



The Alan Turing Institute

Trustworthy Digital Infrastructure
for Identity Systems

The Global Imperative

Introduction

In 2020, The Alan Turing Institute (Turing) embarked on The Trusted Digital Infrastructure for Identity Systems project to advance knowledge and enable progressive innovation for countries around the world as they turn to digital identity and verification technologies. It is a four-year research and development endeavour that brings together a vibrant community of thought leaders, practitioners and field experts.

This project acknowledges that advances in digital technologies are redefining opportunity around the world to develop new economic value, to govern and serve within more accessible societies, and to empower individuals. Legal recognition of identity, the ability to establish trust in who we are, is a foundational component of society, a powerful tool that confirms access to life-sustaining resources and services, alongside evolving opportunities: It is enshrined in the Universal Declaration of Human Rights. Digital innovations in identity bring new opportunities to create transparency, fairness, and better governed services. They also create the potential to distribute and interpret significant

amounts of information about people and their communities. Appreciation for what makes digital identity systems trustworthy has yet to be widely explored.

Often when people speak of trust in the context of identity systems, the focus is on the technical security of the systems and data. Developing the capacity for trust must reach far beyond this requirement: It is grounded in the ability to develop with a contextual understanding of the communities and environment served.

This project begins with the particular need to develop a richer understanding of the evolving threats to identity systems and processes, and the risks these present within lower income countries. It examines the complex interplay of social and technical considerations and draws from multi-disciplinary expertise. It also seeks to develop new tools, including a Trustworthy Digital Identity System Framework (TDISF), to guide countries' assessment of the trustworthiness of their systems.

Follow the progress [#trustworthyidentity](#)

<http://www.turing.ac.uk/research/research-projects/trusted-digital-infrastructure-identity-systems>

Contents

5/6

A Growing Digital Imperative

Gateway to services and Support

8/9

Identity as a Development Imperative

Ability to meaningfully participate

10/11

Trust as a Systematic Imperative

Designing for the trust assumptions

12/13

Advancing Knowledge

A unique opportunity to take stock

14

Engaging a Global Community

Applying multi-disciplinary expertise

16/17

Trustworthy Digital Infrastructure

for Identity Systems

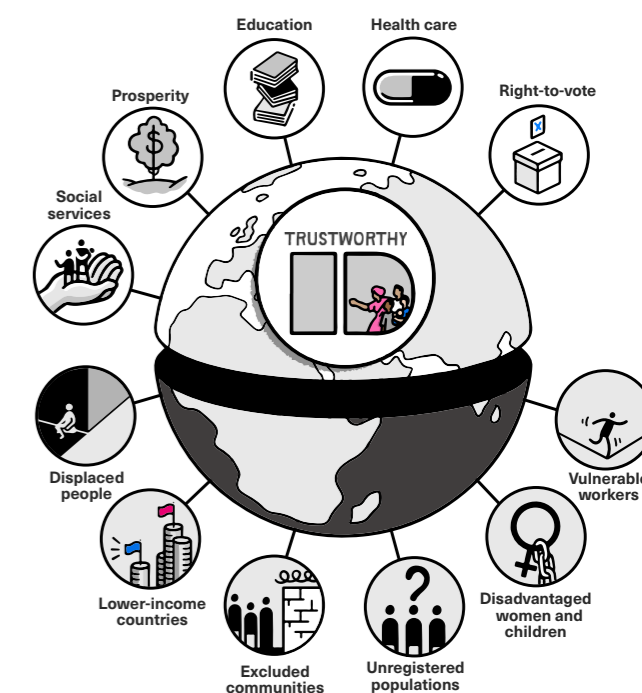
“The search for new techniques must be regarded as carried out by the human community as a whole”

Alan Turing

A Growing Digital Imperative

Reliance on the need to produce documented confirmation of individual identity has evolved to become a foundation of society as people's lives developed beyond their local community, beyond their ability to simply be recognised. Observations going back to ancient societies, indicate that jewellery and adornments¹ are known to have served to identify people with familial or tribal communities. The Babylonians and Romans adopted census taking as their empires expanded.² Since the 15th century, birth and civil registration has increasingly developed as a societal pillar³, while the English King Henry V has been credited with establishing the precursor to the modern passport.⁴ This rich history underpins well-established norms in modern society that now demands individuals have a reliable way of verifying who they are: Without it, people cannot travel, secure a job, open a bank account, access social care, or secure a home.

