# Introducing EQUIP

## European QUantum-safe Implementations for security and Performance

NOVEMBER 2026

**The Horizon Europe project "EQUIP" will advance secure, efficient and certifiable implementations of post-quantum cryptography across embedded microcontrollers, application-class processors and hardware platforms.**

Quantum computing is progressing rapidly, creating a long-term threat to the public-key cryptography that protects digital infrastructure, connected products and sensitive information. Europe therefore needs to move towards post-quantum cryptography (PQC), while ensuring that new algorithms remain secure not only in theory but also in real devices exposed to side-channel and fault-injection attacks.

EQUIP addresses this challenge through a coordinated, cross-disciplinary approach spanning algorithm design, countermeasure development, hardware and software implementation, attack analysis, testing, certification and legal compliance. The project connects the full design-evaluate-attack cycle so that advances in one area directly inform and strengthen the others. Its work will support practical deployment in application areas ranging from IoT and automotive systems to cloud services.

**The key innovations and aims of EQUIP are:**

- Systematise the fragmented state of the art through taxonomies, metrics and gap analyses for secure PQC implementations, countermeasures and attacks.
- Develop reproducible and highly automated testing and self-assessment procedures, including objective PASS/FAIL criteria, to support alignment with the Cyber Resilience Act and EU Cybersecurity Certification.
- Create new paradigms for efficient countermeasures and adapt PQC algorithms so that side-channel and fault protection can be integrated with substantially lower overhead.
- Deliver reproducible implementations of key-encapsulation and digital-signature schemes across microcontrollers, application-class CPUs and FPGA-based hardware, targeting technology readiness level 4.
- Analyse side-channel, fault-injection and combined attacks under realistic conditions, using the results to continuously refine countermeasures, testing methods and security metrics.
- Maximise uptake through open and verifiable artefacts, scientific dissemination, training, exploitation and contributions to European and international standardisation.

EQUIP is a 36-month project funded by the European Union under Grant Agreement No. 101308625. The consortium brings together six partners from five European countries: Technikon Forschungs- und Planungsgesellschaft mbH (Austria), KU Leuven (Belgium), CryptoExperts (France), PQShield (The Netherlands), Tampere University (Finland) and Graz University of Technology (Austria). Three universities, two deep-tech SMEs and one industrial partner combine complementary expertise in cryptographic design, physical-attack security, secure hardware and software implementation, testing, certification, standardisation and project exploitation.

By transforming isolated research activities into a unified innovation ecosystem, EQUIP will help make PQC implementation security measurable, reproducible and deployment-ready. Its results are expected to strengthen Europe's cybersecurity resilience, semiconductor industry, technological sovereignty and capacity to deliver trustworthy quantum-safe products and services.

*About the coordinator: Technikon is a private research service company based in Austria with extensive experience in coordinating and communicating technology-oriented European collaborative research projects. As coordinator of EQUIP, Technikon is responsible for administrative, financial and organisational management and drives the project's communication, dissemination and exploitation activities.*

For more information about EQUIP, please contact the project coordinator:

CONTACT: Barbara Gaggl
E-MAIL: coordination@horizon-equip.eu
PHONE: +43 4242 233 55 85
WEB: https://horizon-equip.eu

Funded by the European Union
ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

The project funded by the European Union under Grant Agreement No. 101308625 is supported by the European Cybersecurity Competence Centre. Views and opinions expressed are, however, those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Competence Centre. Neither the European Union nor the European Cybersecurity Competence Centre can be held responsible for them.