Specific Challenge: The fast evolution of ICT technology together with the uses that are made of it are exponentially introducing new threats, vulnerabilities and risks. There is a growing consensus that the state-of-the-art approach to secure ICT is becoming obsolete and, in addition, the walled-garden concept for security is becoming invalid.

The challenge is to find solutions guaranteeing end-to-end security that withstands progress for the lifespan of the application it supports, regardless of improvements in attacker hardware or computational capabilities.

Scope:

a. Research & Innovation Actions

Security-by-design for end-to-end security

Security-by-design paradigms have to be developed and tested, to providing end-to-end security, across all hardware and software layers of an ICT system and application and business services. Special attention has to be paid to the interaction of the layers and to a holistic approach. Platform independent solutions are needed to provide context aware and self-adaptive security in highly connected, complex and interoperable networks.

Automated security policy governance for such environments has to be addressed, allowing for run-time verification, customisation and enforcement between operators or virtual entities, in multi-layer and multi-service systems, spanning multiple domains or jurisdictions.

Open and dynamically reconfigurable environments need special attention, as well as environments where the user or provider has to rely on other providers, not necessarily of trustworthy origin.

The developed security-by-design solutions are expected to be usable in their deployment and implementation in order to decrease the security risks associated with improper use or misconfiguration and thereby allowing the user to trust devices and services intuitively.

Cryptography

Research projects have to address the key challenges to guarantee the security for the lifespan of the application it supports, to stay ahead of the evolution of the ICT environment and keep pace with the performance increase of ICT technology. The challenges to be addressed include:

- Resource efficient and highly secure technology for hardware based real-time cryptography;
- Resource efficient, real-time, highly secure fully homomorphic cryptography;
- Distributed cryptography including functional cryptography;
Cryptographic tools for securely binding applications to software, firmware and hardware environments, with or without the possibility to adapt the cryptographic primitives which are used;

- Post-quantum cryptography for long term security;

- Quantum key distribution (QKD) systems and networks for long-term security by design, as well as networks supporting information theoretic cryptographic primitives, including but not restricted to the integration into existing optical networks (e.g. trusted nodes and/or using multiplexing), addressing:
  
  i. low cost components for short-distance, low-bit-rate quantum key-distribution;

  ii. high-bit rate QKD systems that are tolerant to noise and loss.

Projects have to demonstrate a net increase in performance, or reduction in energy or power consumption, compared to state-of-the-art approaches and have to validate the proposed technology in realistic application scenarios, taking into account the current trends in ICT like cloud, mobile, IoT, etc. Activities may include methods for provable security against physical attacks, as well as research toward security certification.

b. Activities supporting the Cryptography Community

To complement the research activities in cryptography support and coordination actions should address the following aspects:

- ensure a durable integration and structuring of the European cryptography community, involving academia, industry, law enforcement and defence agencies.

- strengthen European excellence in this domain.

- provide technology watch, joint research agendas and foresight studies.

- identify technology gaps, market and implementation opportunities.

- provide technical expertise to the cybersecurity and privacy communities.

- contribute to the development of European standards, including for the public sector.

- solve training needs and skill shortage of academia and industry.

- evaluation and verification of cryptographic protocols and algorithms.

- organize open competitions with security and implementation benchmarking.

- dissemination and outreach, strengthening the link with institutional stakeholders.

Expected impact:

At macro level:

- a new paradigm for the design and implementation of ICT technology.

- ICT designed in Europe offering a higher level of security and/or privacy compared to non-European ICT products and services.

- ICT products and services compliant with Europe's security and privacy regulation.

- ICT with a measurably higher level of security and/or privacy, at marginal additional cost compared to ICT technology following the traditional designs (i.e. implementing security as add-on functionality).

At societal level:

- increase user trust in ICT and online services.

- improve users' ability to detect breaches of security and privacy.

- improved protection of the user's privacy, in compliance with applicable legislation.
more resilient critical infrastructures and services.

At research and innovation level: a new generation of ICT systems, applications and services that empowers users to take control over their data and trust relations.

provides security and privacy as a built-in feature, simpler to understand and manage for the user compared to traditional ICT.

ICT solutions allowing the user to monitor if her/his rights-online are respected and in compliance with the EU regulation.

simplify the implementation of cryptographic primitives.

ICT technology that is proofed to be more secure than ICT designed the traditional way.

**Instrument, funding level and budget**

a. Research & Innovation Actions – A mix of proposals requesting *Small and Large contributions are expected*

b. Coordination and Support Actions