NGI

Partnership for innovative technological solutions to ensure privacy & enhance trust for the human-centric Internet

25-27 September 2019 – Ruth Puente, Kantara Initiative Europe

NGI TRUST

NGI_TRUST in a snapshot

Project partners

EFIS

Fraunhofer IAO

GÉANT Networks • Services • People

tecnalia Inspiring Business

ebn innovation network

kantara INITIATIVE EUROPE

Key facts & figures

- Duration: December 2018- November 2021
- 3rd party funding: €5.6m
- Three rounds of open calls
- Aim is to:
  - engage a variety of players & not just "usual H2020 suspects";
  - explore privacy & trust enhancing topics (defined with the support of an advisory board) critical to building a Human Centric Internet

NGI TRUST

NGI_TRUST objectives

1. Reinforce, structure and develop the community of researchers, innovators and technology developers in the field of privacy and trust enhancing technologies
2. Build on the state of the art in privacy and trust enhancing technologies by focusing support for third-party projects in a limited number of priority topics
3. 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
4. Foster the exploitation and commercialisation of the results of selected third-party projects through a tailored process of coaching and mentoring

NGI TRUST

Three types of third-party projects

Type 1 (viability)	Type 2 (execution)	Type 3 (transition to commercialization)
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.	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).	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).

Maximum award to any single third-party will be €200,000.
Duration of third-party project : 9-12 months

NGI TRUST

Schedule for the open calls

1st open call

- Open Call period: 1 February 2019- 30 April 2019
- Evaluation panel selected project by mid-June
- 18 third-party projects selected and launched from July 2019

2nd open call

- **Launched : 1 October 2019**
- **Deadline for proposals : 1 December 2019**
- Contracting and launching of projects: February 2020

3rd open call

- Launched: 1 February 2020
- Deadline for proposals : 1 April 2020
- Contracting and launch of projects: July 2020

NGI TRUST

1st call – key figures

109 proposals received, of which

- Type 1: 81
- Type 2: 26
- Type 3: 2

177 Partners from 27 countries

68 out of 109 (62%) lead partners have not received Horizon 2020 funding before (information to be verified).

Country	# partners	% of total
France	32	18.1%
UK	22	12.4%
Germany	18	10.2%
Spain	15	8.5
Netherlands	14	7.9%

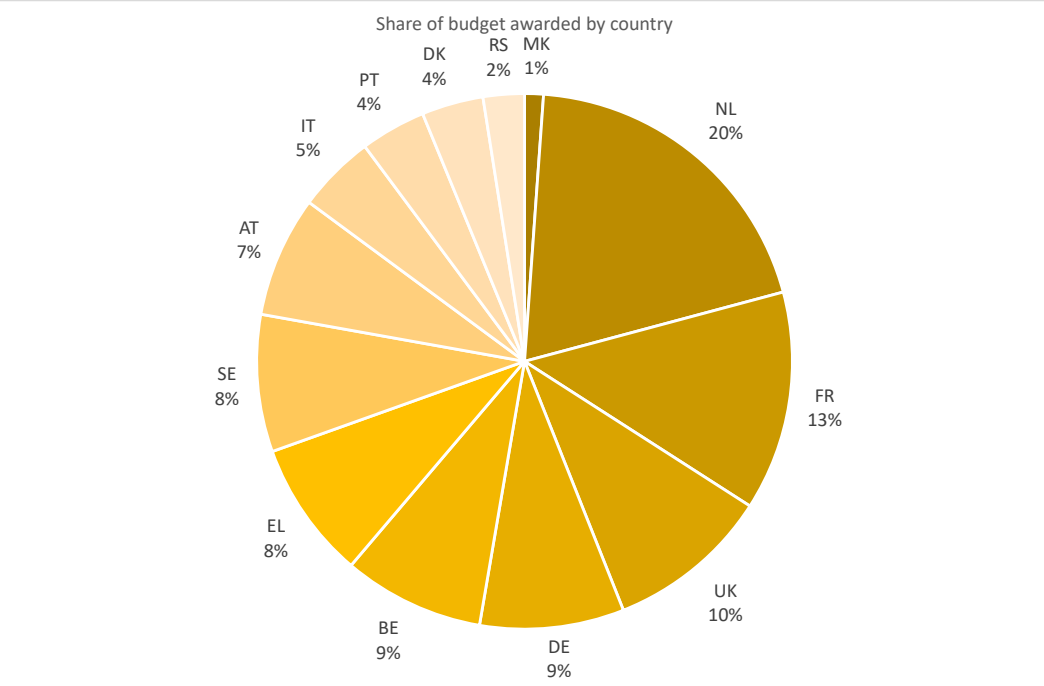
Funding (total for 109 projects)
Total budget : € 15,311,092
Total funding requested : €12,487,796

NGI TRUST

1st call awardees

Number of projects awarded	18
Total budget allocated	€ 2,112,723
Total number of Third Parties	27
New to H2020 (per TP)	17

Type of Third Party organisations	Number	% total
SMEs	13	48%
Higher Education (e.g. university)	7	26%
Other not-for-profit (NGO, foundation,...)	4	15%
Research organisation	2	7%
Natural person	1	4%
Total	**27**	**100%**



NGI TRUST

1st call themes: beyond passwords, better privacy, safer browsing and user control.

