April 2020

The Alan Turing Institute

Call for research proposals – Trusted Digital Infrastructure for Identity Systems

Contents

INTRODUCTION

Governments around the world are committed to supporting the roll out of national digital IDs, but there are privacy and security implications associated with scaling these systems at a national level.

Responsible implementation of ID services is a critical enabler for financial inclusion; it enables access to services and enactment of civil rights. According to the World Bank, more than 1 billion people are currently living without an official digital identity.

The Alan Turing Institute is joining a vibrant community of NGOs, charities, private sector providers, universities and think tanks addressing global identity challenges in the digital age.

Questions of trust are based around the complex interplay of socio-technical considerations, requiring multi-disciplinary expertise. The 'trustworthiness' of digital IDs is characterised by multiple inter-related dimensions that include security, privacy, ethics, resilience, robustness and reliability. These dimensions are required to provide the knowledge, tools and guidance needed to implement privacy-preserving, secure identification systems

This initiative is funded through a grant from the **Bill & Melinda Gates Foundation.**

Project aims

The project aims to enhance the privacy and security of national digital identity systems, with the ultimate goal to maximise the value to beneficiaries, whilst limiting known and unknown risks to these constituents and maintaining the integrity of the overall system.

The project is comprised of three major workstreams:

1. **Knowledge**: Undertake the fundamental research required to develop new solutions that realise trustworthy identity systems, and understand the social, economic and ethical issues pertaining to these systems. This research effort will seek to increase shared understanding of the key issues and risks for national ID systems.

2. **Development**: Develop new software and technical components to apply the state-of-the-art research to existing systems and translate it into high priority application areas. Working with existing open source providers we will analyse the complex, interface and various functional requirements for a large-scale identification system.

3. **Implementation**: Work with priority countries, ecosystem collaborators such as World Bank's ID for Development (Id4D) initiative and open source providers to pilot and scale new knowledge and technical components including development of

architecture for optimal solutions, assessment of technical implementation risks,and modification of components to make them context and scale appropriate.

This is a multi-disciplinary project bringing together skills from diverse fields such as threat modelling and read teaming, dynamic cyber security and real-time governance, risk modelling, cloud solutions/ID-as-a-service, privacy enhancing technologies (PETs) and security policy development.

This project will be spearheaded by three leading professors in privacy and security (a growing field of excellence for UK research):

- Professor Mark Briers, Director of Defense and Security program at the Alan Turing Institute

- Professor Carsten Maple, Director of the NCSC-EPSRC Academic Centre of Excellence in Cyber Security Research, and Professor of Cyber Systems Engineering at the University of Warwick

- Professor Jon Crowcroft, Marconi Professor of Networked Systems in the Computer Laboratory at the University of Cambridge

Funding available

Projects will be funded dependent on duration and scope. These should be 9, 12 or 18 months long.

The funding can be used for direct and indirect costs (please note that indirects are capped at 15% in line with the flow down conditions of this funding). More information on eligible costs is available on the Turing call webpage and the flexigrant call page. Please consult with your institution for guidance as to costs when you prepare your application.

Research challenges for this call

Governments around the world are committed to supporting the roll out of national digital IDs, but there exist many risks associated with scaling these systems at a national level. Building an ID system that meets developmental goals is a multifaceted challenge, and questions of trust are based around the complex interplay of socio-technical considerations, requiring multi-disciplinary expertise. The 'trustworthiness' in digital IDs is characterised by many dimensions that include security, privacy, ethics, resilience, robustness and reliability.

Several high-level sets of principles have been defined by organisations like the World Bank Group's Identification for Development (ID4D) Initiative, in accordance with the Principles on Identification for Sustainable Development and other international standards. They provide a primer on why ID matters, the risks of ID systems, and the international stakeholders. They also outline the critical principles that practitioners need to follow to ensure that ID systems are implemented responsibly. Such principles include robust, secure and sustainable design,

universal coverage and accessibility, as well as strong governance and accountability frameworks.

Yet, the existing technical implementations come with a set of trade offs that need to be evaluated in a systematic way against the high-level design and implementation principles. The Turing will convene a multi-disciplinary research team to develop a Trustworthy Digital Identification System Framework in order to promote and enhance the adoption of privacy-preserving and secure systems. This framework will link complex concepts such as privacy and trust to existing technological capabilities and assess the requirements of priority countries in order to address any gaps.