Society's norms continue to evolve with digital transformation significantly picking up the pace and now bringing revolutionary change to the economic opportunities that lay before us, how we interact and how we are identified in the process. Over the last decade, Identity-as-a-Service models have emerged as a gateway to public and private-sector services, affirmation of basic rights, and humanitarian aid.



Governments around the world are embracing digital identity infrastructures with trailblazers such as Estonia,⁵ India⁶ and the UAE⁷, each very different in their approach, held up as examples of how society and economy is evolving. With their global scope, humanitarian organisations such as UNHCR and the World Food Programme, both United Nations agencies, have become custodians of some of the largest digital identity systems in the world.⁸

¹ https://www.researchgate.net/publication/255619015_Adornment_Identity_and_Authenticity_Ancient_Jewelry_In_and_Out_of_Context

² <https://rss.onlinelibrary.wiley.com/doi/pdf/10.1111/j.1740-9713.2013.00706.x>

³ <https://www.cgdev.org/publication/identification-revolution-can-digital-id-be-harnessed-development>

⁴ <https://www.theguardian.com/travel/2006/nov/17/travelnews>

⁵ <https://medium.com/metadium/how-estonia-is-pioneering-the-digital-identity-space-4008c709fbb8>

⁶ https://www.mitpressjournals.org/doi/pdf/10.1162/inov_a_00204

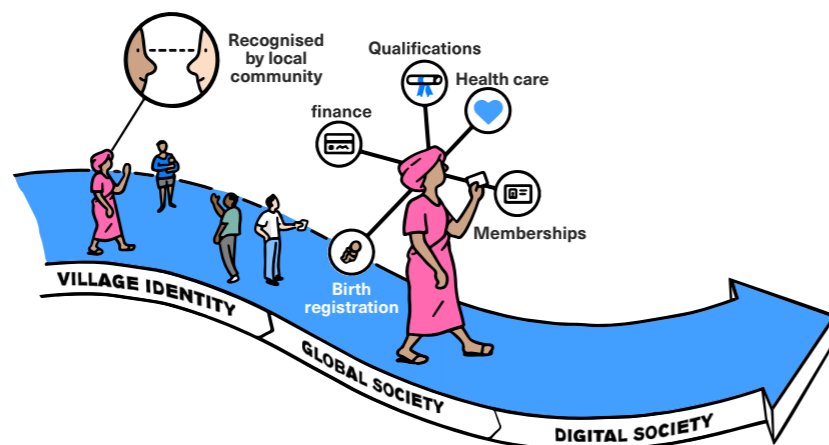
⁷ <https://gulfnews.com/uae/government/uae-pass-creates-first-national-digital-identity-1.2290616>

⁸ <https://www.theengineroom.org/wp-content/uploads/2018/03/Engine-Room-Oxfam-Biometrics-Review.pdf>

Further, commercial initiatives and alliances, particularly within finance⁹ and telecommunications,¹⁰ are driving functional digital identity systems to solve particular industry or regulatory concerns, including anti-money laundering with many aspiring to address broader requirements. Commercial impetus also comes from global technology giants, Google, Apple, Facebook and others that have strategically developed customer accounts as social logins¹¹ to serve as convenient identities for a breadth of opportunities including one trial from Amazon to facilitate contactless in-person payments and secure venue entry with a scan of an individual's palm.¹²

With such development, increasing levels of personal details and biometric data— fingerprints, photos, palm, facial and iris scans— is collected and used widely, often given freely in exchange for convenient access to a product, service or support from governments and companies alike. Verification services are both supplementing and sometimes replacing the presentation of physical ID, while some traditional paper documents, including passports and identity cards, are emerging in a digital form.

