Protecting AI Traffic with Certes DPRM: A Symmetric Quantum-Safe Solution

In the rapidly evolving landscape of artificial intelligence (AI), securing data in transit is essential to safeguard against threats like data poisoning and man-in-the-middle (MITM) attacks. As quantum computing looms on the near horizon, traditional cryptographic methods face new vulnerabilities, driving the need for quantum-safe alternatives. Certes DPRM, a symmetric quantum-safe form of data protection offers a robust and efficient way to protect AI traffic. This paper explains how Certes DPRM works and how it defends against these threats, ensuring the integrity and confidentiality of AI data.

What is Certes DPRM?

Certes DPRM is a cryptographic solution designed to secure data in a quantum-safe manner. Here's what sets it apart:

- Symmetric Cryptography: It uses a single shared secret key per individual data flow for both encryption and decryption with individual rotation schedules, unlike asymmetric systems (e.g., RSA) that rely on public-private key pairs. This symmetry makes it faster and more efficient, ideal for the high-volume data flows in AI applications. The granular level and regular rotation of the key makes this even more secure and prevents lateral movement from one flow to another.

- Quantum-Safe: Symmetric algorithms like AES-256-GCM, are resistant to quantum computer attacks (as verified by NIST) when paired with sufficiently large keys. Quantum computers pose little threat to these systems, ensuring long-term security.

> **With symmetric algorithms like AES-256-GCM, Certes DPRM is built to resist even the most advanced quantum computing threats, ensuring long-term data protection.**
>
> *Paul German – CEO, Certes*

- No Certificates: Traditional systems like TLS use digital certificates for authentication making them vulnerable to attacks, but Certes DPRM skips this complexity. Instead, it relies on pre-shared secret keys, streamlining the process while maintaining strong protection.

This combination makes the post-quantum-computing (PQC) compliant Certes DPRM a lightweight yet powerful tool for securing AI traffic against both current and future threats.

The Threats to AI Traffic

AI systems depend on vast datasets and real-time data streams, making them prime targets for cyberattacks. Two key threats stand out:

Data Poisoning
Data poisoning involves tampering with data to corrupt AI models. For example, in federated learning—where multiple devices collaboratively train a model—attackers could inject malicious updates to skew the model's outputs. Protecting data integrity during transit is critical to prevent this.

Man-in-the-Middle (MITM) Attacks
In an MITM attack, an adversary intercepts data between two parties, such as a data source and an AI system. This allows them to eavesdrop or alter the data, potentially feeding false inputs to the AI or stealing sensitive information. Confidentiality and tamper detection are vital to thwart such attacks.

How Certes DPRM Protects AI Traffic

Certes DPRM leverages symmetric quantum-safe cryptography combined with PQC compliant protected key material delivery to provide three essential protections: confidentiality, integrity, and efficiency.

1. Confidentiality: Keeping Data Secure

Certes DPRM encrypts individual data flows using a unique shared secret key, ensuring that only authorized parties with the key can decrypt it. If an attacker intercepts AI traffic—say, model updates or input data—they'll see only meaningless ciphertext. This blocks MITM attackers from reading or modifying the data. The primary algorithm used for data in transit is based on the current NIST standard recommendation. As of February 2025 NIST considers AES-256-GCM to be sufficiently robust as to be able to resist quantum computer attacks for the foreseeable future. Since symmetric encryption like AES-256-GCM remains secure against quantum computers, Certes DPRM offers future-proof confidentiality.

2. Integrity: Preventing Tampering

To combat data poisoning, Certes DPRM ensures data remains unchanged in transit. It can pair encryption with message authentication codes (MACs) or use authenticated encryption modes (e.g., AES-GCM) to verify integrity. If an attacker tries to alter the data—such as injecting poisoned inputs—the integrity check fails, alerting the system to reject the compromised data. This keeps AI models safe from manipulation.

3. Efficiency: Supporting AI Workloads

AI traffic often involves large datasets and real-time processing, requiring a lightweight security solution. Symmetric cryptography is computationally faster than asymmetric alternatives, making Certes DPRM ideal for encrypting and decrypting data without slowing down AI workflows. This efficiency is a key advantage for applications like real-time analytics or cloud-based AI services.

Practical Examples

Federated Learning

In federated learning, devices send encrypted model updates to a central server. Certes DPRM secures these updates with its shared-key encryption, ensuring attackers can't decipher or tamper with them. Any attempt to inject poisoned data would be detected by integrity checks, preserving the model's accuracy.

Cloud-Based AI

When users send data to cloud-hosted AI systems (e.g, for speech recognition), Certes DPRM encypts then inputs. This prevents MITM attackers from intercepting or altering the data, ensuring the AI processes only legitimate requests.

The Role of Key Management

Symmetric cryptography's strength lies in it's shared secret key, but this also makes key management critical. The key must be securely exchanged between parties and protected from unauthorized access. Certes DPRM uses patented techniques to distribute kay material (not the key itself) with PCQ wrapper - uniquely Certes DPRM never send the exposed key over the network, ensuring only authorized entities can enrypt or decrypt data. Robust key management underpins it's defences against both data poisoning and MITM attacks.

> **As quantum computing advances, traditional cryptographic methods are becoming increasingly vulnerable. Certes DPRM offers a future-proof, quantum-safe solution that ensures AI data stays secure—today and tomorrow.**
>
> *Paul German – CEO, Certes*

Conclusion

Certes DPRM, a symmetric quantum-safe form of data protection that avoids the use of certificates, is a powerful solution for securing AI traffic. By encrypting data with a shared secret key, it ensures confidentiality against MITM attacks and verifies integrity to block data poisoning. It's efficiency supports the demands of AI workloads, while it's quantum-safe design prepares it for the future. For organizations relying on AI, Certes DPRM offers a streamlined, secure way to protect data in transit, safeguarding both performance and trust in a quantum-threatened world.

Contact Certes

300 Corporate Center Drive,
Suite 140 Pittsburgh, PA 15108

1 (888) 833-1142

sales@certes.ai