WORLD ECONOMIC FORUM

COMMITTED TO
IMPROVING THE STATE
OF THE WORLD

Insight Report

Identity in a Digital World
A new chapter in the social contract

September 2018

“

Our identity is precious; any digital identity program must be based on enabling meaningful trust, control and accountability. Yet even agreeing these principles are proving hard - implementing them will be even more so because of a confluence of political, economic, technological, cultural, legal and social factors.

”

Amanda Long, Director-General, Consumers International

“

Each individual is unique. There are many factors that define us and our health, ranging from our genes and the way we manage our own health, to the environment and social context in which we each live. It is vital to create a secure information infrastructure where our Digital Identity can enable research to find new cures and optimized care pathways, as well access to quality care.

”

Jeroen Tas, Chief Innovation and Strategy Officer, Royal Philips

“

If designed well, digital identities can foster inclusion in almost all aspects of lives in transformational ways. For small holder farmers, they hold the potential to help overcome the pervasive issues of social, economic and geographic isolation, and fragmentation which are at the root of poverty. And do so at an unprecedented scale.

”

Ishmael Sunga, Chief Executive Officer, South African Confederation of Agricultural Unions (SACAU)

“

We must finally learn that there are no technological solutions to complex socio-economic problems. We should pause and understand the reasons why identity is a barrier to so much, and remove unnecessary barriers instead of resorting to complex identity systems. We also need to safeguard against political and financial wills that build identity systems for efficiency and targeting, instead of the well-being of individuals.

”

Gus Hosein, Executive Director, Privacy International

“

We want everyone to thrive in the digital world - no one should be left behind. That means educating everyone on how to keep themselves and their data safe online, which is something that we at Barclays are very passionate about. But it also means ensuring universal access to a safe, secure and easy to use digital identity, so that everyone can confidently unlock the benefits of the digital economy.

”

Jes Staley, Barclays Group Chief Executive Officer, Barclays

“

Digital identity is a powerful force for both positive and negative human experience. To create a digital identity system that is positive and sustainable for the long term we must develop user-centered solutions that enhance user safety, control and benefit.

”

Mitchell Baker, Chairwoman of the Board, Mozilla Foundation and Mozilla Corporation

“

We are on the threshold of a new model of digital identity that expands beyond individuals to organizations, ‘things,’ devices and places. It will provide the foundation by which our digital selves will interact with online systems, control our connected devices, leverage the learnings of applied intelligence and protect the earth’s resources. Getting this right is critical to our future growth, responsibly harnessing technology innovation and enabling a better, more responsible digital life.

”

Paul Daugherty, Chief Technology and Innovation Officer, Accenture

World Economic Forum
91-93 route de la Capite
CH-1223 Cologny/Geneva
Switzerland
Tel.: +41 (0)22 869 1212
Fax: +41 (0)22 786 2744
Email: contact@weforum.org
www.weforum.org

Contents

Foreword

Derek O’Halloran, Head – Future of Digital Economy and Society, Member of the Executive Committee, World Economic Forum

As more people, devices and associated personal data get online, there is growing focus on a foundational element of this new digital environment – our identities. The ability to prove we are who we say we are will increasingly determine our opportunities to establish trust with each other and to carry out meaningful interactions in a digital economy.

All over the world, a growing number of organizations – from the public and private sectors – are advancing systems that establish and verify digital identities for people, devices and other entities. This community is expanding in scope, growing beyond traditional identity practitioners to include a broader set of actors exploring the promises and perils of digital identities – from domains such as healthcare, financial services, humanitarian responses and more.

Yet we are still learning what “identity in a digital world” means. We are also still evolving policies and practices on how best to collect, process or use identity-related data in ways that empower individuals without infringing on their freedoms or causing them harm. There is significant room to improve how identity data is handled online, and how much control individuals have in the process.

At the World Economic Forum’s Annual Meeting 2018 in Davos, a diverse group of public and private stakeholders committed to shared cooperation on advancing good, user-centric digital identities. Since then, a broader group of stakeholders has joined this conversation: experts, policy-makers, business executives, practitioners, rights advocates, humanitarian organizations and civil society.

This publication reflects their collective insights, synthesized and translated into a format useful for decision-makers and practitioners. It takes stock of where we are today and identifies gaps in coordination across sectors and stakeholders. It outlines what we’ve learnt to date on what user-centricity means and how to uphold it in practice. It attempts to offer a shared working agenda for leaders: an initial list of immediate-term priority actions that demand cooperation. It reflects, in short, the first stage in collective learning and the creation of shared goals and paths.

We urgently need deeper cooperation to shape user-centric identities; otherwise, we risk aggravating or creating digital divides, as well as failing to provide citizens and consumers with the opportunities that the Fourth Industrial Revolution presents.

We hope this publication serves as a reference point to advance such cooperation.

Executive summary

Our identity is, literally, who we are, and as the digital technologies of the Fourth Industrial Revolution advance, our identity is increasingly digital. This digital identity determines what products, services and information we can access – or, conversely, what is closed off to us.

As digital services explode, and billions of elements in our everyday lives become connected to the internet, individuals are losing control of how they are represented digitally in their interactions with institutions. Others lack any digital identity at all, essentially excluding them from digital life.

The result is a challenge to the social contracts that govern the relationships between individuals and institutions in a digital world.

If we fail to act now, we could face a future in which digital identity widens the divide between the digital haves and have-nots, or a future where nearly all individuals lack choice, trust and rights in the online world.

If we act wisely today, digital identities can help transform the future for billions of individuals, all over the world, enabling them to access new economic, political and social opportunities, while enjoying digital safety, privacy and other human rights.

This report explores some ideas for how to achieve that better future, starting with a transformation that puts value on the individual at the centre.

The need for shared understanding and coordinated action

Digital identities have evolved. They are no longer simple and isolated pieces of information about individuals, but complex webs, crossing the internet, of their personal data, digital history and the inferences that algorithms can draw from this. Our digital identities are increasingly embedded in everything we do in our daily lives.

Verifiable digital identities create value for businesses, governments and individuals alike. Yet there is a lack of shared principles, standards and coordination between various stakeholder efforts in this rapidly evolving landscape.

The five elements of user value

At the World Economic Forum's Annual Meeting in Davos 2018, a community of stakeholders from government, business and civil society made a commitment to advance towards a "good" future for digital identities. Since then, a broader group has joined the conversation and identified an initial set of five elements that a good identity must satisfy. All five are equally important, and tensions exist between some: for instance, features to enhance security for individuals and their identities may reduce their convenience. User-centric digital identities – that deliver real value to individuals and therefore drive adoption – must succeed in all aspects.

1. **Fit for purpose**. Good digital identities offer a reliable way for individuals to build trust in who they claim to be, to exercise their rights and freedoms, and/or demonstrate their eligibility to access services.

2. **Inclusive**. Inclusive identity enable anyone who needs it to establish and use a digital identity, free from the risk of discrimination based on their identity-related data, and without facing authentication processes that exclude them.

3. **Useful**. Useful digital identities offer access to a wide range of useful services and interactions and are easy to establish and use.

4. **Offers choice**. Individuals have choice when they can see how systems use their data and are able to choose what data they share for which interaction, with whom and for how long.

5. **Secure**. Security includes protecting individuals, organizations, devices and infrastructure from identity theft, unauthorized data sharing and human rights violations.

Today, there are three main archetypes of identity systems in the world. In the most traditional and commonly seen "centralized" archetype, institutions – governments or enterprises – establish and manage identities and related data in their own systems while in a second "federated" archetype, this role is shared among multiple institutions. Systems that follow the newest "decentralized" archetype, mostly still in the pilot stage, seek to give individuals greater control to manage their own identity data.

Priorities for collaboration

Government, private-sector and civil society communities from the World Economic Forum network have identified six priority areas for collaboration to help shape digital identities of the future:

- Moving the emphasis beyond identity for all to identities that deliver user value
- Creating metrics and accountability for good identity
- Building new governance models for digital identity ecosystems
- Promoting stewardship of good identity
- Encouraging partnerships around best practices and interoperability where appropriate
- Innovating with technologies and models and building a library of successful pilots

As the International Organization for Public-Private Cooperation, the World Economic Forum offers a platform for such collaboration that advances the practice of "good" identities and maximizes value to individuals.

How to use this publication

Chapter 1 explains the importance of digital identities: why they may determine whether digital technologies increase inequality or promote sustainable, shared prosperity. It also offers a brief overview of existing and emerging digital identity systems.

Chapter 2 explores what a good identity system, which delivers the five key elements of value to individuals, could look like. It examines how to achieve these elements of value and considers their application through real-world examples.

Chapter 3 examines the emerging trends, opportunities and challenges for designers, policy-makers and other stakeholders to consider as they advance towards good digital identities.

Chapter 4 identifies and explores six priority areas for near- and medium-term collaboration among the World Economic Forum's multistakeholder community.

An appendix offers design considerations for practitioners setting out to build digital identity systems.

Note: This publication is not a comprehensive representation of all of the World Economic Forum stakeholder gatherings and conversations about digital identity. It focuses on the digital needs of individual human beings. Many topics, such as pseudonymous and anonymous access systems, remain part of the ongoing dialogue, but are not covered in depth in this publication. Others, such as the representation of devices, legal entities and artificial intelligence (AI) are touched on here, but they will require a deeper exploration into how they relate to individuals – thereby influencing personal identity – as well as into their other unique challenges.

Chapter 1: The case for good digital identity

Identity – shaping social contracts

Nothing is as fundamental to human beings as identity. Our identity is, literally, who we are: a combination of personal history, innate and learnt beliefs and behaviours, and a bundle of cultural, family, national, team, gender or other identities. However we understand it, identity always matters.