The World Bank Group's global dataset¹³ reveals that 161 countries, the lion's share of the 175 countries known to have national identity programmes, are using digital technologies. Against this background, its Identification for Development (ID4D) programme highlights a need to close an identity gap for an estimated one billion people who do not yet have any form of legally recognised Identity. Their initiative supports a United Nation's Sustainable Development Goal to provide legal identity for all, and highlights that fast-evolving digital identity solutions, particularly biometrics-based enrolment systems, are increasingly facilitating a way forward where systems for allocating unique identifiers to people may be lacking.



The impact of the COVID-19 pandemic has gone on to both illustrate and intensify the growing reliance on digital identity systems as the world's population went into lockdown, and governments and businesses fast-tracked plans to digitally enhance operations. Before this, the World Economic Forum (WEF) had forecasted that over 60% of global GDP was expected to be digital by 2022.¹⁴ As identity systems evolve, they play an ever-greater role in prospects for economic as well as societal inclusion. For the one billion without any legally recognised form of identity, the associated digital transformation of services, social support, and economic opportunity offers hope of addressing many inequalities as it enriches participation in society.

For many people, however, their trust in identity systems may be assumed, or concerns over their lack of it suppressed in favour of benefit. It behoves us to enhance understanding of the requirements for the development of trustworthy identity systems as their role in underpinning society continues to move at pace. In spearheading independent research and development, the Turing embraces an ambition to both showcase good practice and advance emerging areas of knowledge. The intent is also to translate learning into system requirements and functional prototypes that are trustworthy by design and can become part of national identity infrastructures implemented by the project's in-country partners. Ultimately, the goal is to inform countries' development of trustworthy identity systems, and positively influence the ecosystem of standards, the decisions of policy makers and the technologies that are taken forward.

Definitions

Foundational ID _ Foundational identification provides identity that is legally verified by a state or government. They can take the form of a national ID, civil or birth registry.

Functional ID _ Functional identification provides access to a particular service or transaction, licenses an ability or professional status, denotes membership or facilitates access to an organisation or community.

Self-Sovereign ID _ is a model for managing control over digital identity in which an individual has ownership and control over their data, eliminating the need to rely on a central authority or central repository of data to verify identity.

Identity as a Service _ cloud-based authentication or verification built and operated by a third-party provider to ensure users are who they claim to be and have the rights to access services and resources.

⁹ <https://www.mobeyforum.org/>

¹⁰ <https://www.gsma.com/identity/>

¹¹ https://en.wikipedia.org/wiki/Social_login

¹² <https://www.aboutamazon.com/news/innovation-at-amazon/introducing-amazon-one-a-new-innovation-to-make-everyday-activities-effortless>

¹³ <https://datacatalog.worldbank.org/dataset/identification-development-global-dataset>

¹⁴ http://www3.weforum.org/docs/WEF_Our_Shared_Digital_Future_Report_2018.pdf

Identity as a Development Imperative

A concerted, global and humanitarian-inspired effort is underway to assure everyone has documentation of their identity and the ability to meaningfully participate in society. Organisations including ID4D, ID4Africa¹⁵, and a range of humanitarian development funds are progressing comprehensive initiatives to improve availability and regard for identity programmes as a foundation for addressing global inequalities.

For some countries, legal identity is considered core to development, while digital systems present the opportunity to leap forward

Their analysis reveals that of the one billion who do not have legally recognised identity, 60% come from lower income countries; and that in these countries up to 45% of women don't have this recognition compared to 30% of men.¹⁶ Further, only 50% of the world's population is online at a time when digital opportunities are driving new value. For some countries, legal identity is considered core to development, while digital systems present the opportunity to leap forward with improved access to both social programmes and digital commerce.¹⁷



Many organisations in the humanitarian sector have pioneered the use of digital Identity systems in developing economies to overcome the need for bank accounts, or traditional identity documents to receive support. These systems are providing a foundation for a range of efforts, such as to protect the rights of migrant workers or to prevent trafficking of people who may not have or may be separated from their documents.

