NGI

Guide for Applicants

NGI_TRUST 3rd Open Call
(ref: NGI_TRUST 2019003)

Closing date for proposals:
4 May 2020 at 18:00 (CET)

Version of 25/02/2020

Table of content

1 Aim of the open call

As set out in the open call text, NGI TRUST will support third-party projects working in the following areas:

- Better management of consent, to give more control to the user of their data when accessing and using services.
- Technical innovation in privacy enhancing technologies, such as cryptography, federated identity, security and privacy for IoT, privacy-enhancing data transports and data at rest.
- The application of artificial intelligence[1]/machine learning/neural networks to serve the user's interests.
- Bootstrapping trust at the protocol level, to maintain a trustable Internet Infrastructure.

An indicative list of possible areas of concern/opportunities (specific topics) is provided below:

1. **Topics focused on App implementations to manage the plethora of Information Sharing Agreements and consents that a person would agree to, manage and re-use over time (Type 2 or Type 3 proposals only)**

   - Solutions enabling users to get trust on privacy terms

   - Solutions enabling users to more easily and uniformly set preferences or terms such as machine-readable privacy terms (IEEE - P7012) and technologies that help to reduce the risk that GDPR is misused to further exploit/ complicate the user experience.

   - Efficient techniques to anonymize personal data in the era of Big Data.

2. **Technical innovation in privacy enhancing technologies, such as cryptography, federated identity, security and privacy for IoT, privacy-enhancing data transports and data at rest.**

   - Simplified multifactor authentication

   - Option for encrypted devices/data at rest. i.e. an option for the user to prevent being forced to decrypt their data under, such as physical threat.

   - Cybersecurity certification for ICT products, processes and services in the EU (EU Cybersecurity Act).

   - Solutions that improve algorithm agility (where deployed algorithms are superseded and must be replaced).

   - Improved information for users about the security mechanisms in use by apps (browsers give the user some clues about e.g. TLS; apps give none).

   - Pilot implementation of specifications, standards, acceptance criteria and measurement frameworks for new identifiers, for instance: Mobile Driving

---

[1] Proposals should take into consideration the Ethics Guidelines for Trustworthy AI, taking account of keywords such as lawful (respecting applicable laws and regulations), ethical (respecting ethical principles and values) and robust (both from a technical perspective, while taking into account its social environment).

Licenses; Delegation in the context of ID; eID and authentication services to support, for instance student mobility and access to educational services, thin file individuals, disabled users, refugees, non-digital natives, lost identities due to natural disasters etc.

- projects which bridge the gap between technological enhancements on one side and their actual uptake by non-expert users of the internet on the other side

- With a view to next generation certificates, how can European grid certificate authorities build up user-friendly mechanisms that promote a changed user experience and awareness and addresses forms of identity that comply with EU law and or meet specific European needs.

3. **The application of artificial intelligence/machine learning/neural networks to serve the user's interests.**

- User-centric design, simplicity, usability, edge AI ('artificial intelligence')

- Taking into account the recommendations of the EU High Level Expert Group on AI, a scientific and empirical approach is needed, such as developing guidance on how to approach access and acquisition of data for the development/expansion of AI, operationalize those recommendations in order to strengthen the capacity/ability of the Internet industry in Europe.

- Explainable artificial intelligence (XAI) for improving human trust in artificial intelligence (AI) systems

- Quantum resistant computing

4. **Bootstrapping trust at the protocol level, to maintain a trustable Internet Infrastructure.**

- DNS-based security of the Internet Infrastructure (DNSSEC, DOH approach), given the need to reinforce trust in a world of "deep fake".

More information on the call topics is found in the call text.

2 Eligibility criteria

2.1 Eligible applicants

The call is open to individuals or organisations, or groupings thereof. The following may apply, either on an individual basis or as a consortium:

- Researchers and developers (holding a Master's degree or higher) employed in third-level education institutes, research infrastructures, non-profit organisations and charitable (scientific) foundations and public research centres;

- Internet technologists and innovators, privacy and trust specialists and action groups;

- Organisations/companies with relevant privacy and trust cases or concerns in specific sectors or 'verticals' (fields such as health, etc.);
- Micro, small and medium-sized enterprises working on Internet or and other related technologies.

Applicants may be legal entities or natural persons. In addition, the following condition apply (see annex 6.4 in the proposal template):

- The organisations or individuals applying should have not have convictions for fraudulent behaviour, other financial irregularities, unethical or illegal business practices.
- The participating organisations should not have been declared bankrupt or have initiated bankruptcy procedures.

In case of selection for funding, official documents issued by the relevant national authorities to prove compliance with these conditions should be provided as part of the contracting process with NGI_TRUST.

