PRESS RELEASE
PiQASO Publishes First Core Technical Deliverable on Post-Quantum Cryptographic Primitives

12/05/2026, by Savvoula Oikonomou, UBITECH

ATHENS, Greece – The PiQASO project has published D3.1, its first core technical deliverable, titled *PiQASO QR Crypto Primitives Design, Optimization and Acceleration*. Led by Tampere University and with major contributions from UBITECH and Bundeswehr University Munich and produced through contributions from nine consortium partners, the document establishes the cryptographic baseline for the PiQASO's post-quantum security framework.

What D3.1 covers

D3.1 defines the design and theoretical foundations of the PiQASO PQC Ensemble, the collection of cryptographic tools and services that the project is developing to enable organisations to migrate from classical to quantum-resistant cryptography without disrupting existing operations. The deliverable covers four areas:

1) **The architecture and building blocks of the PiQASO framework.** D3.1 describes the three main components through which PiQASO delivers post-quantum capabilities: a Software Library containing optimised implementations of NIST-standardised algorithms ML-KEM and ML-DSA; a Quantum-Resistant Trusted Computing Base (QR-TCB), which is a hardware-anchored environment for securely executing cryptographic operations; and a PQC-as-a-Service modality, which allows devices with limited computational capacity to offload cryptographic operations to a secure backend.
2) **The forward security for cloud storage.** D3.1 introduces PiQASO's approach to protecting data stored in the cloud over long time horizons. The scheme is based on Updatable Public Key Encryption (UPKE) and is particularly relevant for sectors such as healthcare, energy, and transport, where data is retained for years and the "harvest now, decrypt later" threat is a realistic concern.
3) **Functional Encryption, with the introduction of ACE of SPADE** (AoS), a novel lattice-based scheme developed by the PiQASO consortium. Functional Encryption allows computations to be performed directly on encrypted data, revealing only the result rather than the underlying sensitive information. As a practical example, a healthcare system could determine whether a patient's heart rate exceeds a clinical threshold without the backend platform ever accessing the raw measurement data.
4) **Hardware and software optimisation.** D3.1 details PiQASO's Software/Hardware co-design approach, which combines algorithmic software optimisations with hardware acceleration.

The deliverable is publicly available on the PiQASO website. The final version of this deliverable is expected by June 2026.

Co-funded by the European Union
ECCC

Disclaimer

The PiQASO project is funded by the European Union and supported by the European Cybersecurity Competence Centre. By uniting academic rigor with industrial expertise, PiQASO is laying the foundation for a secure, quantum-resistant future.

For more information on the project's latest developments, visit our website: www.piqasoproject.eu

PIQASO Email: info@piqasoproject.eu

About PiQASO

PiQASO : *Post-Quantum Cryptography As-a-Service for Common Transmission Systems and Infrastructures* is a European collaborative project developing agile, service-based PQC solutions to protect critical digital infrastructures against future quantum threats. The project is co-funded by the European Union and supported by the European Cybersecurity Competence Centre (ECCC).

The project is co-funded by the European union, funded under Grant Agreement No. 101190366 and is supported by the European Cybersecurity Competence Centre.