Their experience informs understanding of both opportunity and challenges. The UNHCR and the World Food Programme, among others, have deployed biometrics-based identification systems to register beneficiaries and ease the distribution of assistance. Their systems are also facilitating an ability to track the effectiveness of the response: The World Food Programme in particular set a priority on developing an “ability to understand the local context, choose the best type of assistance and, to the extent possible, predict the occurrence or reoccurrence of crises.”¹⁸ Given the prevalence of work in unstable environments, they alongside UNHCR are reported to have faced demands from governments looking to identify terrorists, while others, including Medecins Du Monde and UNICEF have been identified as targets for covert surveillance.¹⁹ Such threats, in undermining individual rights to privacy, also risk undermining confidence in the assistance.

Innovations in blockchain-based, self-sovereign systems²⁰ have helped efforts to prioritise individual's right to privacy. They have been deployed within a growing number of projects supporting vulnerable populations by using biometrics to verify access to records as well as the services they facilitate, but they haven't necessarily been designed for analysis. Some organisations including Oxfam, which commissioned a report into the use of biometrics in the humanitarian sector have officially taken

At the most basic level, a lack of trust prevents participation, risking digital transformation and associated inequities broadening, rather than closing the humanitarian divide

a “watching brief” on their use, citing a general desire for more comprehensive understanding of the potential impact on the communities they serve.²¹

This complex landscape belies the need to develop a robust understanding of emerging risks, alongside unforeseen outcomes as digital Identity systems evolve. At the most basic level, a lack of trust prevents participation, risking digital transformation and associated inequities broadening, rather than closing the humanitarian divide.

¹⁵ <https://id4africa.com/>
¹⁶ ID4D Global Dataset & Findex Survey
¹⁷ http://www3.weforum.org/docs/WEF_Our_Shared_Digital_Future_Report_2018.pdf
¹⁸ <https://www.wfp.org/analyses-and-assessments>
¹⁹ <https://www.theengineeroom.org/wp-content/uploads/2018/03/Engine-Room-Oxfam-Biometrics-Review.pdf>
²⁰ <https://www.irespond.org>
²¹ <https://www.theengineeroom.org/wp-content/uploads/2018/03/Engine-Room-Oxfam-Biometrics-Review.pdf>

Trust as a Systematic Imperative

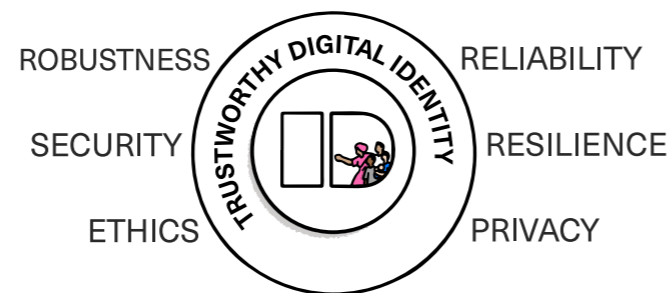
Numerous approaches to delivering digital identity systems, are supported by vast and complex ecosystems of data stores, networks and interfaces with services. Unlike the physical documents that precede them, the information associated with the use of digital identity can be interpreted to provide a wealth of information tracking an individual's movements, use of public services, consumer habits and more. National foundational identity systems can be linked to functional services, facilitating new opportunities for managing services financial transactions, crises, or public governance.

Unlike physical documents, the information associated with the use of digital identity can be interpreted to provide a wealth of information

The trust assumptions required in and of governments, service providers, and the services that rely on verifiable authentication of an individual can be poorly understood. They speak to reliance on all parties to be lawful and competent, as well as transparent, particularly with their access, management, and use of identity data.

An emotive illustration of the possibilities emerged as the COVID 19 pandemic inspired proposals to link airport facial recognition and temperature reading devices with national identity systems as a tactic for controlling the disease.²² Fierce public debate and global campaigns focus on the perceived intrusions that occur when the use of identity data evolves in this way.

Questions regularly raised include: How much information should be collected about individual citizens? What choices should they be given? What are the priorities for protecting populations?



