

## INDUSTRY'S FIRST AND ONLY QUANTUM-PROOF ENCRYPTED COMMUNICATION PLATFORM



### THE QUANTUM THREAT LANDSCAPE

Quantum computing holds immense potential for advancements in healthcare, scientific research, and artificial intelligence. However, it also poses significant cybersecurity risks, particularly to cryptographic algorithms, such as RSA, rendering sensitive data vulnerable.



#### Harvest Now, Decrypt Later (HNDL) Attacks

Cybercriminals can acquire encrypted data today, anticipating future decryption with quantum computers.



#### Quantum Power

A 4,099-qubit quantum computer could crack RSA 2048 encryption in just 10 seconds (QuintessenceLabs).



#### Timeline

Asymmetric encryption may become unsafe by 2029 and fully breakable by 2034 (Gartner).

### THE QUANTUM-PROOF SOLUTION

To combat these emerging threats, post-quantum cryptography (PQC), also known as quantum-proof, quantum-safe, or quantum-resistant encryption has been developed. PQC leverages advanced quantum frameworks to secure data against quantum attacks. In a groundbreaking effort, the U.S. Department of Commerce's **National Institute of Standards and Technology (NIST)** has finalized a fundamental set of *Post-Quantum Cryptography Standardization* to protect systems from the risks posed by quantum computing.

# NetSfere's Quantum-Proof Encryption Advantage

**NetSfere**, a global leader in next-generation secure and compliant messaging and mobility solutions, offers the industry's first Quantum-Proof Secure Communication Platform, powered by ML-KEM 1024 (Module-Lattice-Based Key-Encapsulation Mechanism - an evolution of CRYSTALS-Kyber) quantum-safe encryption.



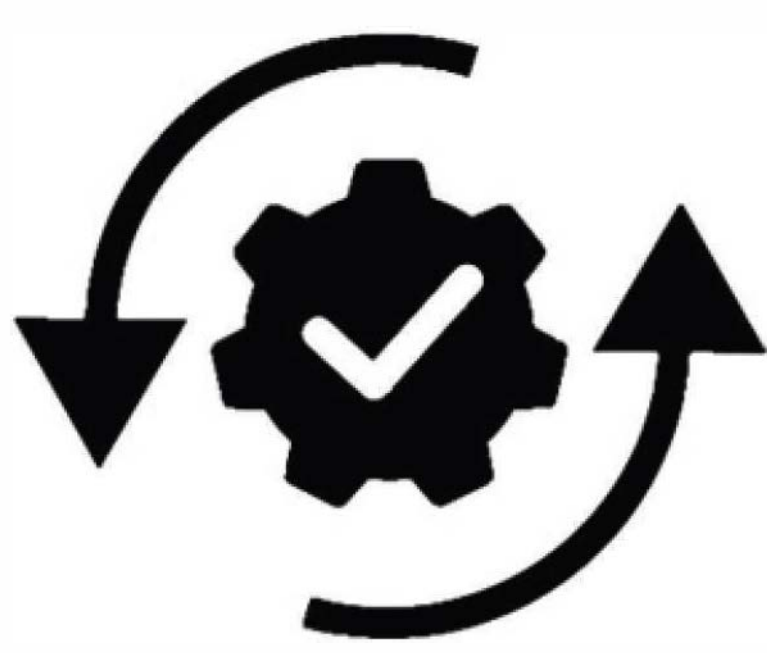
## **Modular Architecture:**

Facilitates easy updates and integration of emerging quantum-safe encryption standards.



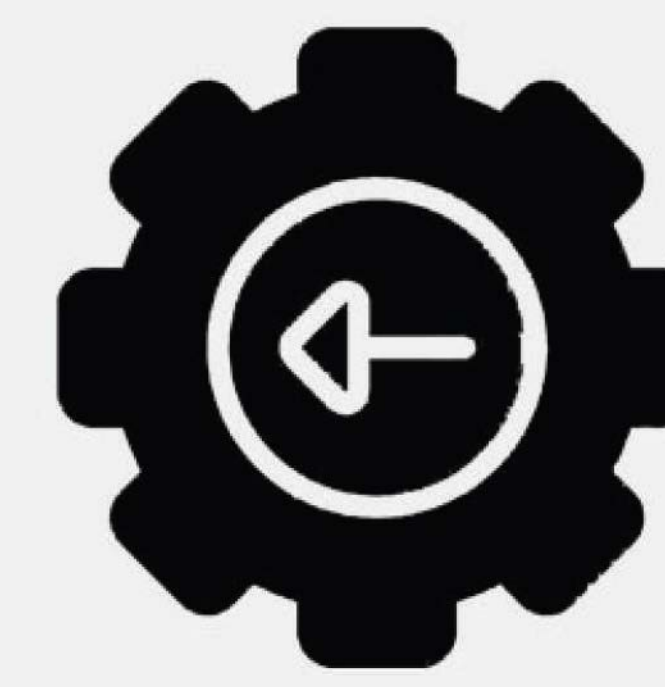
## **Standard Compliance:**

Ensures secure implementation of quantum-safe cryptography.



## **Automated Updates:**

Continuous updates of cryptographic algorithms, keys, and certificates.



## **Backward Compatibility:**

Seamless interaction between new quantum-proof encryption and legacy systems.



## **Enhanced Security:**

ECC upgraded to ML-KEM 1024, the strongest quantum-proof key allowed by today's standards.



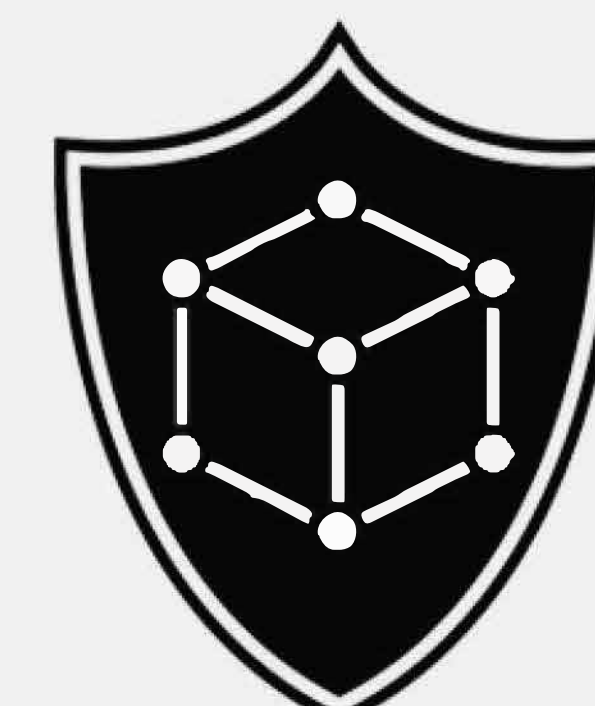
## **Quantum-Safe AES-256:**

Provides strong encryption alongside newer quantum-safe protocols.



## **Seamless Communication:**

ECC backward compatibility ensures smooth transitions to quantum-safe security.



## **Rust-based ML-KEM 1024 Implementation:**

Offers memory safety, high security, and cross-platform compatibility.

## Secure Your Communication with NetSfere

Quantum computing is on the horizon, and the time to prepare is now. With NetSfere's quantum-safe cryptography, enterprises can ensure their data remains protected against the threats of today and tomorrow. By adopting advanced quantum-proof encryption, businesses can safeguard sensitive information and maintain robust security in the face of evolving cyber threats.