Draft outline for possible cooperation in the application under

Post-quantum cryptography transition
HORIZON-CL3-2024-CS-01-02

Tentative title: Secure PQC implementations in support of electronic signature related trust services

<SigneQ – tentative acronym>

Project description:

The goal of the project is twofold.

One is to develop a modular system for automatic evaluation and testing of post-quantum cryptography algorithms. The project deliverables address the needs of various expert groups involved in the development and/or assessment of cryptographic schemes. In the initial stages of algorithm construction, formal verification of security proofs and estimation of computational problem complexity shall be applied, and such deliverable would serve the need. Further, support for testers of cryptographic modules will include non-invasive methods of assessing the occurrence of side-channel leakage, according to ISO/IEC 17825. Thus, possible extension of ISO/IEC 17825 towards post-quantum cryptographic algorithms is expected as the deliverable of the project. Such extension allows to offer automated methods for determining the potentials of cryptographic attacks according to AVA_VAN levels within the Common Criteria IT security evaluation framework.

All deliverables will be verified using hardware implementations of post-quantum algorithms.

Second, with the solid estimation of robustness of PQC algorithms, a preparation to develop a full-scale implementation in the secure system providing the qualified server signature to users should be performed in testing and then in limited production environment (trial) of one of the trust service provider.

Potential participants:

(vacat1): Developing the PQC test implementations utilizing FPGA and RISC-V

(vacat2) Development of non-invasive methods and tools for attacks on PQC implementations

NIT (Poland): Conducting formal verification of PQC algorithms and developing evaluation methods based on the work

(Trust service provider, Poland or possibly affiliate from other MS): preparation for full-scale implementation based on work of other participants and development of trial

Analysis of expected outcome compliance by the European Commission resulted from the call:

- Increasing the maturity of current post-quantum cryptographic algorithms and contribution to further standardisation; - yes

- Easy-to-use tools for the large-scale implementation of post-quantum cryptographic algorithms, based on state-of-the-art standards; - yes
- Secure and efficient transition from pre- to post-quantum encryption through tools implementing a hybrid approach combining recognised pre-quantum public key algorithms and additional post-quantum algorithms; - not planned yet
- Phase-in of post-quantum algorithms or protocols to new or existing applications; -yes
- Demonstrators and good-practice implementations of post-quantum cryptographic algorithms on varied hardware and software platforms - yes
- Application-oriented recommendations for the widespread implementation of post-quantum cryptography across the EU -yes