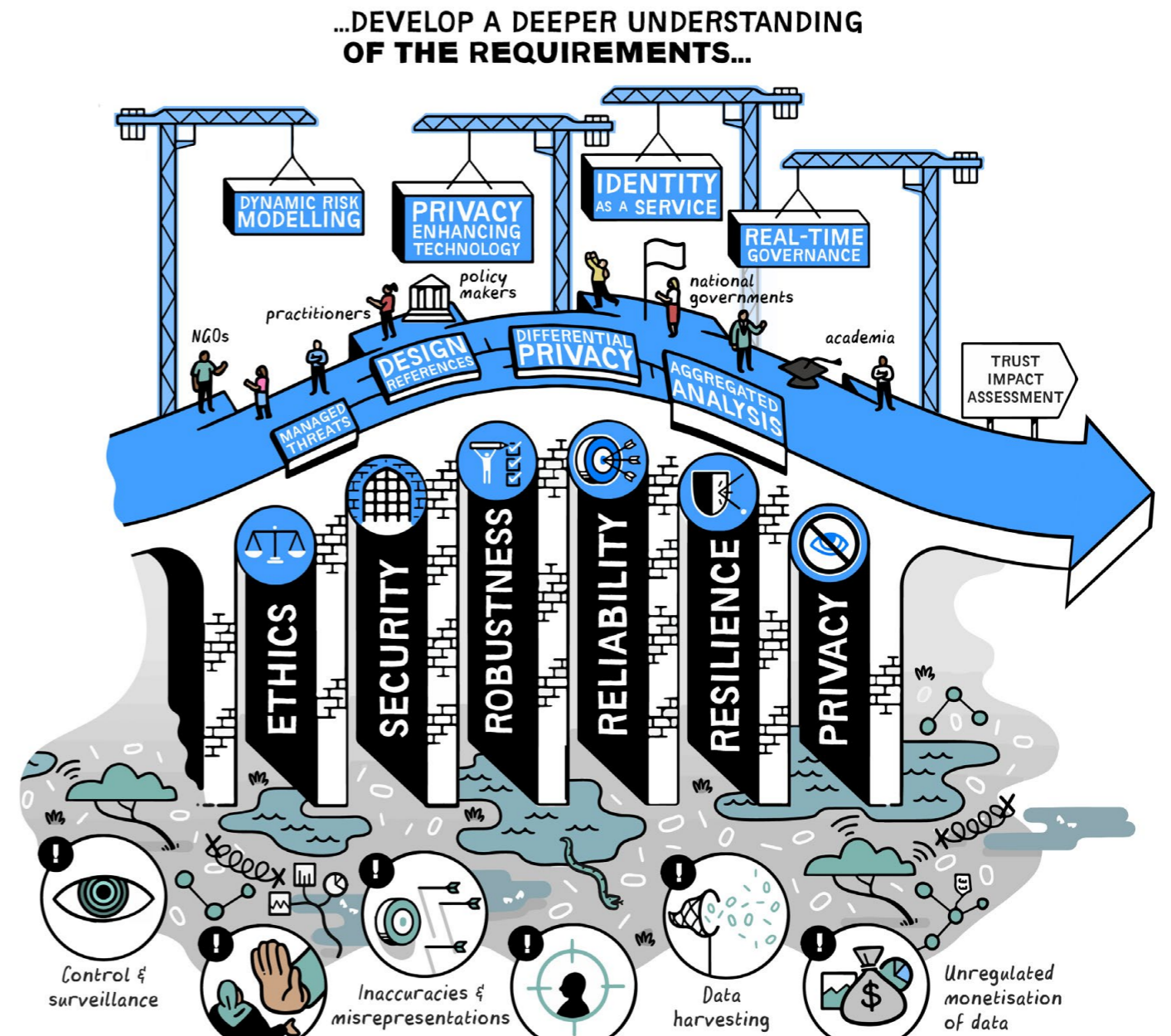
The Alan Turing Institute's Trusted Digital Infrastructure for Identity Systems project outlines six criteria for assessing the impact on the trustworthiness of the design and implementation of an identity system: security, privacy, ethics, resilience, robustness and reliability. They set out the importance of assuring transparency of purpose,

²² <https://www.biometricupdate.com/202004/uidai-proposes-public-aadhaar-facial-biometrics-and-temperature-checks-to-boost-containment-efforts>

that an individual's data remains confidential, is only accessed by those with the right to do so, is available when needed and that it retains its integrity. Resilience across the system, including supported services must also be built in to cope with and recover from unforeseen events.

