Wire Magazine, January 15, 2025