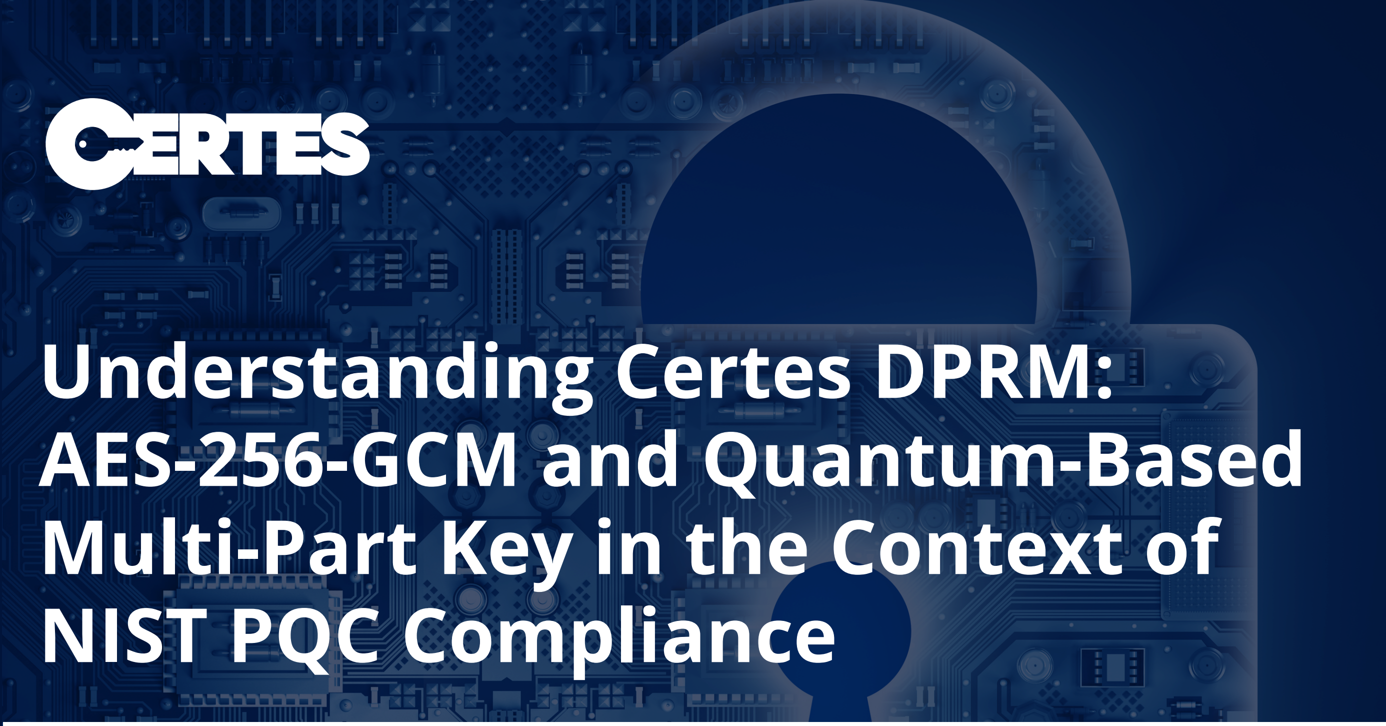

Understanding Certes DPRM: AES-256-GCM and Quantum-Based Multi-Part Key in the Context of NIST PQC Compliance

As quantum computing looms on the horizon, the need for cryptographic systems resilient to quantum threats has never been more urgent. The National Institute of Standards and Technology (NIST) has been leading the charge with its post-quantum cryptography (PQC) standardization efforts, providing a roadmap for securing data in a quantum future. In this article, we delve into how Certes DPRM—Data Protection and Risk Mitigation—utilizing its AES-256-GCM algorithm and quantum multi-part key (combining amongst other things a true quantum random number and unique customer key material) , aligns with NIST's PQC compliance framework as of March 10, 2025.

The Quantum Threat and NIST's PQC Initiative

Quantum computers threaten traditional cryptography through algorithms like Shor's, which can break asymmetric systems such as RSA and ECC, and Grover's, which halves the effective security of symmetric keys.
For instance, a 256-bit symmetric key offers only 128 bits of security against a quantum adversary. To address this, NIST launched its PQC standardization process in 2016, finalizing its first standards—FIPS 203 (ML-KEM), FIPS 204 (ML-DSA), and FIPS 205 (SLH-DSA)—on August 13, 2024. These focus on quantum-resistant asymmetric algorithms, but NIST also provides guidance on symmetric cryptography's role in a post-quantum world, which is crucial for evaluating systems like Certes DPRM.

> **"Cybercriminals target data, not networks. Financial records, customer details, and intellectual property are the real assets at risk, making data protection the top cybersecurity priority."**
>
> *Paul German – CEO, Certes*

What is Certes DPRM?