The Turing project aims to produce a Trustworthy Digital Identity System Framework (TDISF) as a baseline for conducting trust impact assessments that consider the six criteria in the round. Research teams will use the Framework to survey the existing landscape and review how identity systems are being used, including the aspirations that governments have for their development.

Their effort will be supported through engagement with a contributing group of countries that are implementing digital infrastructure for identity systems. Ongoing dialogue will develop understanding of the specific challenges they face and facilitate opportunities to test technical components and benchmarks with real operational data. Engagement with humanitarian organisations, citizen groups, and in-country fieldwork will also inform the effort.



Advancing the Imperative

The Turing project is facilitating a unique opportunity to take stock and develop responses to challenging questions while highlighting practical considerations for currently abstract concepts in systems development. Academic pursuit of new understanding inherently examines opportunities for enhancing even the best of current instantiations of digital identity systems. Discrete research efforts examine how risks and their governance are evolving, and the impact on ethical responsibilities that may not have been a systematic development consideration.

Many implementations of digital identity systems came before current levels of appreciation for privacy-by-design, for example. Data protection, recently influenced by Europe's General Data Protection Regulation (GDPR), is perhaps one of the most important regulatory issues influencing digital transformation, elevating expectations for responding to the lack of attention initially given to the right to privacy.

While the GDPR has extended awareness of common principles for assuring this right, more work is needed to advance the practical considerations. Systems and

solutions available today have largely evolved within developed economies, underpinned by robust power and advances in smart phone technology and communications infrastructures.

The Trusted Digital Infrastructure project brings new perspective to this landscape. The project also offers a specific opportunity to bring forward promising advances in technologies that have yet to emerge on commercial markets. These include privacy enhancing technologies and techniques to pass on learning or verify the right to access a service, without necessarily passing on underlying data. Such techniques can facilitate encryption without the need for huge processing power or authentication without smart phones, opening up new possibilities for serving remote populations as well. They may also underpin new approaches for governments to analyse data, protect society and govern for public good within privacy preserving systems designs.

Academic pursuit of new understanding inherently examines opportunities for enhancing even the best of current instantiations of digital identity systems.

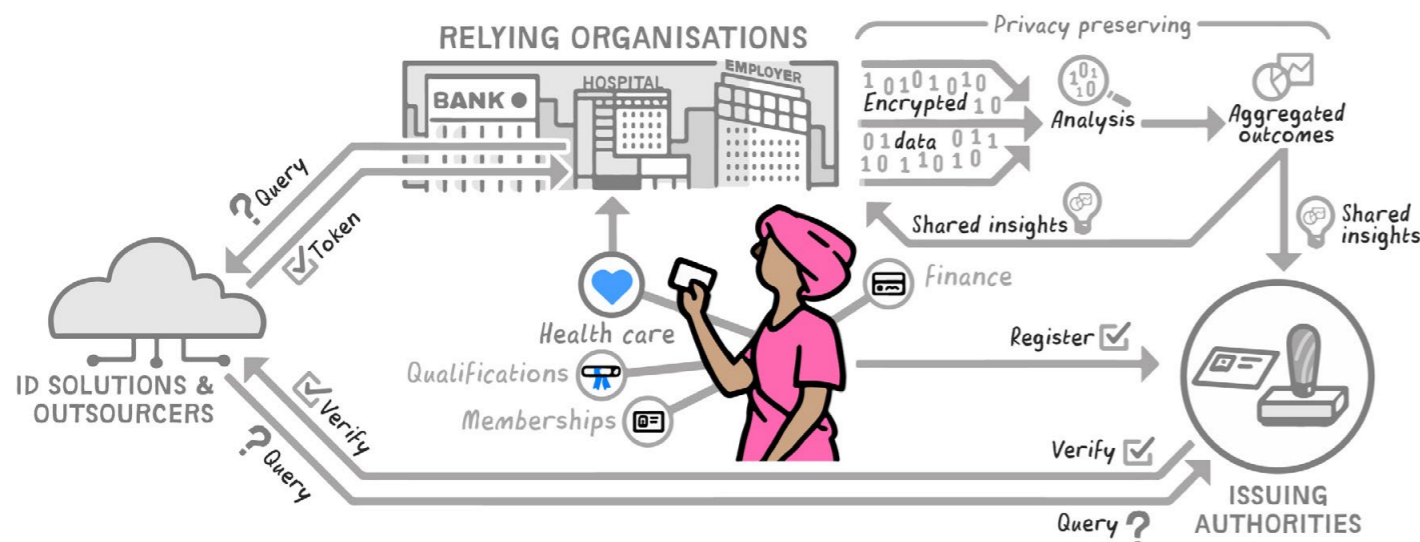
Overall, primary research is underway to advance knowledge and understanding in three core areas:

