Leading the Charge Towards Quantum-Safe Data Protection

Certes stands as a pioneer in safeguarding sensitive data against emerging threats, particularly those posed by quantum computing advancements. Certes current deployed algorithms include AES-256-GCM – this is widely accepted as 'Quantum Safe'* – The ETSI (European Standards Organisation) states "AES is considered quantum-safe because the cipher can adapt to a quantum attack by increasing its key size to rectify a vulnerability introduced by quantum computing."

Certes has utilized Quantum physics in the generation of its Key material for many years, our approach to data protection deploys separate (multi-part) keys with separate key rotation schedules to each policy-controlled data flow. The combination of a Quantum Safe algorithm combined with unique regularly rotated keys per data flow makes Certes able to qualify as currently Quantum Safe.

The existence of widespread harvest now, decrypt later Ransomware As A Service (RaaS) has been seen as a motivation for the early introduction of post-quantum algorithms, as data recorded now may remain sensitive many years into the future. Because of the regularly rotated keys per dataflow Certes defends against this by not only being Quantum Safe but also changing the key every 60 minutes to ensure that efforts carried out to break one key will not expose all keys.

Certes software architecture is abstracted from any specific application, as new algorithms are certified for public use we will QA/test and release via software upgrade – as a result, Certes is Crypto-Agile** and fully positioned for the post-quantum era.

"By seamlessly integrating quantum principles into our data protection strategies and employing regular key rotation, we're not only quantum-safe but also future-proofing our solutions against emerging threats."

Simon Pamplin – CTO, Certes

**As cryptographic algorithms are deployed, researching their security intensifies, and new attacks against cryptographic primitives (old and new alike) are discovered in short intervals.

Crypto-agility tries to tackle the implied threat to information security by allowing swift deprecation of vulnerable primitives and replacement by new ones.
*Post-quantum cryptography (PQC), sometimes referred to as quantum-proof, quantum-safe, or quantum-resistant, is the development of cryptographic algorithms that are thought to be secure against a cryptanalytic attack by a quantum computer. While as of 2024, quantum computers lack the processing power to break widely used cryptographic algorithms, cryptographers are designing new algorithms to prepare for Q-Day, the day when current algorithms will be vulnerable to quantum computing attacks.

Key Highlights:

Summary

Certes employs AES-256-GCM, acknowledged as "Quantum Safe" by ETSI due to its adaptability against quantum attacks. Quantum physics has long informed our key generation. Our data protection strategy involves multi-part keys with separate rotation schedules, ensuring quantum safety. Regular key rotation, combined with AES, mitigates the threat of Ransomware As A Service. Certes' abstract software architecture facilitates swift integration of new algorithms, ensuring crypto-agility and readiness for the post-quantum era.

Contact Certes
300 Corporate Center Drive,
Suite 140 Pittsburgh, PA 15108
1 (888) 833-1142
sales@certes.ai