- We need to move **beyond passwords**, and find a better way for users to manage the complexity of shared secrets and technical trust. 4 projects (**Keyn, COP-MODE, CryRev, and TCN**) will work in this area, looking at how we can use our mobile devices more effectively as tokens instead of the need for passwords, how we can better protect data on our mobile devices, and how we can improve the way that cryptography is used on hardware and in the core of our internet infrastructure.
- It is essential to provide **better privacy**, particularly in areas where data is more sensitive and in how we present privacy information to our users. 4 projects (**b-smart, Edge-TINC, CAP-A and MyPCH**) will look at how we can both protect and utilise health data, how we deal with managing large amounts of data in the cloud and how we can better support users in understanding the legal issues around consenting to use services.
- Safer browsing is essential to an **ecosystem of privacy and trust**. 3 projects (**CASPER, D4S, and ISIBUD**) will look at providing better informed safety for children online that doesn't block access unnecessarily to useful information, how we can improve VPN technology to provide a better user experience and how we can support the users needs more effectively in internet search rather than being driven by the wants of advertisers.
- To achieve a truly human-centric Internet, we need to have **user control**. The complexity and options when navigating a globally connected internet can be a daunting task. 6 projects (**Cozy Cloud, EUACTIVE, DECIDE, Protect Yourself, INSTANT, and Decentralised Messaging**) will focus on user control to ease the decision making and customisation of settings to give the user a role in their internet.

NGI TRUST

Proposal Acronym	Lead Partner (name)	Keywords	Country
b-smart	THINGS	privacy settings, IoT, informing users	Italy
CAP-A	FORTH	consent, privacy, terms of service	Greece / Germany
CASPER	School of Electrical Engineering (ETF)	child protection, filtering, DNS	Serbia / Portugal / North Macedonia
CCS Cozy Cloud's	Cozy Cloud	GDPR, privacy, personal cloud	France
COP-MODE	Joao P. Vilela	user data, mobile phones	Portugal/UK
CryRev	Assured AB	HSM, open source hardware, key management	Sweden
D4S	DTU	VPN, open source	Denmark / Netherlands
Decentralized messaging	Danube Tech GmbH	SSI, messaging, privacy	Austria
DECIDE	University of Stuttgart	SSI, blockchain, PETs	Germany
Deep-Learning	SensifAI	image manipulation, personal data, privacy	Belgium
Edge-TINC	Fluentic Networks Ltd	blockchain, IoT	UK
EUACTIVe	VDP	SSI, advertising data	Netherlands / Germany
INSTANT	Virtual Angle BV	AI, big data, privacy	Netherlands
ISIBUD	Better Internet Search Ltd	internet search, personalisation, privacy	UK
Keyn	Keyn B.V.	smartphone, strong authenication	Netherlands
MyPCH	Diabetes Service ApS	health data, data exchange, privacy	Denmark / Austria
PY	PANGA	SSI, IoT	France
TNC	Athena Research and Innovation Centre	blockchain, named data networking	Greece/UK

1st Open Call – funded third-party projects

2nd Open Call priority topics

- 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/machine learning/neural networks to serve the user's interests.
- Bootstrapping trust at the protocol level, to maintain a decentralised Internet Infrastructure.

NGI TRUST

Indicative areas of concern that could be addressed by proposals for the **2nd open call**

- 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.
- DNS-based security of the Internet Infrastructure (DNSSEC, DOH approach). The need to reinforce trust in a world of “deep fake”.
- Post-quantum technologies to avoid brute force attacks.
- Reinforcing reputation systems and thereby enhance the potential to measure the value of personal data and transparency; valorisation of data that respects the principles of GDPR.
- Pilot implementation of specifications, standards, acceptance criteria and measurement frameworks for new identifiers (e.g. Mobile Driving Licenses; Delegation in the context of ID; eID and authentication services to support: thin file individuals, student mobility and access to educational services, disabled users, refugees, non-digital natives, lost identities due to natural disasters).
- Services and technologies that enhance transparency, user intervenability, and accountability in data processing.

NGI TRUST

2nd Open call process and timing

- 1 October 2019: open call launched
- 30 November 2019 : deadline for submission of applications
- December 2019 : eligibility check and individual evaluations of proposals
- January 2020 : Meeting of evaluation panel and of NGI_Trust Management board to approve list of selected projects.
- Submission of the list of selected projects to European Commission for final approval.
- February 2020 : contracting and signature of approved third-party grants.
- March 2020 – onwards : projects implemented.

Projects will receive coaching from technical experts during their implementation and follow-up support on IPR and business mentoring to help implement their solutions.

NGI TRUST

More information/contact us

Project coordinator

- Mr Alasdair Reid @ EFIS Centre - www.efiscentre.eu
- Email : NGI-Trust-support@lists.geant.org
- Twitter: @NgiTrust
- NGI_TRUST wiki : https://wiki.geant.org/display/NGITrust
- NGI.eu website : https://www.ngi.eu/opencalls/ngi_trust-open-call/

The NGI_TRUST project has received funding from the European Union's Horizon 2020 Research and Innovation Programme under Grant Agreement No 825618

NGI TRUST