Risks: This includes modelling and simulated exercises to assess the nature of threats in public and private-sector implementations. It identifies adversaries and the techniques deployed to compromise identity systems. Risk models will then be developed using data-driven techniques to rate the likelihood and potential impact of the threats that can inform a relevant response, including the social, technical and policy decisions to be made.

Technologies: This research area assesses developments in privacy enhancing technologies, such as differential privacy and multi-party computation, and facilitates experimentation with systems architectures and approaches to Identity as a Service, including the relative contributions being made today by self-sovereign, federated and centralised approaches to identity systems. It also examines opportunities presented by open-source technologies and interfaces to enhance Interoperability and flexibility for the future.

Governance: This covers the design and development of a real-time audit and security layer that allows for maintained records about system use and behaviour, system analytics, and addresses potential threats and issues. Using machine-learning techniques, the intent is to not only monitor systems for the anomalies in fulfilling their purpose and intended operational outcomes, but also learn from and react to them.

The Alan Turing Institute's Research Engineering Group is working alongside the research teams, analysing platforms, simulating data flows and testing resilience within sandboxed environments. This presents significant opportunity to disaggregate current models and trial new designs for evolving requirements, including the technical agility needed to accommodate future advances and developing expectations. This applied area of the research is working to produce functional prototypes to be developed and tested in preparation for implementation and further analysis within real-world implementations.



Engaging a Global Community

The Alan Turing Institute (Turing) is named in honour of Alan Turing, whose pioneering work in theoretical and applied mathematics, engineering and computing is considered to have laid the foundations for modern-day data science and artificial intelligence. It brings together over 400 academics from the UK's leading universities and hosts visiting fellows and researchers from over 16 international centres of academic excellence. Research into data science, artificial intelligence, and privacy enhancing encryption is delivering significant impact in the fields of health care, national security, finance, and criminal justice. Multi-disciplinary research activities in these areas involve collaborations with major national and international organisations, including the United Nations Development Programme.

The principal investigators driving this project are renowned for their work across privacy, security, and computing science:

Professor Mark Briers, Director of Defence and Security program at the Alan Turing Institute and Honorary Senior Lecturer, Imperial College London

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

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

As a global collaborative effort, the Trusted Digital Infrastructure for Identity Systems project is working to develop tangible impact by maturing collective appreciation for the design and development opportunities to be had, and the policy choices to be made in upholding trust as a systematic imperative. An International Advisory Board assures a focus on current demands and aspirations that are driving development in national identity programmes. Founding members draw from global organisations advocating identity as a development imperative, including the World Bank Group ID4D and ID4Africa, and field practitioners:

Dr. Joseph Atick, chairman and co-founder of ID4Africa, and founder and chairman of Identity Counsel International (ICI)

Vyjayanti Desai - Programme Manager, Identification for Development (ID4D) at World Bank Group

Dr. Michiel Van Der Veen - Director of Innovation & Development, National Office for Identity Data, Netherlands