Our identity is important because it exists in relation to others. It exists in relation to the economic and social structures in which we live. How we are represented in economic, political and other societal systems – and our degree of choice and control as to how we are represented in these systems – sets the parameters for the opportunities and rights available to us in our daily lives.

Throughout history, we see again and again hard-fought battles and revolutions where individuals demand recognition and rights. From "no taxation without representation" to the ending of apartheid, how individuals are represented in society has been the bedrock for reimagining and renegotiating the rights, freedoms and responsibilities of individuals and the organizations to which they relate. The earliest definitions of the polis and citizen in Ancient Greece, the Magna Carta and the US Constitution were all acts that defined the social contracts between people and institutions.

Whether we want it or not, our identity is increasingly digital, distributed and a decider of what products, services and information we access. This identity online is not simply a matter of a website login or online avatar – it is the sum total of the growing and evolving mass of information about us, our profiles and the history of our activities online. It relates to inferences made about us, based on this mass of information, which become new data points.

Today, the average internet user has 92 online accounts, and is likely to have over 200 by 2020.[1] The drivers for most of these online "logins" and related data are near-term goals of institutions to improve efficiency or enhance revenue relating to specific services. Each may be well intentioned. However, when combined, the explosion of digital services and the lack of common norms mean that the systemic effect is greater than the sum of its parts. The result for individuals is a decreasing understanding of or control over how they are represented online. With that digital representation determining so much of how we live our lives, these changes add up to a rewriting of the social contract, and we are barely even aware of it.

Any discussion on shaping digital identities should start and end with the individual – one who is born into a fully digital world – and what these identities mean for that person's future. We must design trust into systems from the outset. We need to be able to understand what "good" looks like, based on values that respect individual freedoms. With digital interactions accelerating – including the billions of "things" that are being connected to the internet – we urgently need to translate these values into guidance for those implementing digital identity systems the world over. These systems must include programmes in developing countries that aim to bring basic services and inclusion to the most impoverished. Digital technologies aside, an estimated 1.1 billion people globally have no formal identity at all – an issue set for the world to address by 2030 through Sustainable Development Goal 16.9.[2] Technology can play a pivotal role in achieving this goal, providing access to healthcare and education, and bringing financial and social inclusion to families and new generations worldwide. There is no time to waste, though we must also remember that a poorly designed digital identity can be worse than no identity at all. We need to safeguard against the possibility of making the lives of the most vulnerable people on the planet even more vulnerable.

We need norms, and a shared understanding of what a good digital identity looks like. This paper is offered as a first step in that direction.

Digital identities in our daily lives

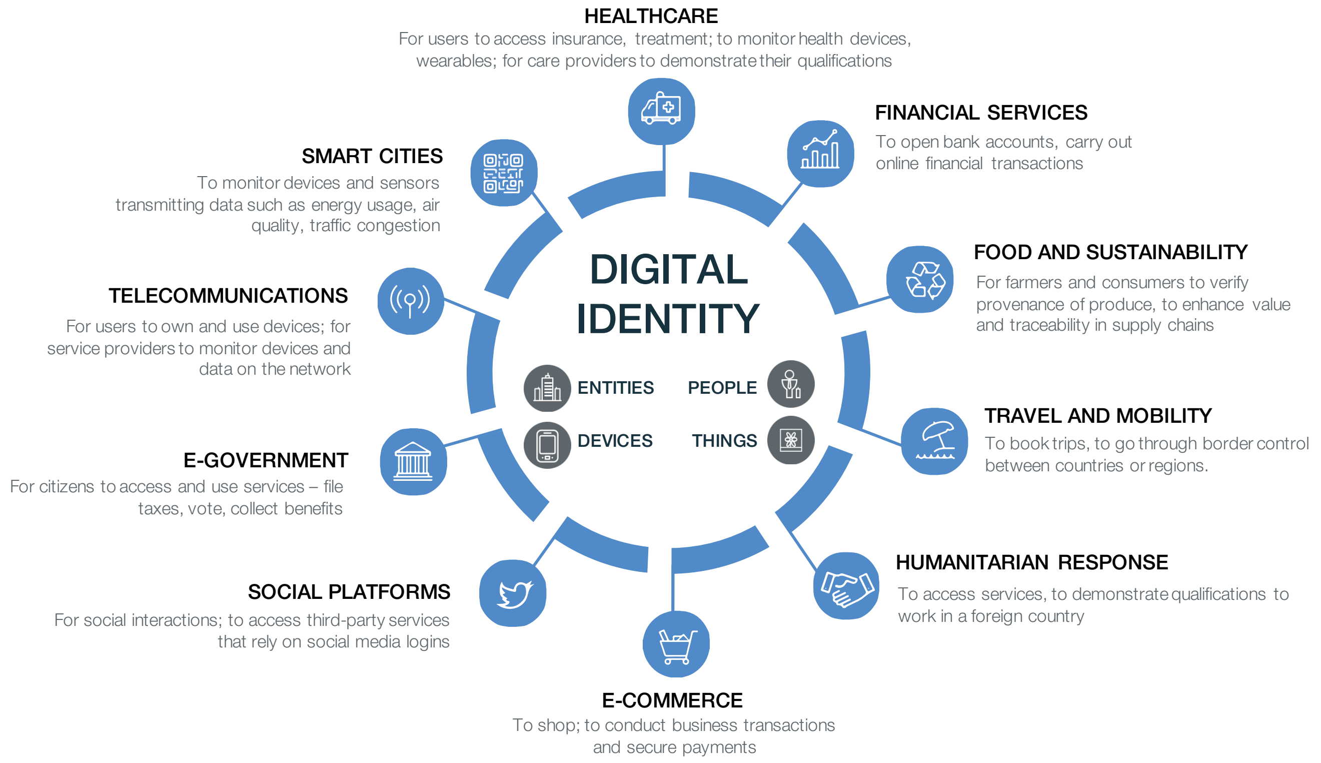
As digital connectivity and the online activities of individuals grow, our digital identities are increasingly embedded in everything we do in our daily lives. Every day, we go through authentication processes that give others confidence in our assertions of who we claim to be, or our right to interact with or use a service. We use account logins or biometrics such as facial recognition or eye or fingerprint scans to access services and carry out digital interactions. We have expanding digital profiles consisting of permanent, unchosen qualities such as place of birth or biometrics and assigned attributes, for instance, our names or government ID numbers.

Digital identity: Evolving scope

- **Authentication**: processes that determine if authenticators used (e.g. fingerprints, passwords) to claim an identity are valid
- **Profile**: may include inherent data attributes (such as biometrics) or assigned attributes (such as names or national identifier numbers)
- **History**: credit or medical histories, online purchasing behaviours
- **Inferences**: judgements or decisions made based on authentication processes, profiles and histories (e.g. a bank decides the attractiveness of an individual for a loan)

Over time, our interactions create digital trails or histories of our personal data and behaviours online: our financial, tax, purchase, legal, medical and credit histories, among others. Individuals and institutions are increasingly using such historical data, as well as our profiles and data from external sources, to make inferences that may inform judgements or decisions. For example, a vehicle insurer may look at driving and legal records, credit history and age to verify customers' identities and assess whether they are high or low risk.

Figure 1: Identity in everyday lives


HEALTHCARE
For users to access insurance, treatment; to monitor health devices, wearables; for care providers to demonstrate their qualifications
FINANCIAL SERVICES
To open bank accounts, carry out online financial transactions
SMART CITIES
To monitor devices and sensors transmitting data such as energy usage, air quality, traffic congestion
FOOD AND SUSTAINABILITY
For farmers and consumers to verify provenance of produce, to enhance value and traceability in supply chains
TELECOMMUNICATIONS
For users to own and use devices; for service providers to monitor devices and data on the network
DIGITAL IDENTITY
ENTITIES
PEOPLE
DEVICES
THINGS
TRAVEL AND MOBILITY
To book trips, to go through border control between countries or regions.
E-GOVERNMENT
For citizens to access and use services – file taxes, vote, collect benefits
HUMANITARIAN RESPONSE
To access services, to demonstrate qualifications to work in a foreign country
SOCIAL PLATFORMS
For social interactions; to access third-party services that rely on social media logins
E-COMMERCE
To shop; to conduct business transactions and secure payments

For businesses, verifiable identities create new markets and business lines, better customer experiences, improved data and a tool against fraud. For governments, they offer a new way of governing: better delivery of services, a more engaged citizenry and a tool against corruption and crime. For individuals, they open up (or close off) the digital world, with its jobs, political activities, education, financial services, healthcare and more.

Growing complexity, and responsibility

As our digital identities evolve, as more service providers rely on verifying identities, and as unprecedented levels of personal data become scattered across the web, there are new challenges facing leaders in business, government and civil society.

– Delivering user value and sustaining trust: In an effort to give users convenient, personalized services, and to manage growing risks such as identity theft, service providers are relying more and more on large amounts of data from multiple sources to reliably and seamlessly authenticate individuals. The associated responsibility this brings to uphold the privacy and security rights of users, and the necessity to retain their trust, is not easy to manage. Different cultural perceptions of privacy and personalization make this challenge even more acute. Governments are increasingly advancing digital identity systems to support multiple goals: efficient public service delivery, sustained rule of law and robust democratic processes. At the same time, they also have a growing responsibility to ensure that systems and processes do not lead to unconstitutional intrusions into a citizen's or resident's privacy, or become a tool for unwarranted surveillance, discrimination and abuse. Prioritizing the needs and rights of individuals offers benefits for institutions too: more valued and trusted products that win more widespread adoption.