Certes DPRM (Data Protection and Risk Mitigation) is a data in motion cryptographic solution designed to safeguard sensitive data against current and emerging threats, including those from quantum computing. It employs AES-256-GCM (Advanced Encryption Standard with 256-bit keys in Galois/Counter Mode) for symmetric encryption and incorporates a quantum-based multi-part key mechanism to enhance security.

AES-256-GCM: Quantum Resistance and NIST's Perspective

AES-256-GCM is a symmetric encryption scheme combining the AES block cipher with a 256-bit key and GCM for authenticated encryption. While Shor's algorithm targets asymmetric cryptography, Grover's algorithm impacts symmetric systems by reducing key strength. For AES-256, this translates to 128 bits of security in a quantum context —still a formidable barrier.

NIST's stance on symmetric cryptography in its PQC FAQs is reassuring: AES with 128, 192, or 256-bit keys remains suitable for use, with no immediate need to transition unless security drops below 112 bits classically (or roughly 56 bits quantumly). AES-256's 128-bit quantum security far exceeds this, making it quantum-resistant under NIST's current guidance. Additionally, its endorsement in standards like the NSA's CNSA suite underscores its reliability for high-security applications.

Thus, AES-256-GCM, as the core of Certes DPRM, aligns with NIST's PQC framework, offering robust protection against quantum threats when properly implemented.

Quantum-Based Multi-Part Key: Strengthening Security

The quantum-based multi-part key is a distinctive feature of Certes DPRM, enhancing key generation, key ownership and management. This ensures the sovereignty of the customers data irrespective of the network infrastructure it travels over.

Quantum Randomness

"Quantum-based" refers to true quantum random number generation (QRNG), it leverages quantum mechanics to produce truly unpredictable keys for AES-256-GCM. NIST emphasizes high-quality randomness (e.g., SP 800-90 series), and QRNG aligns with this by providing entropy resistant to both classical and quantum attacks. This bolsters the system's overall security without requiring a shift away from symmetric encryption.

Multi-Part Key Design

The “multi-part” aspect suggests key splitting or threshold cryptography, where the AES-256 key is divided into segments, requiring multiple parts to reconstruct it. This distributes risk—compromising one part doesn’t break the system—and enhances resilience. While NIST’s PQC standards (FIPS 203–205) target asymmetric cryptography, they don’t restrict symmetric key management innovations. Guidelines like SP 800-57 support such techniques, and the multi-part key integrates a quantum-resistant distribution method that is a patented capability of Certes DPRM.

> **Quantum randomness isn't just theory - Certes leverages true quantum random number generation (QRNG) for unbeatable unpredictability**
>
> *Simon Pamplin – CTO, Certes*

PQC Compliance

Since NIST’s PQC standards focus on public-key systems, symmetric key management falls under existing frameworks unless quantum vulnerabilities emerge. The quantum-based multi-part key in Certes DPRM complements AES-256-GCM’s quantum resistance, potentially exceeding NIST’s baseline by incorporating advanced, quantum-aware techniques. It thus supports PQC compliance by enhancing security without introducing weaknesses.

Certes DPRM in the NIST PQC Ecosystem

As of March 10, 2025, NIST’s PQC standard address asymmetric needs (e.g., key encapsulation via ML-KEM), but symmetric algorithms like AES-256 remain vital in hybrid systems. NIST encourages pairing AES-256 with PQC algorithms for comprehensive security—Certes DPRM fits this model with its multi-part key Coupled with a NIST-approved method for distribution. Even standalone, its AES-256-GCM core meets NIST’s quantum resistance criteria, while the multi-part key adds a forward-thinking layer aligned with PQC’s proactive ethos.

Critical Considerations and Future Outlook

Pairing its AES-256-GCM and multi-part key with NIST's PQC standards (e.g., ML-KEM for key exchange) makes Certes DPRM a benchmark for quantum-resistant data protection.

Conclusion

Certes DPRM—Data Protection and Risk Mitigation—with its AES-256-GCM algorithm and quantum-based multi-part key, is PQC-compliant per NIST's framework as of March 10, 2025. AES-256-GCM delivers 128 bits of quantum security, exceeding NIST's symmetric encryption threshold, while the quantum-based multi-part key enhances this with innovative key management, leveraging quantum randomness or threshold techniques. Certes DPRM aligns with NIST symmetric guidance and complements the broader transition to a quantum-safe world.

For organizations seeking robust data protection amid quantum uncertainty, Certes DPRM offers a compelling, NIST-aligned solution—bridging today's security needs with tomorrow's challenges.

Contact Certes

300 Corporate Center Drive,
Suite 140 Pittsburgh, PA 15108

1 (888) 833-1142
sales@certes.ai

CERTES