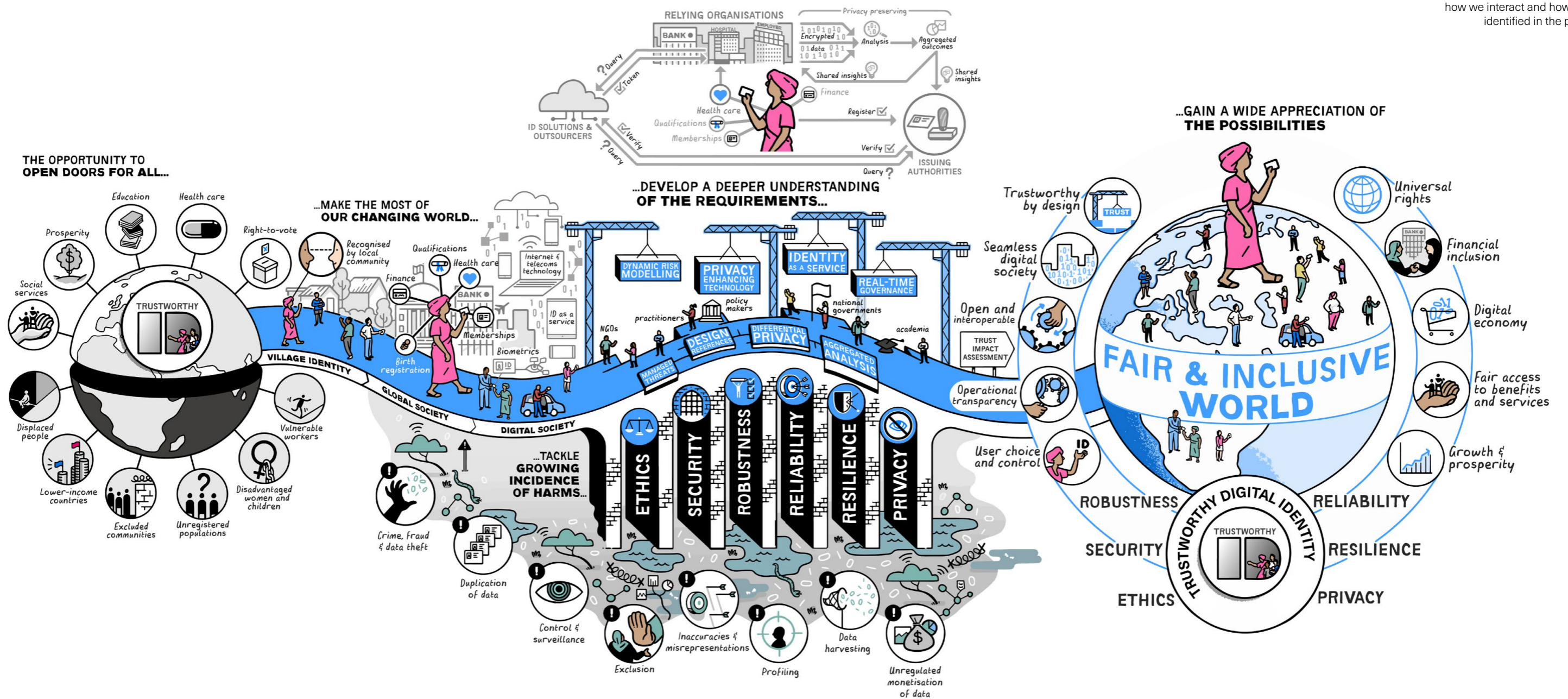
Dr. Pramod Varma – Chief Architect of Aadhaar, Aadhaar a digital identity project serving a population of 1.3 billion

Further perspective and collaborative support is curated through the influence of a technical academic working group, events and workshops to engage the strongest academic ideas from across the Turing's reach.

As a global collaborative effort, the Turing project is working to develop tangible impact by maturing collective appreciation for the design and development opportunities to be had...

Trustworthy Digital Infrastructure for Identity Systems

Society's norms continue to evolve with digital transformation significantly picking up the pace and now bringing revolutionary change to the economic opportunities that lay before us, how we interact and how we are identified in the process.



This initiative has received initial funding through a grant from the Bill & Melinda Gates Foundation.
This document was prepared by Lyndsay Turley with the support of the project team

Follow the progress **#trustworthyidentity**

<http://www.turing.ac.uk/research/research-projects/trusted-digital-infrastructure-identity-systems>

Twitter **@turinginst**

LinkedIn **[school/the-alan-turing-institute/](https://www.linkedin.com/school/the-alan-turing-institute/)**