– Avoiding fragmentation, and harmonizing standards: The world today has a host of different identity systems, run by government agencies, banks, retailers and other organizations. Each gathers and uses identity data on users for its own purposes, such as forming electoral rolls or health insurance premiums. Most individuals provide similar sets of basic information to many such organizations during their lives; they have multiple "versions" of themselves online. But these systems typically do not communicate. They operate in isolated digital groups that increase costs, inefficiencies and friction. Enhancing interoperability between systems could address these challenges and enhance the individual's experience. At the same time, it is important to consider the security and privacy implications of stand-alone and interoperable systems alike. With systems serving various purposes, requiring varied identity assurance levels and data, and their designs being influenced by diverse technical, policy, cultural and geographic contexts, it is clear that there will be no universal, "one-size-fits-all" identity solution. Yet it is important that there are shared principles and standards guiding the design and implementation of systems across the world. The challenge is to enhance the experience and value for all involved, while also strengthening privacy and security.

Divergent futures

We are building and expanding digital identities on a daily basis – and pulling more and more people into the digital era. Given the foundational role that identity plays in a digital society, we can easily imagine radically different paths emerging in the near and medium term. Our choices and decisions on the design and execution of digital identity systems today will determine which elements of these possible futures will occur tomorrow.

Future No. 1: Digital haves and have-nots, and intergenerational exclusion

In an environment of rapid technological evolution, adoption and innovation, the benefits of the digital economy are exponential. Those who can use it to their advantage stand to reap transformative benefits. Those who cannot, face the risk of being left behind. In the absence of focused and thoughtful efforts to include those excluded today, the gap between the digital haves and have-nots may grow ever wider and perpetuate from generation to generation. Today, half of the world's population – over 4 billion people[3] – have no reliable connection to the internet and its opportunities. Over 1.1 billion remain "invisible": they have no legally recognized form of identity, online or offline. This highly unequal playing field for individuals is often layered on top of existing gender, income and geographic divides. We urgently need to address the question of inclusion to avoid creating structural inequality and two digital classes of humans.

Future No. 2: No choice, no trust, no rights

Another foreseeable future is one in which everyone is included – in a world of powerlessness and vulnerability. If individuals have no real understanding of or control over their online identities, and how their identity data may be used or misused, their ability to shape opportunities and benefits in a digital economy will be limited. Worse, individuals interacting with systems that offer little privacy or data protection may find themselves vulnerable to security risks and new forms of exclusion. In this future, governments or enterprises running identity systems or managing personal data may risk losing the trust of their consumers or citizens.

Future No. 3: Transformative inclusion

If designed for an inclusive and user-centric future, identities translate into opportunity, value, safety and respect for individual freedoms. They could enable systemic transformations across almost every area of our lives, from health to education, from social inclusion to financial inclusion.

To take one example where there is growing energy and innovation: digital identity can transform healthcare systems. As people live longer, more chronically ill patients and ageing populations will need support. We will need to rethink healthcare delivery models and transcend traditionally isolated data-storage systems to enable a more efficient, patient-centric approach. We need to create a secure information infrastructure that can enable research to find new cures and optimized care pathways, as well as access to quality care. By connecting people, data and systems, we can create a network that allows information to flow seamlessly across care providers, locations and systems.

Today, most patients have little or no ownership over their health records. Many technology-related barriers still exist, such as standardization, data access, interoperability and identity management. When solved, our individual digital identity will be at the core of healthcare transformation. If patients and their medical devices can be securely identified and authenticated anywhere, and vital medical data accessed with robust consent management, the foundations for a new wave of medical innovation will be set.

Or take the case of food systems: digital identity can empower millions of smallholder farmers and promote economically sustainable livelihoods. Many small-scale farmers across the world today struggle to make a living. Incomes are unpredictable, and they often receive just a tiny share of the price paid by the consumer for their produce. Yet there is growing consumer interest in verifying that produce is farmed using sustainable practices.

New technologies such as Internet of Things (IoT) that establish and verify identity of produce can enable an end-to-end supply-chain traceability model. This helps offer the consumer transparency into the produce's life cycle, from its origins to its travels and transformation across the supply chain. With enhanced transparency and trust, the consumer can also directly reward farmers with premium prices for a superior product. Such a model can create compelling incentives for actors across the supply chain to adopt sustainable practices.

Identification vs. authentication

Identification is the process of establishing who an entity is within a given population or context. It often takes place through *identity proofing*, which verifies and validates attributes (such as name, birth date, fingerprints or iris scans) that the entity presents.

Authentication is the process of determining if the authenticators (such as a fingerprint or password) used to claim a digital identity are valid – that they belong to the same entity who previously established the identity.

Five elements of 'good' identity

At the World Economic Forum's Annual Meeting in Davos 2018, a community of stakeholders from government, business and civil society made a commitment to advance towards a "good" future for digital identity.

In the months since, this community has identified an initial set of five elements that a "good" identity must satisfy. All five are equally important. A user-centric digital identity – one that delivers real value and therefore drives adoption – must succeed in all aspects.

These elements can build on each other, but tensions exist between some: security measures, for example, may make convenience more challenging for designers. Part of the shared vision that stakeholders must build is an understanding of how best to manage these trade-offs.

1. **Fit for purpose**. A good digital identity offers a reliable way for individuals to build trust in who they claim to be, to exercise their rights and freedoms and/or in their eligibility to carry out digital interactions. With more and more digital transactions between people with no preexisting relationships and involving AI bots, this process is a growing challenge.

2. **Inclusive**. An inclusive digital identity enables anyone who needs it to establish and use a digital identity, free from the risk of discrimination based on their identity-related data, and without facing processes that exclude them.

3. **Useful**. A useful digital identity offers access to a wide range of useful services and interactions and is easy to establish and use. At present, many digital identities have onerous and repetitive requirements and limited uses.

4. **Offers choice**. Individuals have choice when they can see how systems use their data and are empowered to choose what data they share for which interaction, with whom, and for how long. Such control is currently rare. In its absence, individuals increasingly face the risk of privacy breaches, identity theft, fraud and other abuses.

5. **Secure**. Security includes protecting individuals, organizations, devices and infrastructure from identity theft, unauthorized data sharing and human rights violations. Such security is often inconsistent at present, in part because identity information is scattered throughout the digital sphere.

Identity systems today: Three archetypes

Identity systems today – and the emerging identity systems of tomorrow – typically fall into three archetypes: centralized, federated and decentralized. As the names indicate, it is their fundamental structure that sets them apart from each other, with implications for adoption and trust levels, and advantages and challenges for individual users.

In the most traditional and commonly seen centralized archetype, institutions – governments or enterprises – establish and manage identities and related data in their own systems while in a second, federated archetype, this role is shared among multiple institutions. Systems that follow the newest, decentralized archetype, mostly still in the pilot stage, seek to give individuals greater control to manage their own identity data.

Figure 2: Five elements of good identity

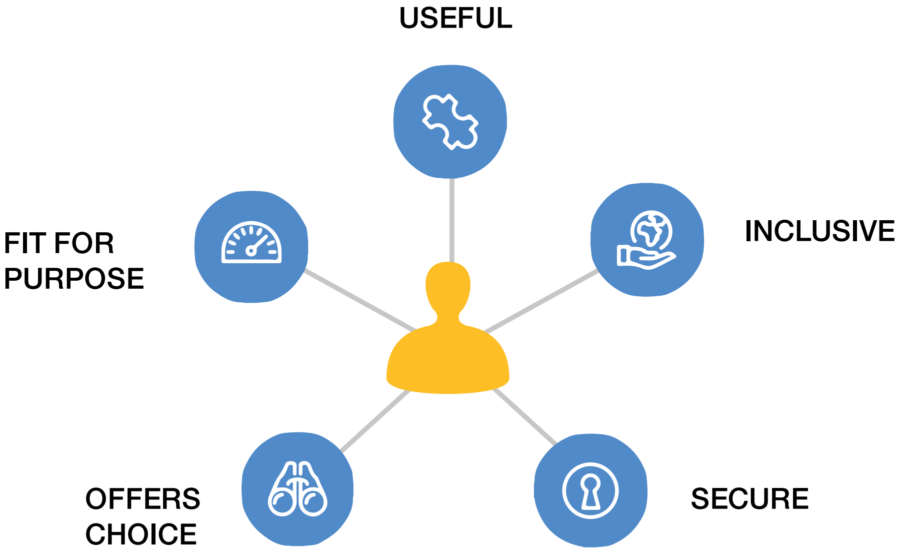


Figure 3: Three identity system archetypes

SYSTEM ARCHETYPES	CENTRALIZED	FEDERATED	DECENTRALIZED
DEFINITION	• A single organization establishes and manages the identity	• Different stand-alone systems, each with its own trust anchor, establish trust with each other	• Multiple entities contribute to a decentralized digital identity; user controls sharing of identity data
EXAMPLES	Government electoral roll, bank, social media platform	Sweden's BankID, GOV.UK Verify	Government of Malta education pilot, city of Antwerp pilot
LEVEL OF ADOPTION AND TRUST	Adoption dependent on value; trust dependent on system owner and identity proofing	Adoption dependent on establishing trust relationship; trust dependent on identity proofing	Adoption currently in early stages (pilot, proof-of-concept). Trust dependent on trust anchors and attestations
STRENGTHS	Can be built with specific purpose in mind; potential for organizational vetting of identity data	Users can access a wider range of services; efficiency for organizations	Increased user control and reduced amount of information collected and stored by organizations
CHALLENGES	Generally low user control; centralized risk and liability; potential for abuse	Generally low user control; high technical and legal complexity	Governance model, acceptance and participation is complex; evolving landscape; complex liability

Centralized

Definition

In these traditional identity systems, an individual uses the services of an organization that owns or manages the system. The system owner or manager (such as a third-party technology provider, acting on the owner's behalf) captures, uses and stores the individual's identity and related data. The system owner or manager supports individuals' transactions with service providers and other relying parties. The system owner could be a government (such as Estonia's e-ID or India's Aadhaar) or a private-sector organization, such as a bank or social media company.