2.2   Eligible countries

Applicants should be registered (for organisations) or resident (for individuals) in an EU Member State or a Horizon 2020 Associated country (list of countries available [here](#)).

2.3   Types of Sub-Project Funded

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

- Type 1 (viability): up to € 75,000 per project 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. Indicative duration: 6 months.

- Type 2 (execution): up to €150,000 per project from NGI_Trust and matching funds of up to €75,000 (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). Indicative duration: 6-9 months.

- Type 3 (transition to commercialisation): up to €200,000 per project 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). Indicative duration: up to 12 months.

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

The maximum award by NGI-TRUST to any single third-party during the lifetime of the NGI_TRUST project will be €200,000.

2.4 English language

English is the official language for NGI_TRUST open calls. The proposal must be in English in all its mandatory parts in order to be eligible.

English is also the only official language during the whole length of the third-party grant process. This means that all communication will be in English and all deliverables will only be accepted if in English.

2.5 Absence of conflict of interest

Applicants shall not have any potential conflict of interest with the NGI_TRUST selection process (notably they should have no legal relationship with any organisation that is a member of the NGI consortium or any person sitting on the advisory board).

3 Preparation and submission of the proposal

3.1 Structure and content of the proposals

Proposals must use the NGI_TRUST template.

A. Project proposal: divided in four main sections:

1) Overview of the proposal including an executive summary and the objective and type of project (**Section 1** of the proposal template)

2) Novelty/innovation (**Section 2** of the proposal template)

- Describe the degree of innovation with respect to existing solutions (either commercially available or currently being researched).

- Describe your project outcomes (which should be clear, measurable, and realistic) and how they will generate added-value with respect to state of the art in privacy and trust enhancing technologies.

The following points provide guidance on elements of novelty and innovation that can be presented in the proposal (where relevant, it is not obligatory to deal with all the points one-by-one):

- Incorporation into the digital environments of users and extensibility and applicability;
- Market potential/global dimension (development, commercialisation, and co-creation/collaborative adaptation);
- Potential technological impact related to the objectives of the call, in terms of privacy, robustness, etc.;
- Contribution to the human-centric Internet;
- Added value and alignment with overall strategy of applicants;
- Relevance to societal, gender, environmental and intellectual property rights (IPR) related issues;
- Creativity of research approach and stakeholders' engagement.

3) Expertise and resources (**Section 3** of the proposal template)

Track record and previous experience of the project team, relevance, technical improvements and value added regarding the specific topics of the call; links with other NGI technology-based firms, stakeholders and users (businesses, government, etc.).

Overview of the team

For each sub-project partner provide:

- The role of each participant (partner) in the sub-project, and their specific responsibilities for the sub-project activities.
- A short biography for each of the persons responsible for carrying out the proposed activities. These should include at least:
  o Previous publications, patents, projects, relevant to the subject of the proposal (list these in the **References** where relevant **(annex 6.6)**;
  o Research quality indices (e.g. H-index, n° citations, n° JCR publications, awards, etc..) where applicable (researchers);
- A description of any previous collaborations with other partners of the sub-project;
- 3-pages CV to be provided in **Annex 6.5**

Access to required resources or knowledge

Please describe any intellectual property (specifying whether your rights as owner or conditions to use it), datasets or and/or any equipment, datasets, etc. that required to carry out the project.

4) Project planning and budget (**Section 4** of the proposal template)

Project activities and milestones

Consistency between the objectives, approach and proposed activities;

Realistic timeframe and description of implementation (milestones).

- Please describe the main activities and steps to achieve the expected results and identify which partner will be responsible for specific activities.
- Provide a work-plan (Gantt chart or similar) including clear milestones and expected results against which progress will be assessed by the coaches and mentors.

Value for money

Provide a description of expected costs, using the tables provided keeping in mind the overall maximum contribution you are applying for. The following activities or types of expenditure qualify for financial support:

- Personnel costs;
- Equipment costs (in as much as they are required for the execution of the project);
- Software licenses (in as much as they are required for the execution of the project);
- Travel expenses;
- IPR search, advice or protection services.

The NGI_Trust Consortium may ask for further details and explanations about the funding requested.

B. Annexes: Legal entity form, statement of overall turnover, declaration on the honour concerning exclusion criteria and absence of conflict of interest: signed by the applicant or lead applicant in the case of a joint proposal, CVs and references.

Evaluators will be instructed not to consider additional material submitted by an applicant.

3.2   Procedure for submitting proposals

Applicants should submit proposals by email to NGI-Trust-calls@lists.geant.org before the deadline (see point 3.3). Applications submitted by any other means will not be considered.

