NEXT
GENERATION
INTERNET

Open Call Text

NGI_TRUST 1st Open Call

(ref: NGI_TRUST 2019001)

Closing date for proposals:

Tuesday 30th April 2019 at 18:00 (CET)

Final Version of 01/02/2019

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 825618

Table of Contents

1 Introduction

NGI_TRUST is funded by the European Union's Horizon 2020 research and innovation programme under the grant agreement No 825618. The NGI_Trust project is part of the European Commission's Next Generation Internet (NGI) initiative[1]. NGI_TRUST aims to

- Reinforce, structure and develop the community of researchers, innovators and technology developers in the field of privacy and trust enhancing technologies
- Build on the state of the art in privacy and trust enhancing technologies by focusing support for third-party projects on a limited number of priority topics
- Improve user trust and acceptance of emerging technologies by focusing on applications and solutions that develop a more open, robust and dependable Internet and strengthen Internet Governance
- Foster the exploitation and commercialisation of the results of selected third-party projects through a tailored process of coaching and mentoring.

The project will provide financial support to third parties to meet these aims. To this end, three rounds of open calls will be organised during 2019-2020.

2 Topics addressed by the 1st open call

Third-party projects may receive financial support if they are working on privacy and trust enhancing technologies and their application to the NGI[2]. In particular, the *aim is to ensure that as sensors, objects, devices, AI-based algorithms, etc. are incorporated in our digital environment, that robust and easy to use technologies are developed to help users increase trust and achieve greater control when sharing their personal data, attributes and information*. More specifically, NGI TRUST will support third-party projects working in the following areas:

- Technical innovation in privacy enhancing technologies, such as cryptography, federated identity, security and privacy for Internet of Things (IoT), distributed ledgers and privacy-enhancing data transports and data at rest.
- The application of artificial intelligence/machine learning/neural networks to serve the user's interests (such as addressing concerns arising from the impact of profiling and mass surveillance).
- Bootstrapping trust at the protocol level, to maintain a decentralised Internet Infrastructure, for the establishment of trust, privacy (and security) between end-users and services.
- Developing means for individuals to make more informed decisions on the relevance of information that they are asked to disclose when accessing and using services.

[1] https://ec.europa.eu/digital-single-market/en/next-generation-internet-initiative

[2] As defined broadly by the Horizon 2020 Work-Programme 2018-20, Information and Communication Technologies Part 5.i - Page 48 of 141

An indicative list of pre-identified areas of concern is annexed. Proposers may use these areas as inspiration for developing their projects or may address additional areas of concern (specific topics) that they identify.

The NGI_Trust consortium expects that proposals submitted to the open call will seek to develop, whenever possible, **use cases** that can be scaled up or deployed as rapidly as possible to support practical privacy and trust enhancing solutions for the human centric internet, putting the "human being in front of the tool" and not vice-versa.

The use cases should address specific opportunities or challenges in the research and education, public sector/government and/or business sectors (or verticals). Applicants should explain how they will adopt a 'user-centric' approach to enhance trust and privacy by consulting or involving individuals, communities of practice or organisations in the co-design of applications and solutions.

3 Who can apply for funding?

The call is open to individual or team applications (see guide for applications for further information). Teams can involve experts from various disciplines including technological, legal ethical, sociological or economic expertise.

Applicants may be legal entities or natural persons and should be registered (for organisations) or resident (for individuals) in an EU Member State or a Horizon 2020 associated country (list of countries).

4 What sorts of projects will be funded ?

Three types of third-party projects will be awarded funding:

- Type 1 (viability) : up to € 100,000 from NGI_Trust, no matching funds required. The objective is to explore and assess the technical feasibility and/or commercial potential of a breakthrough innovation that aims at enhancing privacy and trust for the NGI. Activities can include conceptual development, risk assessment, market study or intellectual property management of a new technology or service, or a new application of existing technologies.
- Type 2 (execution) : up to €180,000 from NGI_Trust and matching funds of up to €90,000 (2/3 - 1/3 model). The objective is to fund R&D or technology development projects underpinned by a strategic plan and feasibility assessment (which can be, but need not be, developed through a Type 1 project funded by NGI_Trust).
- Type 3 (transition to commercialisation): up to €200,000 from NGI_Trust and the equivalent in matching funds (50/50). These projects should pursue the commercialisation of a privacy and trust enhancing innovation for the NGI (which can be, but need not be, developed through a Type 2 project funded by NGI_Trust).

Projects will receive support in the form of technical coaching, business mentoring and IP advice from the project partners and other NGI projects.