Level of trust and adoption

Adoption of some centralized identity systems is widespread. Governments have widely adopted such systems, in some cases because the law mandates their use. Many individuals use social media platforms whose identity systems also offer authentication services (e.g. "log in with Facebook") to access other enterprises' services. Banks too offer identity systems that many individuals use to access financial services.

Identity systems from governments or heavily regulated sectors such as financial services often carry out robust identity proofing; relying parties and individuals often trust these systems for high-risk transactions. In systems where identity proofing is limited – in some social media platforms it is easy to create multiple or fraudulent identities – trust is also limited, thus curtailing the types of transactions that could be carried out using the identity provided. Yet some digital platforms are evolving to serve the authentication needs of a wider range of service providers, such as the ongoing pilot involving WeChat and the government of China.

Strengths

Individuals, once established in the system, can access the system owner's offerings, whether public services, banking services or social media networks. The system owner determines the level of due diligence carried out for identity proofing based on regulation and compliance requirements, risk appetite and policies, potentially creating strong levels of assurance for individuals. The owner can also act as a gatekeeper, reducing the spread of false information. Many owners reach agreements with other relying parties to accept the identity documents that are issued to the individuals such as passports, ID cards or bank statements, offering individuals access to more services.

Challenges

Centralized systems typically offer individuals little choice over how their personal data is used. Some support just a few types of transactions and lack interoperability with other systems. Centralized architectures may represent "honeypots" of individuals' identity data – attractive targets for hackers – and they may concentrate risk and liability with the system owner. Centralization also gives owners power that, if unchecked, leaves the door open for abuses such as surveillance, tracking and profiling; exclusion and discrimination; or political repression of individuals.

Who's who in digital identity

Historically an "identity ecosystem" often had just two participants: two people who recognized each other. Today, a digital identity ecosystem has many different actors:

- **The individual** who needs a digital identity to safely access digital systems and transactions
- **Entities** such as devices, groups of devices, legal entities and physical and virtual assets that individuals may own or use, and which also need digital identities
- **Trust anchors**, authoritative sources of identity proofing
- **The controller or delegate of the identity data**, typically a trust anchor (such as a government) that issues and/or has the ability to control the identity data
- **The operator of the identity system**, who may be the entity that issues and owns the identity, or who may be a separate organization (such as a third-party technology service provider) that acts on behalf of the system owner
- **Relying parties**, the organizations that rely upon digital identities to allow or deny access to goods, services, or data
- **Custodians or guardians**, whom an identity subject empowers to act on his or her (or its) behalf
- **Regulators**, who mandate and/or guide how to manage and use identities

Federated

Definition

When two or more centralized system owners establish mutual trust– either by distributing components of proofing and trust, or by mutually recognizing each other's trust and proofing standards – a federated identity system results. Governments or international bodies, for example, may establish common standards and agree to accept each other's digital identity systems – such as eIDAS provides for in the European Union,[4] or as ICAO standards do for international cross-border travel.[5] Enterprises may agree to accept each other's credentials and thus the standards that are used in identity proofing, such as many banks (as well as other organizations) do in Sweden's BankID,[6] or as a number of public and private institutions do through GOV.UK Verify in the United Kingdom. The different system owners usually establish one-to-one trust through legal agreements and/or technical standards. The network grows as the number of trusted one-to-one relationships increases.

Level of trust and adoption

Some federated identity systems are widely adopted. Individuals often like the convenient access to multiple systems that this archetype can provide. However, the complexity of building one-to-one trust relationships between system owners can limit implementation.

As with centralized systems, trust levels vary according to the system owners involved and the degree of identity proofing and data vetting that they perform.

Strengths

Federated networks can offer individuals access to a wider range of transactions, using a single set of credentials, compared to solitary centralized systems. This interoperability provides greater convenience for users. It can also help the system's multiple owners manage individuals' identities and access more efficiently.

Challenges

Like centralized systems, federated systems may give individuals little choice over how their data is used. For the system owners, complexity arises from the potential need for legal agreements, including the division of risks and liabilities, and for shared data and technical standards. This complexity may make implementation expensive and keep the system from including many of the services that individuals would like to access.

Decentralized

Definition

Decentralized identity systems don't depend on a single system owner or set of owners to establish and manage identities. Instead, they usually consist of a digital device, owned by an individual, and an identity data store, also managed by the individual. This data store – often the user's device memory or cloud storage – holds attestations from traditional trust anchors, such as governments or banks, as well as from other trust anchors such as employers, retailers, media outlets or personal relations. The individual chooses which attestation or data attribute to share and with whom to share it.

Level of adoption and trust

This archetype is new and exists mostly in the pilot and proof-of-concept phases.

In the public sector, the government of Malta is piloting a program where, using blockchain technology, educational institutions can issue credentials (such as diplomas and professional certifications) to an individual, who can access and manage them through a mobile application.[7] The city of Antwerp has piloted a system for individuals to create and manage a through-life identity on a mobile application employing blockchain technology, starting with identity attestations at birth from doctors, hospitals and the government birth registry.

In the private sector, banking consortiums are piloting shared know-your-customer and other decentralized identity frameworks. Several airline loyalty programmes and insurance companies are experimenting with similar initiatives, aiming at achieving greater efficiency for the enterprise and greater control for the individual.

Trust levels vary depending on the attestations in the data store – which come from different trust anchors – and on which of these attestations the individual chooses to share. An individual who shares an attestation from a government, for example, may create more trust than one who shares an attestation from a personal relation.

Strengths

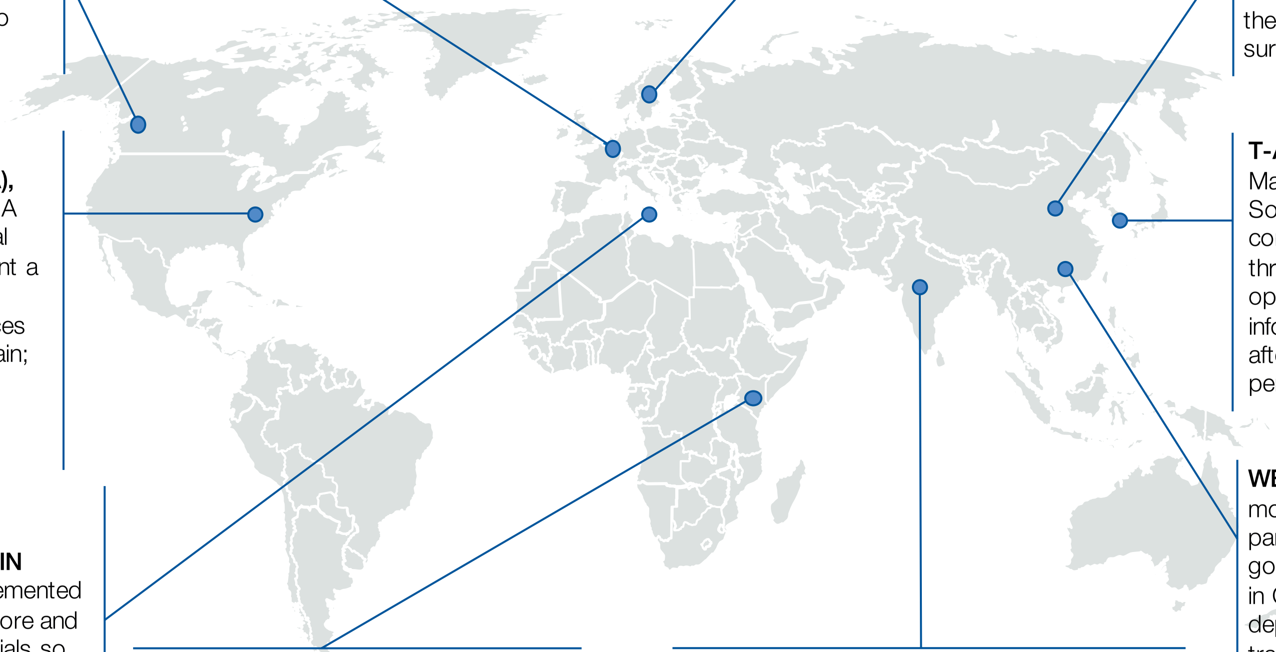
The great strength of a decentralized system is the control and transparency it offers the individual user: control over what identity-related information to share, with whom to share it, and for how long. Decentralized systems can also support a more appealing digital consumer experience, since individuals increasingly expect and can manage greater personalization and transparency. They can also facilitate interoperability between existing, isolated systems through verifiable claims.

Challenges

For a decentralized identity system to enable an individual to conduct higher-risk transactions, traditional trust anchors, such as banks and government agencies, will have to contribute attestations to the data store. Many such trust anchors are currently running centralized systems, where they own the user relationship. Changing the nature of this relationship and the ownership of the valuable data is a challenge, but some traditional trust anchors are embracing this change. Service providers and relying parties will also have to trust this decentralized model enough to accept it.

Technologies and standards to enable decentralized identity systems are rapidly gaining momentum, but most operating models and regulatory frameworks today are designed for centralized systems; they will have to evolve to enable and govern decentralized systems. Assigning liability for potential breaches or abuses may be especially complex. Individuals may need education to adopt decentralized systems and use them responsibly.

Figure 4: Select examples of identity systems across all three archetypes



BRITISH COLUMBIA – The province has developed the BC Services Card, which acts as a three-in-one driver's licence, health ID card and electronic ID, all rolled into one smart card.

FOOD AND DRUG ADMINISTRATION (FDA), USA – The FDA in the USA has regulated that medical device providers implement a standard method of identifying individual devices throughout the supply chain; this informs actors and protects end users from potential risks.

THE MINISTRY FOR EDUCATION AND EMPLOYMENT (MEDE) IN MALTA – Malta has implemented a blockchain system to store and verify educational credentials so that institutions, employers and employees can share and verify as authentic an individual's academic achievements.

CITY OF ANTWERP – Antwerp piloted distributed ledger technology to allow individuals to manage their own identity data.

M-KOPA, KENYA – This pay-as-you-go system harnesses digital payments and IoT technology to track assets in the field remotely, and record which customers are using them.

SWEDEN BANKID – Led by several financial institutions, the Swedish government has recognized BankID as a legal form of identification, which uses identities established through banks.

AADHAAR, INDIA – The Indian government enrolled 99% of its population, with a unique ID given to every Indian citizen using biometric inputs, free of charge, providing identification to many who previously had none.

MOUNT TAI TREE ID, CHINA – About 20,000 ancient trees on Mount Tai in Shandong have an ID card that allows rangers to monitor the health of the tree and its surrounding environment.

T-AUTH, SOUTH KOREA – Major mobile network operators in South Korea have created a common identity solution where, through a user's phone number, operators share relevant information with service providers after customers grant explicit permission.

WECHAT ID, CHINA – The mobile app with c. 1 billion users partnered with the Chinese government and is providing a trial in Guangzhou to allow people to deploy WeChat ID as a digital ID to transact with – e.g. to book hotels or to accept deliveries.

Chapter 2: What could good look like?

Doing digital identity better

All around the world, digital identity systems still exclude individuals, or they are so inconvenient that individuals either can't use them or don't want to. Many systems fail to give users access to the services they need, especially if they cross borders. Most do not give individuals choice over how their data is used. Many individuals also face discrimination based on identity data, which is often exposed to identity theft and other cyber threats.

We can do better, starting with a new paradigm. The digital identity of the future needs to aim to maximize value *to the individual user*, and balance it with the needs of system owners, relying parties and other actors. By focusing on individuals, system owners can better serve them and drive adoption of their digital identity systems.

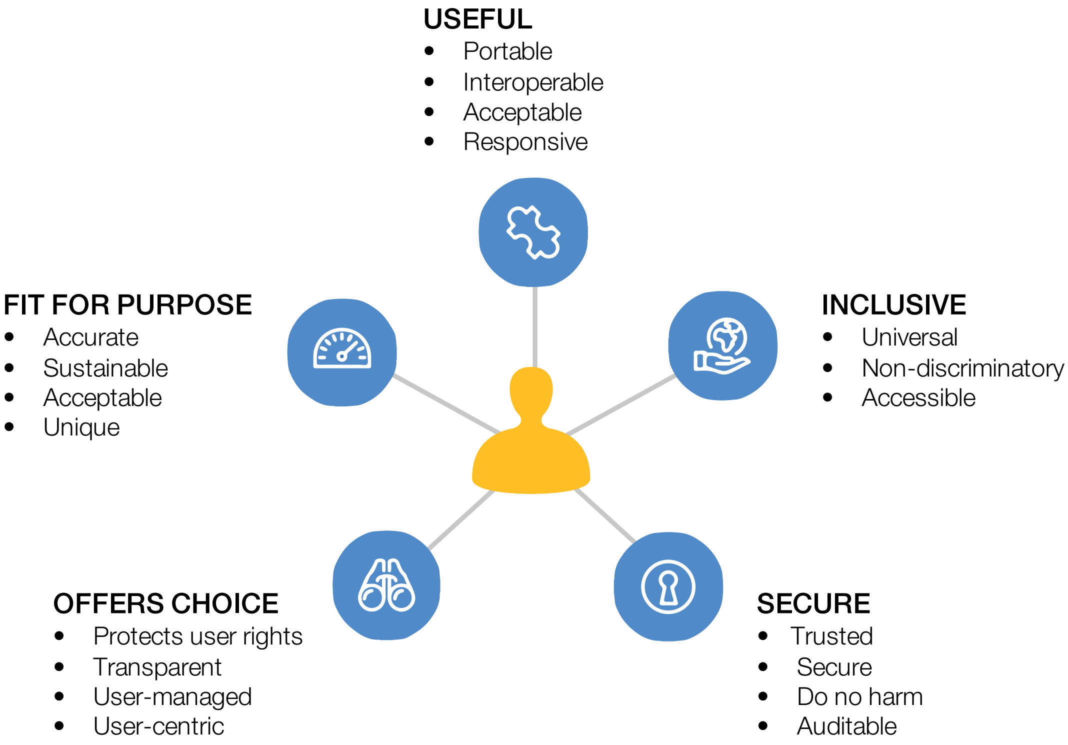
In their deliberations, contributors from the public sphere, the private sector and civil society identified at least five key elements of user value in a digital identity. In chapter 1, we touched on these elements. In this chapter, we'll examine what defines each, what good could look like and provide real-world examples.

As we consider these elements one by one, it's important to keep these guidelines in mind:

- All elements are equally important, and a user-centric digital identity – one that delivers real value to individuals and therefore drives adoption – must succeed in all five aspects.
- These five elements relate to each other and can build on each other. For example, strong privacy measures will support security.
- Tensions exist between some elements – security, for example, may make convenience more challenging for designers – but it is possible and necessary to manage the trade-offs.

Providing user value in digital identities thus requires solving challenges in all five elements in light of cultural and legal contexts. We will now look at what this solution might consist of and offer real-world examples for each element. These examples do not necessarily represent best methods, but they do offer insights.

Figure 5: The five key elements of designing user-centric digital identity



1. Fit for purpose

A fit-for-purpose identity system is one that provides:

- **Accuracy**: Identity-related data does not contain any errors, is precise in all details, and is up-to-date.
- **Uniqueness**: There is assurance that each individual is unique, within the broader user population in any system. The need to establish uniqueness will be higher in transactions that carry higher levels of risk and thus require stronger identity assurance.
- **Sustainability**: Systems have robust financial models and an approach to technology and policies that enable them to stay relevant into the future.
- **Scalability**: Systems are able to grow as demand increases.

Why is it important?

Accuracy and uniqueness are prerequisites for identifying and authenticating individuals. If the identity data in a system isn't accurate, individuals and relying parties won't trust or accept it.

Sustainability and scalability makes it attractive for individuals and relying parties to be able and willing to participate. To ensure future effectiveness, systems must be able to invest as technology, the threat landscape, policies and political landscape, and user expectations evolve.

What could good look like?

Establishing uniqueness

Uniqueness in a given user population is critical for both reducing the potential for identity fraud and for increasing the reliability of the identity.

There are multiple ways to establish uniqueness in a user population. One common method today is to give individuals unique usernames or identifiers (such as account numbers or payment card numbers), combining these with shared secrets (such as passwords), and then also collecting multiple data points such as IP addresses, activity history and location. Another common method is to use biometrics: unique and inherent personal attributes such as facial features, fingerprints or iris scans.

However, despite its potential to provide a strong assurance of uniqueness, biometrics requires caution, education and expertise. When poorly designed, the cost may lead to exclusion. The quality of fingerprints may decline over time, especially for manual labourers, and scarring, loss of a limb or other physical changes can also make authentication problematic unless systems are designed to meet these challenges. As biometric data is sensitive personal identifiable information, security and privacy practices must be impeccable.

It is advisable to combine methods, or vary them depending on the interaction, the organization's risk appetite, the regulatory and compliance requirements, and the level of assurance that a given interaction requires. For example, to receive a travel visa, to prove his or her unique identity, an applicant might need to submit (among other data points) name, date of birth, travel history and biometrics such as fingerprints and/or facial image. Typically, the more trusted data points collected about an individual and the smaller the user population, the easier it is to establish uniqueness.

Public-private partnerships

Digital identity systems need technological innovation, robust regulatory frameworks, widespread public trust and acceptance, a design that appeals to consumers and long-term financial sustainability. This makes them ideal candidates for public-private partnerships, with clearly defined roles and incentives for all involved. Possibilities for collaboration include sharing financial burdens, working together on user-centric design, jointly owning identity systems, ensuring mutual recognition and interoperability between systems, and building ecosystems that offer greater value to all participants.

Sustainable business model

Digital identity systems need long-term financial feasibility and functional longevity, and many suitable business models are emerging. Examples include consortiums of trust anchors and service providers sharing costs and charging those who gain value from the system – whether service providers or individual users. However, it is important that the financial incentives in these business models encourage inclusion and don't put individuals' choices or rights at risk. If digital identity systems are to be sustainable in the long term, they must also adapt to changes in user values and expectations for the user experience and functionality. The business model must also be able to support technological evolution, especially for a seamless experience and cybersecurity: security breaches and the ability to recover from these effectively can undermine sustainability by eroding both functionality and trust.

Real-world examples

Public-private partnership: BankID in Sweden
In Sweden, financial institutions have created an identity system, BankID,[8] which the government recognizes as legally binding for documents, transactions and more. Both government authorities and individuals use the digital BankID for multiple public and private services. This private-led partnership with government has 7.5 million active users.

Financial sustainability: NADRA in Pakistan
Through service fees and earnings, Pakistan's National Database and Registration Authority (NADRA)[9] enables low-income residents to register and receive ID cards free of charge. Revenue comes from small fees on a wide range of domestic services, such as opening a bank account. The service provider (such as a bank) that needs to conduct identity proofing of the individual pays the fee. This structure enables NADRA to reinvest in technology without needing a regular budget from the government.

Enabling refugees' identities: The United Nations
The United Nations High Commission for Refugees (UNHCR) has been deploying a new biometric identity management system (BIMS). In accordance with UNHCR's Policy on Biometrics in Refugee Registration and Verification (2010), biometrics should be used as a routine part of identity management to ensure that refugees' personal identities cannot be lost, registered multiple times or subject to fraud or identity theft.[10] As of May 2018, the UNHCR's BIMS and its use of the IrisGuard system in MENA had enrolled over 5 million people.[11]

2. Inclusive

To include all individuals and give them the access they need, identity systems must provide:

- **Equal opportunity**: Everyone within the target population is able to establish and use digital identities that can be authenticated.
- **Safeguards against discrimination**: No one faces special barriers in establishing and using identities or risks discrimination or exclusion as a result.
- **Mechanisms to manage unintended consequences**, such as data and security standards that exclude individuals who should be able to join.

Why is it important?

Embedding universal access and inclusion into design supports widespread adoption and reduces the digital divide. This boosts both the system itself and broader economic development. Widespread usage also creates sustainability, allowing identity systems to take advantage of a bigger user base to establish successful operating models.

What could good look like?

Accessibility and multiplicity
It should be easy for individuals of any socioeconomic or demographic segment to enrol in identity systems of their choice. To maximize inclusion, multiple entry points could help all individuals gain the access they need. Digital registration and enrolment options can boost adoption and inclusion among remote populations. However, mandatory enrolment or reliance on a single identity programme may not translate into sustained usage and trust. Users must be able to choose between multiple identity systems, based on their needs, concerns and rights. Absence of such multiplicity can translate into lack of choice and new forms of exclusion.

Design for all
To avoid excluding or marginalizing anyone, identity systems would consider and design for differences in abilities, age, digital literacy, access to technology and use-cases. To maximize inclusion, they could offer multiple access points and ways to use the digital identity – for example, offline enrolment and usage options for those with limited internet connectivity, or acceptance of a broad range of evidence and documents to establish an identity.

Designers must also consider how technology can support broad adoption while not causing a greater digital divide through challenges such as high costs (e.g. purchase price of a smartphone), unrealistic infrastructure demands (e.g. requires unbroken 4G data access) or compatibility barriers (e.g. requires every individual to subscribe to a particular service). Engagement with individuals during design can help ensure that an identity will meet their needs and be accessible.

Minimum data
Design could mitigate discrimination or unintended consequences by collecting, using or disclosing only information that is critical for a given transaction. For example, to assess if an individual is above the legal age to use a service, the party they are transacting with need not have visibility of that individual's age, or name or other attributes. This principle is especially pertinent when involving information that could harm individuals. For example, it may be best for systems not to collect, retain, use or share data on religion or ethnicity, as this could be used as the basis for discrimination and persecution.

Standards for inclusion
A digital identity framework will be more inclusive if it has standards for identity data and for interactions with trust anchors that all individuals can meet. Otherwise, data may be rejected and relying parties may have more confidence in certain identities than others – potentially leading to discrimination. Standards can proactively anticipate and address loopholes that can create exclusion. Standards for user protection, consent and control can also help individuals exercise their rights to privacy and security.

High-impact distribution channels

It is possible to reach out to large populations of people through widely used technology or distribution channels, such as mobile network operators. Tapping into existing, far-reaching channels can be an effective method for widespread inclusion.

Real-world examples

Accessibility: The IoT in Kenya

In Kenya, Internet of Things (IoT) sensors allow pay-as–you-go providers to identify petroleum gas canisters and control access to gas-powered cooktops remotely. These sensors also enable individuals to make payments through a mobile wallet and give them the opportunity to begin to establish a credit profile and access financial services.[12]

Making enrolment easy: Aadhaar in India

How do you enrol over 1.3 billion people in an identity system? The Indian government's Aadhaar system is available to all residents and accepts a wide range of documents to prove identity and address. It also offers options for those who lack any prior identification documents. Mobile centres enrol residents in remote rural areas and those without internet connectivity, and enrolment is free of charge. Between 2009 and 2018, over 1.21 billion people (99% of India's population) were enrolled in Aadhaar. However, ongoing legal deliberations and policy-making in India are still seeking to balance the scope and utility of the system with the protection of constitutional rights and freedoms.[13]

3. Useful

For individuals to want to use digital identities, the identity systems must offer:

- **Utility**: Useful digital identities offer access to a range of meaningful digital interactions and services.
- **Convenience**: Convenience in digital identities includes use, registration and management.
- **Ease of use**: Ease of use comes from identification and authentication that are as straightforward as possible, with friction proportionate to the use-case.
- **Interoperability and portability**: Digital identities should work across services, sectors and geographies while upholding security and privacy.

Why is it important?

Utility, convenience, ease of use, interoperability and portability don't just make individuals' lives easier; they also raise the odds that individuals and organizations will adopt the system. That increases incentives for relying parties to use it too and raises the odds of widespread acceptance.

Widespread acceptance, in turn, can support not just financial sustainability (see page 19), but also greater efficiency. With digital identities accepted across sectors and geographical boundaries, individuals will need fewer identities to interact with all the counterparties that they need to. Fewer identities, in turn, means fewer stand-alone data silos, with their accompanying inefficiencies and risks.

What could good look like?

Work across borders and sectors

Digital services frequently cross geographical and sectorial boundaries, as well as public and private sectors, but many identities do not. A landlord in a foreign country, for example, may not accept your local electricity bill or credit history when you try to rent an apartment.

Mutual recognition – where credentials issued by one system are accepted by another to authenticate and access services – could boost collaboration and reduce costs especially for many cross-border or cross-sector activities. Interoperable systems, which can communicate with each other or exchange data, increase convenience. Yet designers must also prepare for the risks that come with interoperability: an interconnected system may offer more loopholes for security threats to spread.

Wide-ranging value

Digital identities are meaningless if they do not translate into a wide range of services and interactions that individuals want to use. Not every activity needs a digital identity, but when a digital identity makes many activities easier, individuals are more likely to find it worthwhile. Such convenience requires attention to daily behaviour and to cultural norms, including the possible use of incentives. It's wise to watch out for common mistakes, too, such as mandating specific identity systems or disproportionate proofing processes for services that do not need the level of identity assurance that those systems provide, undermining user choice and perceived value.

Value over time

What's valuable to the user today may not be so tomorrow. For digital identity systems to continue to deliver value to individuals, operators must continuously monitor and evaluate what they want and need.

The right friction

Complex, high-risk transactions may require extensive information and vetting, but many transactions could have less friction and simpler identification and authentication. The context and use-case should determine the level of rigour and friction for identity proofing and authentication. In some cases, public/private-sector collaboration can also lower friction by reducing the number of times individuals undergo identity proofing.

Real-world examples

Crossing borders and mutual recognition: eIDAS in the EU
The EU's eIDAS regulation creates standards for electronic signatures, qualified digital certificates, electronic seals, timestamps and other proof-for-authentication mechanisms. Based on existing technology structures, its standards enable EU-based organizations that provide digital services to recognize and accept digital identification from multiple sectors in all other EU member states. This boosts trust in cross-border digital transactions, promotes interoperability, reduces duplicate identities and makes identity systems usable in more places.

Integration into everyday life: T-Auth in South Korea
Major mobile network operators in South Korea have created a common identity solution. The network provides the phone number, and operators share relevant information with service providers after customers grant explicit permission. Customers enter a PIN code on their phone to complete a transaction. Convenience has driven adoption: 99% of South Korea's websites and over 30,000 service providers, including banks, content providers and social media, accept it. Over 13 million monthly users carry out about 650 million transactions annually.[14,15]

4. Offers choice

The principles of choice for a digital identity include:

- **Transparency**: Individuals can see who is collecting and divulging their data, how they are using and processing it, and for what purpose.
- **Privacy**: Identity systems must embed privacy rights in technologies and processes, so that individuals can choose who controls, uses and accesses their identity data, for how long and for what purpose, and have the ability to update and remove their data as needed.
- **Data protection**: Technology design, operational controls and regulations governing the use of personal data will safeguard it from breaches, corruption or loss.
- **User control**: The more individuals can choose which identity systems to use, and how to manage, update and own their data, the more control they will have over related opportunities and risks.

Why is it important?

The design of digital identities can uphold or undermine an individual's right to privacy, included in the 1948 Universal Declaration of Human Rights.[16] Increasingly, individuals are demanding control over their personal data. Identity systems that meet these demands will likely boost trust, minimize the risks of exploitation or manipulation, and enjoy more adoption by users. Regulators, too, are focusing more on privacy and data protection.

What could good look like?

Self-management
Empowering individuals to manage their identity data is a powerful privacy tool, allowing them: to decide who can see and share the data; determine any changes; and permit or deny others the right to process and generate inferences from it. Individuals should be given a choice, in most transactions, to selectively disclose only those attributes required for the transaction. There may, however, be instances where this choice has to be balanced with the need for disclosure in support of goals such as crime prevention or national security. Where individuals are offered a direct benefit (such as a discount) for sharing their data, they should be able to understand both these benefits and the potential impact on their privacy. The digital interface and the processes for users to offer or manage their consent should be proportionate to the value of services being accessed and their level of risk – otherwise, they may lead to user apathy and low adoption.

Legal protections
Regulations, particularly those that govern data-protection and privacy frameworks, are a prerequisite for implementing identity systems. Regulators worldwide may want to consider shaping digital identities to offer transparency and data, as defined above. Public and private actors in different countries could agree on data-protection rules for cross-border governance. Designers will have to consider identity-specific regulations, more general data-related and privacy regulations, and cultural and transaction-specific contexts. They will also have to build frameworks that can evolve as regulations do and that will be in compliance across geographies.

Independent oversight
Privacy commissioners or data-protection authorities with well-defined roles and incentives can help enforce the law, protect sensitive data and – in the case of violations – assign responsibility and liability and support recourse mechanisms. These authorities should be independent of both government and private interests to help ensure resolution and clarity, especially when conflicting interests (such as between matters of national security and individual privacy or data protection) are involved.

Awareness and empowerment
The most extensive rights will do little if individuals do not know or use them. Many need education to support digital literacy and awareness of their rights to privacy and control over their data. The goal is to empower individuals to make informed decisions about their identity and privacy, based on the trade-offs, such as convenience versus privacy. The user experience may be an important guide for education and awareness.

Privacy by design
Privacy must be integral to the system's design, build and run processes. That means a user-centric approach to privacy that includes collecting the minimum required data for each use-case, minimizing its processing, controlling its storage, building easy-to-understand consent mechanisms that include the right for users to revoke others' access to their data, and giving individuals a view of where, how and why their data is used.

Real-world examples

Regulatory protections: GDPR in the EU
The European Union's General Data Protection Regulation (GDPR) expands the definition of personally identifiable information (PII). For example, it now includes emails and IP addresses. The GDPR also clarifies how PII can be treated and establishes several rights for EU residents relating to their personal digital data, including identity data. These rights include the right to information on how organizations are collecting and processing data about them. Users can also request that their data be erased and restrict its use for marketing.[17]

eID with transparency rights: Belgium and Estonia
Belgium's government identification card, eID, has an electronic chip for users to digitally sign documents, access online public services and identify themselves to authorities; it also grants the ability to see if public authorities have accessed users' personal files, and, if so, the name of the department of the official who did so. Citizens can then follow up with an electronic request for the authorities to explain why their files were accessed.[18]

In Estonia, too, users of the national digital identity system can view their personal information and also see, via the government's log files, how the authorities have been using it.[19]

Decentralization with blockchain: Antwerp
The city of Antwerp has piloted blockchain-based technology to allow individuals to establish and manage their own data.[20] These users decide what information is stored and with whom it is shared. As more organizations participate, this single source of truth could reduce administrative burdens and give individuals control over more and more data. By enabling individuals to decide what data is collected and divulged, this decentralized system supports a minimal disclosure model (see below.)

5. Secure

A secure digital identity system must offer:

- **Protection**: Rigorous cybersecurity practices evolve continuously to mitigate threats and block unintended or unauthorized access, disclosure or manipulation.
- **Data integrity**: Secure systems uphold digital identity data integrity, although individuals should be able to request that their data be removed.
- **Liability**: Frameworks should embed an audit trail, assign responsibility and provide for recourse in the case of a security leakage or breach.

Why is it important?

Security is crucial to build trust among both individuals and relying parties, to reduce cybercrimes such as identity theft, and to avoid unwanted outcomes, including human rights violations. A secure system that protects data helps individuals at all socioeconomic levels receive maximum benefits.

As connected devices permeate the daily lives of individuals and organizations, they are becoming prime targets for attackers. Verifiable digital identities can help identity-compromised and rogue devices to minimize the harm they might cause to individuals and systems.

What could good look like?

Minimal disclosure
Identity systems should empower individuals to disclose the minimum of data necessary to authenticate a given transaction; when individuals lack such control, the system itself should customize data disclosure according to the transaction, divulging the minimum necessary. Today, it's common for individuals to present far more sensitive information than a transaction requires. An official ID card, for example, may show your address when you merely need to prove your age.

Education
Educating individuals on the best methods to help keep their data secure, and what they can do to mitigate risk, provides a front line of defence against data theft and misuse.

Remediation
Even the best security system may fail on occasion and reveal sensitive information. The ability to recover rapidly from an incident, with organizational support and the financial means for remediation embedded into the incident response capability, will enable the system to retain or regain trust.

Real-world examples

Security and protection: Itsme in Belgium
The digital identity platform itsme uses multifactor authentication, including biometrics, to enhance security.[21] For authentication, the system then requires three elements: the mobile phone linked to the user, the SIM card whose security the mobile operators guarantee, and the user's personal itsme code.[22] The platform is compliant with GDPR and certified for eIDAS.

Chapter 3:
Looking ahead: trends, opportunities, challenges

What happens next?

Digital identities are already permeating our lives. As Fourth Industrial Revolution technologies such as the Internet of Things, artificial intelligence and self-driving vehicles advance, digital identities will too. With change accelerating, identity systems must be ready to evolve, while keeping value to individuals as their focus.

In this chapter, we will look at some of the digital identity trends, challenges and opportunities that policy-makers and system designers may encounter in the near future.

Trends

Decentralized identity systems, new trust anchors and more non-humans – these are just some of the developments that may require more attention in the coming years.

– **Decentralized identity systems**. New technologies and architectures, such as distributed ledger technology, could change the way in which individuals control and manage their identity-related data. Adoption of these systems may vary depending on culture, digital literacy, technology access and the participation of service providers and traditional trust anchors.

– **Evolving trust anchors**. Many more actors interacting with each individual will likely emerge as trust anchors who offer identity proofing and attestations – expanding from governments and banks that played this role traditionally to retailers, technology platforms, hospitals, mobile operators, e-commerce platforms, social media, personal relationships and more.

– **Identity ecosystems**. As digital life crosses geographic and sector boundaries, identities will too. Identities will become more interoperable across borders (such as in the X-Road data-exchange platform used by Estonia and Finland) and across sectors (for example, between telecom and banking sectors, or between land registries and supply-chain companies).

– **Local adaptation**. Even as digital identities grow more global, user adoption will depend on adapting them to local culture, habits and behaviours and collaborating to make the system focused on user value.

– **Identity of non-humans**. The need for devices, legal entities, assets and natural resources (including food) to have digital identities will grow as IoT, AI and other technologies advance, including "digital twins": the digital replicas of physical or virtual assets with which people and organizations interact. Designers and policy-makers will have to carefully consider evolving interactions between humans and non-humans, and what that means for user-centricity and accountability.

Challenges

What new challenges will emerge in light of evolving technologies, emerging trends and a new emphasis on individual value?

– **Optimizing user experience**. As new systems compete for users, especially in the absence of shared principles and standards, designers will have to avoid siloed systems that enhance risk or hinder value for users. They may have to offer individuals more choice on how to access and manage the many identity systems in their lives.

– **Sharing ownership**. Identity system owners, currently used to fully controlling identities, may have to adapt to systems in which ownership is shared, the individual has more rights, and collaboration helps identities operate across sectors and geographies.

– **Keeping regulations up to date**. Policy-makers will have to keep pace with the evolving digital identity landscape to shape laws and regulations that enable innovation and reduce hurdles to adoption, while safeguarding data, privacy and other constitutional rights. Identity systems will require new legal and regulatory frameworks for interoperability, new technologies and more.

– **Operating efficiently**. As new systems emerge, designers and policy-makers need to watch out for overlaps and duplicated efforts that could raise costs and inefficiencies.

– **Spreading digital literacy and access**. For individuals to adopt and use digital identities effectively – especially as the trend towards self-management accelerates – they will need both access to technology and a high level of digital literacy.

– **The digital identity divide**. It is an easy scenario to imagine: on one side, some users managing their own identity data with strict privacy or security safeguards; on the other side, users with their data and privacy at the mercy of others, or without any digital identity at all. The risk of falling on the wrong side of the divide is especially great in countries that lack a strong regulatory and oversight framework to protect privacy, security and other constitutional rights.

– **User apathy**. One possible result of the proliferation of many new identity systems and options for individual control is information overload: individuals may tire of managing their convenience/privacy trade-offs and adopt behaviours that undermine their safety or other freedoms.

- **Risks and liabilities**. As the field continues to expand, with new actors joining, clear risk and liability ownership and management is needed.

- **Unintended consequences from poor design**. Poor design can lead not just to poor performance, but also to harm to individuals. For example, a poorly designed digital identity could open the door to illegal surveillance and espionage. Every design decision needs to be carefully considered in light of how it might negatively affect individuals.

Opportunities

User-centric digital identities can be good not just for their users, but for society as a whole.

- **A more secure, trusted and portable digital world**. A trustworthy, convenient digital identity will not just help keep you, your devices and your assets safe; it will open doors for far more digital activities, helping to establish a web of trust larger than that which face-to-face interactions can achieve, across geographical and sectorial boundaries.

- **Simplicity, efficiency and trust in data sharing**. With digital identities that offer convenient, trusted access, along with individual choice and control over their data, enterprises will likely find the new digital identities to be more efficient and cost effective in the longer run than what exists in the data silos of today. Enabling individuals to manage their choices, while employing new technology innovations and building better collaboration between enterprises, will help ease the burden of compliance and improve efficiency by reducing repetition in data validation across different organizations and systems.