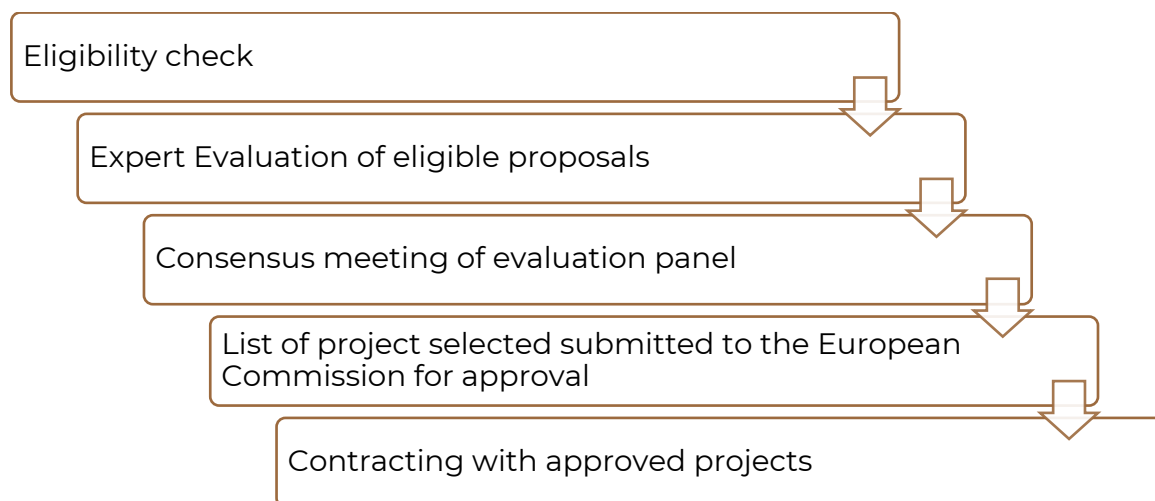## 3.3   Deadline for submission of proposals

The deadline is 4 May 2020 at 18:00 CET

Applicants are recommended not to wait until the last minute to submit the proposal.

Failure to submit on time for any reason, including extraordinary circumstances, will result in the rejection of the proposal.

4 Selection Process

The evaluation procedure is as follows:

Eligibility check

Expert Evaluation of eligible proposals

Consensus meeting of evaluation panel

List of project selected submitted to the European Commission for approval

Contracting with approved projects

4.1   Phase 1: Eligibility check

To be eligible for evaluation, applications will be checked for compliance with the following:

- Comply with all the eligibility criteria listed in Section 2
- Be submitted by email to NGI-Trust-calls@lists.geant.org
- Be submitted before the deadline (i.e. 4 May 2020 at 18:00 CET). The time recorded by the NGI_TRUST email system for the receipt of the email will be the official one.

All applicants eliminated from the process after the eligibility check will be notified in writing by email. Similarly, an email will be sent to all participants passing the eligibility check.

4.2 Phase 2: Expert evaluation

All eligible applications will be assessed and scored by three independent experts. The experts will be drawn from a panel of experts approved by the NGI_TRUST consortium – all experts will sign a non-disclosure and non-conflict of interest statement prior to receiving proposals for evaluation).

Proposals will be judged against the following criteria:

- **Novelty/innovation (40% weighting**) – section 2 of the proposal template.
- **Expertise and excellence of the proposed team (30% weighting)** – section 3 of the proposal template
- **Project planning and value for money (30% weighting**) – section 4 of the proposal template

4.3 Phase 3: Consensus meeting of the evaluation panel

Following the individual evaluations, a consensus meeting of the evaluation panel will be organised. During this meeting, a final ranking will be agreed and where necessary an additional review of projects for which there was a lack of consensus in terms of scoring by individual evaluators or for which additional clarifications are required will be undertaken.

The NGI_Trust Management Board will then formally approve a list of projects within the limits of the available funding.

4.4 Phase 4: Approval by European Commission prior to contracting

The list of selected projects (indicating clearly for each project, the third-party grantees identity, the amount of funding requested and the topic) will be submitted to the European Commission for final approval.

5 Third-party grants contracting and payment procedure

5.1 Duration

The duration of the projects selected in the call will be up to 12 months depending on the type of project (see 2.3). Applicants who consider they require more time should justify the longer-time frame clearly, and such requests will be considered on a case-by-case basis during the evaluation procedure.

5.2 Funding

The amount of financial support offered will be determined by the NGI_Trust Management board based on the submitted budget and planned deliverables from a value for money perspective. The proposed budget may be adjusted for costs that are deemed ineligible as well as for the cost of any additional activities recommended by NGI_TRUST. The final amount is established in the third-party

sub-grant agreement between EFIS Centre (on behalf of the NGI_Trust consortium) and the sub-grantee. If the sub-grantee does not agree with the amount of the grant offered, they are at liberty to withdraw their proposal.

