Programme: EU-HORIZON 2020 Information and Communication Technologies - 2018-2020

Call:

SU-ICT-02-2020

Topic/s:

Specific Challenge:

Algorithms, software and hardware systems must be designed having security, privacy, data protection and accountability in mind from their design phase in a measurable manner. Relevant challenges include: (a) to develop mechanisms that measure the performance of ICT systems with regards to cybersecurity and privacy and (b) to enhance control and trust of the consumer of digital products and services with innovative tools aiming to ensure the accountability of the security and privacy levels in the algorithms, in the software, and ultimately in the ICT systems, products and services across the supply chain.

Scope:

Proposals are invited against at least one of the following three subtopics:

a) Cybersecurity/privacy audit, certification and standardisation

Innovative approaches to (i) design and develop automated security validation and testing, exploiting the knowledge of architecture, code, and development environments (e.g. white box) (ii) design and develop automated security verification at code level, focusing on scalable taint analysis, information-flow analysis, control-flow integrity, security policy, and considering the relation to secure development lifecycles, (iii) develop mechanisms, key performance indicators and measures that ease the process of certification at the level of services and (iv) develop mechanisms to better audit and analyse open source and/or open license software, and ICT systems with respect to cybersecurity and digital privacy.

b) Trusted supply chains of ICT systems

Innovative approaches to (i) develop advanced, evidence based, dynamic methods and tools for better forecasting, detecting and preventing propagated vulnerabilities, (ii) estimate both dynamically and accurately supply chain cyber security and privacy risks, (iii) design and develop security, privacy and accountability measures and mitigation strategies for all entities involved in the supply chain, (iv) design and develop techniques, methods and tools to better audit complex algorithms (e.g. search engines), interconnected ICT components/systems (v) devise methods to develop resilient systems out of potentially insecure components and (vi) devise security assurance methodologies and metrics to define security claims for composed systems and certification methods, allowing harmonisation and mutual recognition based on evidence and not only on trust.

The trusted supply chain for ICT systems/components should be considered by proposals in its entirety, in particular by addressing the IoT ecosystems/devices that are part of the supply chain.

c) Designing and developing privacy-friendly and secure software and hardware

Innovative approaches to establish methods and tools for (i) security and privacy requirements engineering (including dynamic threat modelling/ attack trees, attack ontologies, dynamic taxonomies and dynamic, evidence based risk analysis), (ii) embedded algorithmic accountability (in order to monitor the security, privacy and transparency of the algorithms/software/systems/services), (iii) system-wide consistency including connection between models, security/privacy/accountability objectives, policies, and functional implementations, (iv) metrics to assess a secure, reliable and privacy-friendly development, (v) secure, privacy-friendly and accountability-enabled programming languages (including machine languages), hardware design languages, development frameworks, as well as secure compilation and execution, (vi) novel, secure and privacy-friendly IoT architectures enabling consistent trustworthy and accountable authentication, authorization and accounting services across all IoT devices/ecosystems with enhancement of Public Key Infrastructures (PKIs) aiming to support PKI services (e.g. registration, revocation) for IoT devices.

For each of the sub-topics above, the outcome of the proposals is expected to lead to development up to Technology Readiness level (TRL) 5.

The Commission considers that proposals requesting a contribution from the EU of between EUR 4 and 5 million would allow this area to be addressed appropriately. Nonetheless, this does not preclude submission and selection of proposals requesting other amounts.

For grants awarded under this topic for Research and Innovation Action the Commission or Agency may object to a transfer of ownership or the exclusive licensing of results to a third party established in a third country not associated to Horizon 2020. The respective option of Article 30.3 of the Model Grant Agreement will be applied.

Expected Impact:

Short/medium term

Improved market opportunities for the EU vendors of security components.

Increased trust both by developers using/integrating the ICT components and by the end-users of IT systems and services.

Protect the privacy of citizens and trustworthiness of ICT .

Acceleration of the development and implementation of certification processes.

Long term

Advanced cybersecurity products and services will be developed improving trust in the Digital Single Market.

The use of more harmonized certification schemes will increase the business cases for cybersecurity services as they will become more reliable.

Validation platforms will provide assessments with less effort compared with nowadays and assure a better compliance with relevant regulations and standards.

Cross-cutting Priorities:

Contractual Public-Private Partnerships (cPPPs)
Cybersec

AG1 priority fields: ICT

Call Budget: 47000000,00€

Co-funding type:

Co-funding type: € euro

Opening date: 25 Jul 2019

Deadline date: 19 Nov 2019

Call presentation and documents: https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunit...