ECHOWORX™

TECHNOLOGY BRIEF

Echoworx Post Quantum Cryptography Readiness

Echoworx recognizes the emerging cybersecurity risks associated with advances in quantum computing and is actively preparing its platform for the transition to post-quantum cryptography (PQC). Through a comprehensive assessment of our cryptographic architecture, we have established a roadmap aligned with industry standards and best practices for adopting quantum-resistant cryptographic technologies.

Our objective is to ensure long-term protection of customer communications while maintaining the security, reliability, and interoperability that organizations expect from the Echoworx platform.

Current Security Posture

Echoworx employs industry-standard cryptographic controls to protect customer communications and sensitive information. We have assessed the major cryptographic communication paths across our platform, including:

- Secure message delivery workflows
- Certificate-based trust services
- Key management infrastructure
- Supporting cryptographic services

This assessment has enabled us to identify areas that will ultimately require migration to quantum-resistant cryptography as standards mature and ecosystem support become broadly available.

Our Post-Quantum Strategy

Echoworx's approach to post-quantum cryptography is built on four key principles:

Crypto Agility

Our platform is designed to support the evolution of cryptographic standards, enabling the adoption of new algorithms and security technologies with minimal disruption to customers and integrations.

Hybrid Cryptography

Echoworx plans to adopt hybrid cryptographic approaches that combine established classical cryptography with post-quantum algorithms. This approach provides strong security while maintaining compatibility with existing technologies and industry ecosystems.

Standards Alignment

Our roadmap aligns with emerging industry standards, including post-quantum cryptography standards published by the U.S. National Institute of Standards and Technology (NIST), as well as related developments across internet and messaging security standards bodies.

Ecosystem Readiness

We are introducing post-quantum capabilities in alignment with the maturity of the broader technology ecosystem, including cloud platforms, certificate authorities, email clients, browsers, and cryptographic libraries. This approach ensures interoperability and minimizes risk during the transition.

Areas of Focus

Post quantum cryptography primarily addresses vulnerabilities in public-key cryptography (for example RSA and ECC), which are commonly used for key exchange, digital signatures, and certificate-based trust. These are the areas where a sufficiently powerful quantum computer could potentially weaken today's cryptographic protections.

Our post-quantum roadmap includes the adoption of quantum-resistant capabilities across key security technologies used within the platform, including:

- TLS-protected communications
- PGP-based secure messaging
- S/MIME certificate and trust services

These capabilities will be introduced through a phased approach that prioritizes customer security, compatibility, and operational stability.

Password-protected PDF messages rely on AES-based encryption for protecting the document contents and are therefore not a primary focus of our post-quantum roadmap.

Portal messages use both AES (symmetric encryption) and S/MIME. While the message content is ultimately protected using AES encryption, the overall portal message workflow incorporates S/MIME-based encryption and supporting key-management services as part of the message processing and storage architecture. As a result, elements of the portal message workflow are included within our broader post-quantum readiness assessment and roadmap.

What This Means for Customers

Customers do not need to take any action at this time.

Echoworx continues to monitor developments in post-quantum cryptography and is actively preparing for the adoption of quantum-resistant technologies as industry standards and supporting ecosystems mature. Our goal is to provide a seamless transition that strengthens long-term security without disrupting existing customer workflows, integrations, or user experiences.