The grant for each project will be paid as a lump-sum grant on the basis of a work-plan and a related budget outline. Each third-party contract will include a work-plan including clear milestones and expected results against which progress will be assessed and interim payments made. The third party cannot request any funding for activities that are already funded by other grants (the principle of no double funding).

Third-party grants may not have the purpose or effect of producing a profit for the third-party grantee.

Financial support will be paid in instalments against the achievement of milestones as follows (interim payments may be divided into smaller amounts with respect to the agreed milestones):

- 40% after signature of the sub-grantee contract by both parties;
- 45% after the completion of the project (submission of the final report) and positive evaluation by NGI_Trust of the project outcomes;
- 15% final instalment paid back-to-back with the European Commission's final payment to the NGI Trust Project Coordinator.

5.3 Legal requirements

The third parties included in the provisional list of awardees will provide documentation to prove their compliance with the Eligibility Criteria. More specifically, the following documentation will have to be provided:

1. Legal status information:
    a. Legal entity form (Natural person, private company or public law body): signed and stamped + supporting documents. See **Annex 6.2** proposal template;
    b. For organisations: Statement of overall turnover for the last two financial years (+ supporting documents on request – see point 2 - balance, profit & loss accounts of the two latest closed financial year and the relation, upstream and downstream, of any parent, partner or subsidiary company/organisations). See **Annex 6.3** proposal template;
    c. Declaration of Honour signed by third-party when submitting the application. (+ supporting documents on request, see **Annex 6.4** Proposal template).
2. All the above-mentioned documents should be provided in English (and if not in English, an English translation should be provided). The supporting documentation related to the statement of overall turnover and Declaration of Honour should be provided within a deadline communicated when notified of the award of a third-party grant. In case the requested information is not provided in time without significant, clear and reasonable justification, this may lead to the termination of the 'Sub-grant procedure'.

5.4 Contractual arrangements

Once all the formalities are concluded each selected third party will be invited to sign an 'NGI_TRUST Third-Party Grant Agreement' with the Consortium (represented by EFIS Centre for the purposes of signature).

The funds awarded under NGI_TRUST Grant Agreement are provided directly from the funds of the Horizon 2020 funded project, and are therefore, funds owned by the European Commission. Management of the NGI_TRUST funds has been transferred to the project partners in NGI_TRUST via the Grant Agreement Number 825618 signed with the European Commission.

The recipients of the third-party financial support must allow the Commission, the European Anti-fraud Office (OLAF) and the Court of Auditors to exercise their powers of control on documents, information, even stored on electronic media, or on the final recipient's premises.

6 Intellectual property rights

6.1 Originality of the sub-granted projects

It is assumed that the applicants base their proposals on original works and going forward any foreseen developments are free from third party rights. If not, third party rights should be clearly stated in the application for funding. The NGI_TRUST Consortium is not obliged to verify the authenticity of the ownership of the future products and services and any issues arising from third party claims regarding ownership are the solely responsibility of the sub-granted parties.

6.2 Ownership of the sub-granted project results

The ownership of IPR created by the Third-Parties using the NGI_TRUST funding will remain with the third parties, who will be the sole owners of the technologies or applications or other forms of IP created within the framework of their funded projects. There are no IPR obligations toward the European Commission (EC).

6.3 Acknowledgement of EU funding

Any communication or publication of the third parties about the sub-project and the result arising therefrom shall clearly indicate that the project has received funding from the European Union under the NGI_TRUST project and must therefore display the EU flag and 'Next Generation Internet' logos on all printed and digital material, including websites and press releases. Moreover, the third parties agree that certain information regarding the projects selected for funding may be used by NGI_TRUST for communication purposes.

7 Support to applicants

For more information, please check NGI_TRUST Open Call website:
https://wiki.geant.org/display/NGITrust/3rd+Open+Call+NGI_TRUST

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

8 Overall time-schedule for the open call

The time schedule for the 3rd round open call for NGI_TRUST is as follows:

- 28 February 2020: open call launched
- 4 May 2020: deadline for submission of applications
- May 2020: eligibility check and evaluations of proposals
- June 2020: 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 2020: contracting and signature of approved third-party grants.
- July 2020 – onward: project implementation.

9 Applicable law

The sub-grant agreement will be governed by Belgian law and relevant regulations of the European Union.

10 Data protection

All data will be held securely by NGI_TRUST Management Team. Data will be treated confidentially and will not be disclosed to external organisations, other than those acting as evaluators on related projects or for other legitimate reasons.