HORIZON-CL3-2025-02-CS-06: Integration of Post-Quantum Cryptography (PQC) algorithms into protocols

Call: HORIZON-CL3-2025-02 Civil Security for Society	
Specific conditions	
Expected EU contribution per project	The Commission estimates that an EU contribution of between EUR 2.00 and 3.00 million would allow these outcomes to be addressed appropriately. Nonetheless, this does not preclude submission and selection of a proposal requesting different amounts.
Indicative budget	The total indicative budget for the topic is EUR 6.00 million.
Type of Action	Research and Innovation Actions
Eligibility conditions	The conditions are described in General Annex B. The following exceptions apply: In order to achieve the expected outcomes, and safeguard the Union's strategic assets, interests, autonomy, and security, participation in this topic is limited to legal entities established in Member States and Associated Countries. In order to guarantee the protection of the strategic interests of the Union and its Member States, entities established in an eligible country listed above, but which are directly or indirectly controlled by a non-eligible country or by a non-eligible country entity, may not participate in the action. Some activities, resulting from this topic, may involve using classified background and/or producing of security sensitive results (EUCI and SEN). Please refer to the related provisions in section B Security — EU classified and sensitive information of the General Annexes.
Legal and financial set-up of the Grant Agreements	The rules are described in General Annex G. The following exceptions apply: Eligible costs will take the form of a lump sum as defined in the Decision of 7 July 2021 authorising the use of lump sum contributions under the Horizon Europe Programme – the Framework Programme for Research and Innovation (2021-2027) – and in actions under the Research and

	Training Programme of the European Atomic Energy Community (2021-2025). [1].

Expected Outcome: Proposals shall address at least to one of the following expected outcomes:

- Design and implementations of at least one post-quantum cryptography protocol along with a security analysis demonstrating that no security is lost;
- Submission of these post-quantum cryptography protocols to standardization bodies and/or submission of the specification and implementation to the respective open source projects;
- Requirements analysis highlighting roadblocks and needs for development of post-quantum cryptography solutions for missing building blocks;

Scope: The transition to post-quantum cryptography requires changing all uses of cryptography. Research and development efforts have provided signature systems and key-exchange mechanisms that are generally accepted to withstand attacks using quantum computers. Efforts are on the way to include these in core Internet applications such as Transport Layer Security (TLS). While this is an important development, many more protocols need to be modified to be quantum-ready. Various application areas, such as Internet of Things, cloud-based applications, and automotive, place constraints on bandwidth or processing time which may prompt different choices than for TLS. Currently used protocols may have components that are specific to Elliptic Curve Cryptography (ECC) or to Rivest-Shamir-Adleman (RSA) or may require additional building blocks next to or in place of signatures and key-exchange mechanisms. While applications that provide authenticity are less urgent to migrate than those for confidentiality, those using embedded hardware such as secure elements, Two-factor authentication (2FA) and Multi-factor authentication (MFA) using hardware tokens and others have a very slow turnover and need to be replaced by the time large quantum computers exist, thus requiring migrating the design in the near future.

Activities should target one or multiple relevant protocols and produce post-quantum versions that guarantee at least as much security as currently deployed solutions. Typically this can be achieved through combining current and post-quantum solutions. Atypical solutions with equivalent security are also welcome.

[1] This decision is available on the Funding and Tenders Portal, in the reference documents section for Horizon Europe, under 'Simplified costs decisions' or through this link: https://ec.europa.eu/info/funding-tenders/opportunities/docs/2021-2027/horizon/guidance/ls-decision_he_en.pdf