Embargoed until July 24, 2025, 11:00 a.m. (UTC)

Press Release

Cryptomator Paves the Way for a Post-Quantum-Secure Future

Open-source encryption solution adopts new standards to defend against quantum computer threats

Bonn, Germany – July 24, 2025 – **Skymatic GmbH**, developer of the open-source encryption software Cryptomator, today announces its plan to **fully secure its software against threats posed by quantum computers**. The core of this initiative is the integration of **post-quantum cryptographic algorithms**, including the new NIST standards ML-KEM and ML-DSA, as well as a combination of classical and post-quantum-secure algorithms known as X-Wing.

“Although quantum computers are not yet capable of cracking the key lengths used today, the time to act is now. ‘There is no glory in prevention’ also applies to IT security.” – Sebastian Stenzel, CTO of Skymatic

The Challenge: Quantum Computers and Cryptography

While symmetric algorithms such as AES are still considered secure with sufficiently large key sizes—especially when using AES-256—new algorithms like **Shor’s algorithm** are undermining asymmetric methods like RSA and ECDH. This development calls for new cryptographic standards.

The Solution: Post-Quantum Cryptography

Cryptomator Hub, the collaboration solution for managing encrypted cloud data, will implement **hybrid encryption** going forward: classical methods will be combined with post-quantum algorithms—similar to putting two locks on a door. The **new technology is based in part on the X-Wing algorithm**, which is already being implemented in hardware by Apple and Google.

The Cryptomator team is also working on **integrating the HPKE** (Hybrid Public Key Encryption) standard based on X-Wing, and on **adapting the JWE** (JSON Web Encryption) format used to transmit encrypted user data. The goal is to ensure maximum compatibility and cryptographic agility.

Standardization as a Cornerstone

Another key objective is to **standardize the so-called vault format**, which defines the structure of encrypted directories. In cooperation with other open-source projects such as **Cyberduck, gocryptfs, and rclone**, Cryptomator is working on a unified format for encrypted folders—to promote interoperability and user-friendliness.

Open Source and Transparency

As with all its developments, Skymatic is committed to full transparency: **all code remains open source**, and the community is invited to review and comment on the new cryptographic components.

“The open source concept is deeply rooted in our company, which is why we have always contributed code to other projects. We are currently in close contact with the RFC authors of future standards such as X-Wing and are implementing these for OpenJDK and JWT libraries, among others.” – Sebastian Stenzel, CTO of Skymatic

Embargoed until July 24, 2025, 11:00 a.m. (UTC)

Availability

The new cryptographic features will be **gradually integrated into Cryptomator Hub**. Initial experimental releases with X-Wing and HPKE are still planned for **2025**.

About Skymatic and Cryptomator

Skymatic is a Germany-based company headquartered in Bonn, dedicated to making privacy solutions accessible to everyone. With Cryptomator, the company offers a highly acclaimed open-source software for client-side encryption of cloud data, used by millions of people worldwide.

Related Links

- Post-Quantum Roadmap: https://cryptomator.org/blog/2025/07/24/post-quantum-roadmap/
- Cryptomator: https://cryptomator.org
- Press Kit: https://cryptomator.org/presskit/
- Skymatic: https://skymatic.de

Press Contact

Kerstin Steiner
kerstin.steiner@skymatic.de