Below is the *non-exhaustive* list of challenges in the technical implementation of digital identity which the research proposal should address:

1. In designing trustworthy identity systems, decision-makers should aim to understand the risks and failure scenarios associated with people's use of such systems. Risk modelling in digital systems is known to be a significant research challenge.

2. ID systems need to be resilient in order to establish robust and accurate identity. Yet, they are exposed to many potential threats and vulnerabilities in the identity management lifecycle, pertaining to data collection, retention, sharing and disposal. These threats can be diverse, and include attackers, their motivations and methods.

3. System design should incorporate privacy and security considerations to mitigate the risk of privacy violations, data theft and misuse, identity fraud, and discrimination. Several Privacy-enhancing Technologies (PETs) can enable these objectives, but it's not always clear how to match these emerging technologies to the exact needs of implementers.

4. Physical storage and processing of identity data is another technical challenge that requires addressing. Significant computing resources are required to store and process the data, making ID-as-a-service a desirable approach.

5. The different modalities of authentication are equally important. For example, biometric recognition has rapidly proliferated in modern ID systems due to its perceived accuracy, however, biometrics are not appropriate in all contexts and have recently spurred significant controversy due to a host of privacy concerns.

6. ID systems require strong legal and regulatory frameworks to ensure data protection and control. The technical implementation of these frameworks needs to reflect the specific requirements dictated by these frameworks (e.g. real-time governance and analytics).

7. Often, key decisions regarding the design and use of ID systems should be driven by the context and people-centred perspectives rather than technology itself, with the aim to make the systems interoperable and responsive to the needs of various users.

This call for proposals will consider proposals from diverse fields and a broad range of topics spanning the entire spectrum of design and implementation considerations. We encourage applications in novel areas that are not explicitly mentioned above to suggest their own proposed research challenge that they wish to address.

APPLICATION PROCESS

Any queries regarding process, post-award requirements, costing or general eligibility should be discussed with the Research Project Manager Amber Raza <araza@turing.ac.uk>

Successful proposals will be funded through an award from the Turing.

The process summary is as follows:

- Online form completed by applicant and submitted online
- First stage: Initial review and eligibility check
- Second stage: applications which pass first stage are then sent to reviewers
- Reviewers review applications based on best fit to call
- Successful applications selected
- Applicants notified of outcome by Research Project Manager

Eligibility

Researchers (Turing Fellows, Turing Research Fellows, Doctoral Student Supervisors and others) and other academics from our partner universities to apply to this research call. Applications from other UK-based universities may also be considered, subject to mutual acceptability of contractual terms.

How to apply

To apply for the research call: please find the form and apply online via **the Turing's Flexigrant site** **by Monday 18 May 2020 13:00 BST**

If you have not already done so, all applicants must first register on the system and provide basic details to create a profile. If you have any question regarding the application form or using the online system, contact the Research Project Manager Amber Raza: araza@turing.ac.uk

The PI should submit the following:

- **Research Challenge you wish to address**

- **Your skills and experiences in this f**

- **Indicative outcome of the proposal**

- **Estimated cost profile and team** (the final budget will be agreed at award agreement stage)

- **Letter from head of department OR research support office** confirming willingness to host the project if the application is successful, confirming costs have been checked and approved, and where applicable, outlining the process for oversight and approval for the project through the university's research Ethics Committee (or equivalent) (pdf format) *(We understand it may not be possible to obtain such letters of confirmation prior to the deadline due to the short timeframe and will accept these after the*

deadline if necessary. Please note, no award can be made prior to receipt of such letter.)

Eligible costs

- **Direct costs** are on FTE basis of personnel working directly on the project – this could include, for example, PIs, postdocs, data scientists or software engineers.

- Please be aware that **PI time can be bought out at up to a maximum of 10%**

- **Other costs**: could include

- Travel and subsistence for project researchers when away from host university (e.g. attending conferences, travelling to/from the Turing)

- Conference fees where the conference is directly application to the research project

- **Please note that indirect costs are capped at 15%** in line with the flow down conditions of this funding. See <u>background & conditions doc</u> for more info on this.

KEY DATES

Publication of call for proposals	27 April 2020
Deadline to submit	18 May 2020
Review and selection of proposals	18-22 May 2020
Award offers and acceptance of terms	25 May 2020
Earliest projects start	01 June 2020
Projects to complete and report by	Depends on date started

CONTACT

Research Project Manager Amber Raza <araza@turing.ac.uk>