5 How will the projects be selected ?

The evaluation procedure of the proposals is set out in the Guide for Applicants. The time schedule for the 1st open call is as follows:

- 1 February 2019: open call launched
- 30 April 2019 : deadline for submission of applications
- May 2019 : eligibility check and evaluations of proposals
- June 2019 : Meeting of evaluation panel and of NGI_Trust Management board to agree on selected projects. Submission of the list of selected projects to European Commission for final approval.
- June 2019 : contracting and signature of approved third-party grants.
- July 2019 – onward : project implementation.

The duration of the projects will be up to 12 months. The amount of financial support will be determined, from a value for money perspective, by the NGI_Trust Management board based on the proposed budget and planned deliverables. Maximum award to any single third-party will be €200,000 over the life-time of the NGI_TRUST project.

Sub-grants may not have the purpose or effect of producing a profit for the beneficiary (third-party grantee). Financial support will be paid in instalments against achievement of milestones

6 Application form and support to applicants

For the application form and detailed guidance for applicants, please download the files available at the NGI_TRUST Open Call pages as well as at the NGI.eu website.

The NGI_TRUST consortium will organise a number of webinars and be present at a number of events during the period February-April to discuss with interested applicants. Please check the NGI_TRUST open call wiki pages & follow our twitter account: https://twitter.com/NgiTrust if you would like to register for one of these sessions.

For further information on the call or if you have any doubts relating to the eligibility rules or the information that is to be provided in the application form, please contact the Support Team: NGI-Trust-support@lists.geant.org

Examples of area of concerns which proposals may address

Area of Concern	Current State	Shortcoming	Ideal state
Users have Consent spread across multiple service providers	Inconsistent breadth and depth, siloed by solution/service provider	Lacks portability & interoperability	Consistent ontology, portable, interoperable machine readable and human readable receipts
Identity and fine-grained access for IoT and non-Web resources	Fine-grained access control is largely limited to web-based applications, requiring human interaction and strong compute intensive crypto.	With IoT a category of devices and services become part of the Internet that often lack capabilities in terms of compute power, battery life and interface possibilities to use the current state-of-the-art in access control.	Rich set of fit-for-purpose tools for fine-grained access control for IoT and non-web services.
Usability/UX of setting privacy controls and IA/ML algorithms revoking and porting them to new providers	Lack of agreed upon interfaces and interaction patterns for users to make informed decisions and manage their data.	Because of the proliferation of methods for interacting with users and lack of consistency and means for users to assess privacy controls privacy is at risk	Consistent set of design patterns and interfaces to allow users to make informed decisions about sharing their data.
Reducing personal info passed in an online transaction	Online merchants and service providers request more information about users than is required to deliver their services.	With GDPR service providers have the obligation to minimize the amount of data they collect and/or keep about users.	A comprehensive set of tools, including federated identity, to allow for minimal disclosure of user data.
Core technologies that ensure the proper operation of the Internet (routing, DNS, transport protocols) are vulnerable to compromise.	Communication over the Internet is under constant threat, adversaries can deploy a number of tools on different layers of the network stack to compromise communication or deny service to users.	The core protocols and technologies were not designed with security and privacy in mind.	New tools like DNSSEC, BGPSec, TLS and others are deployed to bootstrap security and trust for end users and devices.
Availability of open crypto software and hardware that can be used by users.	There is a very limited set of readily available crypto software libraries and even smaller set of hardware modules to bootstrap secure communications.	Due to shortage of options that are available and/or affordable appropriate security measures are avoided, and reliance on only a few products lead to high risk of massive compromise in case of vulnerabilities.	Large set of freely or affordable solutions for securing connections, including crypto libraries, certificates and hardware modules.

Area of Concern	Current State	Shortcoming	Ideal state
Vulnerabilities in software and hardware	Time to market is often more important than adherence to secure coding standards.	Providers open themselves up to breaches of security and privacy by using soft and hardware that is not properly designed.	Code that is exposed to the Internet (i.e. almost all code) should be designed with security and privacy in mind, tooling should be available to facilitate that.
Dominance of only a few app stores	To combat the risk of using random software from the Internet the large OS vendors have invested heavily in proofing mechanisms for content in their app stores.	By users increasingly relying on app stores, effectively three parties control what is on user devices (Apple, Google and Microsoft), this leads to concerns about autonomy, jurisdiction but also to the permissionless innovation character of the Internet.	Ideally there is an independent (from the large OS vendors) process for assessing software and quality proofing.
User Information Overload	Users are overwhelmed and overloaded with information regarding privacy and security decisions.	Security and privacy preferences and tools not being optimally used	Users would have a smart assistance that helps to make sure that their privacy and security preferences are met
Security Technology Fails Market Needs	Often Security Technology isn't developed with the market needs in mind and then experiences market shortcomings	Security Technology isn't addressing Market, Business, User, and Societal needs throughout the entire development process	Security technology would apply and address interdisciplinary and market needs to establish a market desired product