- **More collaboration for better systems**. The need for interoperability and a seamless user experience offers opportunities for the public and private sectors and civil society to work together. With fewer isolated identity systems, individuals and organizations can reduce costs and find new opportunities and a better digital experience.

- **Widespread value to individuals**. New trust anchors could make day-to-day, minimal-risk transactions low cost and highly convenient, increasing access to a wider variety of digital services and transactions.

- **Better incentives and behaviours**. Digital identities for children can provide incentives for ethical and sustainable practices. For example, digital identities could help organizations to track sustainable practices in mining and ensure that no child labour is used.

- **Traceability in supply chains**. When digital identities are attached to farm produce or other goods, the increased confidence in the end-to-end supply chain increases trust as all members can confidently declare that the element in question has the provenance that was promised.

- **The Fourth Industrial Revolution**. The Fourth Industrial Revolution's promise is a seamless integration of digital technologies to make our lives better. Secure, effective, convenient, private and inclusive digital identities would help enable that integration.

Chapter 4:
Priorities for public-private cooperation

As the International Organization for Public-Private Cooperation, the World Economic Forum offers a platform for stakeholders to discuss ideas, set priorities and act to help shape digital identities of the future.

Our partners in government, business and civil society have identified six priorities for collaboration on digital identities going forward:

1. **A focus on user value**. Giving everyone an identity is not good enough. Bad identities can be worse than having no identity at all. Designers and policy-makers must focus on the real prize: demand-led adoption of identities that deliver all five elements of user value and better access to services, plus safe, meaningful online interactions.

2. **Accountability**. How to measure value delivered by digital identities and hold systems accountable? The answer will differ across functions and domains, and it will evolve over time, but there is a need to develop shared metrics for user value for systems, countries and cross-border movements.

3. **Governance**. New ecosystems for digital identity will need new governance models to establish independent oversight, accountability across borders, and mechanisms to enforce compliance, manage liability and provide recourse as needed. The goal of collaboration should be to develop frameworks flexible enough to evolve over time.

4. **Stewardship**. Good digital identities will require political will and attention from government, business and civil society leaders. Shared understanding of principles could help policy-makers, organizational leaders and designers to advance standardized and coordinated practices. A cross-sector narrative on good identity would be especially helpful.

5. **Partnerships**. Digital identities run the risk of fragmentation and isolation, unless organizations communicate agendas and solutions to encourage best practices, shared priorities, partnerships and interoperability where appropriate.

6. **Innovation**. Whether "lighthouse projects" that solve specific use-cases, "agile sandboxes" that stress test assumptions or other methods to keep pace with new technologies and user needs, organizations can work together for better results on shared priorities – and build a library of successful pilots from which to learn.

Areas for collaborative action

To conclude, we offer a priority list for collaboration as we move towards truly user-centric digital identities.

Policy and governance

- Authentication mechanisms and policies proportionate with the level of assurance required
- Appropriate legal frameworks for privacy, cybersecurity and data protection
- National policies on digital identity that integrate with broader strategies for cybersecurity, patient safety, economic development and more
- User-centric policies and processes for private-sector providers
- Transparent collection, processing and use of data to support user trust
- Independent oversight within national identity and data-protection frameworks
- A shared global framework for cross-border governance
- Leadership on policy and practice within governments, businesses and other organizations

Community and public good

- Shared narratives and understandings of good identity and value to individuals
- Funded research to look at identity-related scenarios from AI and the Internet of Things (IoT)
- Metrics, tools, use-cases that illustrate the value of good identity
- Defining good identity for specific pilot populations, domains and use-cases

Capabilities

- Partnerships between governments, the private sector and civil society to make individuals aware of their rights, duties and risks, and the liability mechanisms around their identities
- Shared accountability frameworks
- Methodology sharing and capability building for policy-makers and practitioners
- Expanding insurance markets as identity-related risks evolve
- Legal and paralegal advocates to assist individuals as needed

Innovation and solutions design

- Embedding security and privacy into business policies and technology solutions
- Agile sandboxes and testbeds for priority challenges to user value, such as interoperability and security
- Innovations in digital and analogue process transition and integration, including digital twins
- Addressing growth in personally identifiable information (PII), especially that due to the IoT

Programme development

- Prioritizing use-cases with the highest potential to reduce friction and deliver user value
- Multistakeholder design and implementation of solutions, with public-private cooperation
- Identifying pilots and opportunities to scale good practice through collaboration
- Collaboration with civil society to identify different user values in different communities

Appendix I: Design considerations for practitioners

Many best practices for a user-centric digital identity are available now – but they may involve trade-offs. Others are not available off-the-shelf, but they will be achievable with investment, collaboration and a new mindset.

In this appendix, we aim to offer practical ideas for what do now: a map for policy-makers and designers to “get to good”. Even if this map contains alternate paths and some blank spaces – our list of ideas is far from exhaustive and context is critical – the hope is that it will still lead to the ultimate goal: digital identities that successfully deliver all five elements of value.

It’s worth emphasizing that policies and legal frameworks must be in place for us to achieve good digital identity; these are the foundation on which the process of getting to good depends.

What follows is a set of guidelines and considerations to support designing, building and running a digital identity system that puts individuals and what they consider valuable at its centre.

Figure 6: Illustrative checklist to consider when beginning the journey to good digital identity

1

GETTING STARTED

1.1 Determine who the users are
1.2 Consider the context
1.3 Capture the landscape
1.4 Determine potential ecosystem partners
1.5 Consult potential users
1.6 Create a narrative
1.7 Educate
1.8 Plan to share risks
1.9 Find new opportunities for sustainability

2

DESIGN AND CONSTRUCT USER-CENTRIC SYSTEMS

2.1 Maximize user value and functionality
2.2 Include the technology, industry, cultural and market landscape
2.3 Determine the right archetype
2.4 Include best practices for compliance and security
2.5 Mitigate risks and resolve trade-offs

3

ITERATE FOR FUTURE VALUE

3.1 Consider evolving needs to fight discrimination
3.2 Prepare for challenges with legal entities, devices, natural resources and more
3.3 Get ready for virtual entities, AI and more
3.4 Consider new technologies’ privacy implications

1. Getting started

1.1 **Determine who the users are**. Value means different things to different users, and there are trade-offs between different user-value combinations. Understand who the system will serve, what they value, and what barriers to adoption might exist for them now and in the future.
1.2 **Consider the context**. Different digital identities face different macroeconomic, cultural, political, legal and technology environments. Understanding this context is crucial for building a digital identity system that meets stakeholder needs and encourages their participation.
1.3 **Capture the landscape**. Before building a new system, map out the existing legacy architecture and stakeholders. This understanding will help plan the journey to the future state, including incentives for current actors to participate. It may also be possible to incorporate or adapt existing capabilities from legacy systems.
1.4 **Determine potential ecosystem partners**. Based on knowledge of individuals' values and the existing landscape (including possible trust anchors and system operators), identify potential ecosystem partners. Each participant will need incentives, most likely from mutualizing costs and benefits. That means rethinking governance models for funding, ownership, intellectual property, system operations, liability and more.
1.5 **Consult potential users**. Experiences in Belgium, British Columbia and Canada confirm that user group research and involving users in identity system design can boost long-term adoption. Engage the users from the start.
1.6 **Create a narrative**. Articulate the proposed digital identity's value and purpose for users, relying parties and other participants. Identity systems have often failed to win adoption because they have failed to communicate benefits and incentives effectively.
1.7 **Educate**. Digital identity advocates often need to start by educating policy-makers on the value of digital identities. Policy-makers and designers together can then educate users and relying parties about digital identity, its value and its risks. Early collaboration with civil society, especially community organizations, can help.
1.8 **Plan to share risks**. Policy-makers and organizational leaders might want to consider proven methods for risk sharing when considering an ecosystem for digital identity. One such method is for insurance companies to underwrite certain risks. For example, insurers often underwrite the risk of credit card fraud, enabling banks to compensate users if fraud occurs, thereby encouraging user confidence.
1.9 **Find new opportunities for sustainability**. The right financial models can generate revenue for digital identity systems, often by sharing the system's costs with multiple parties that derive benefits from it and creating revenue from new services. In South Korea, private companies saw financial benefits in building a single-identity solution, T-Auth, with full market coverage and technical and commercial integration through their resellers. Data sharing can also generate revenue, so long as it respects individuals' privacy rights and offers them benefits proportionate to the value that the data they choose to share creates.

With the groundwork laid, the next step for policy-makers, organizational leaders and designers is to arrive at a design that will deliver value to users. Each system and ecosystem will need a different design, based on the needs of their particular users and ecosystem partners, but the following principles may serve as general guidelines.

2. Design and construct user-centric systems

2.1 Maximize user value and functionality

- **Design for wider acceptability and mutual recognition**. The more relying parties accept an identity, the more individuals will adopt it and the more often they will use it. That will make it easier to keep data up to date and to build sustainable business models. Mutual recognition helps drive acceptability and usage.

- **Design for real-world access**. Besides creating a digital identity that provides for convenient, non-discriminatory enrolment, designers must consider what relying parties will demand to allow access. For a government ID, for example, to enable an individual to open a bank account, it may need more than basic identity information.

- **Define and communicate**. To drive adoption, systems must not just be convenient and useful; individuals must understand this convenience and utility. Clearly articulate and communicate use-cases to individuals, relying parties and ecosystem partners. Offering an immediate benefit (as SIM card registration does) can support communication.

- **Consider humans' links to non-human identities**. More and more devices, legal entities, and physical and virtual entities need digital identities. Designers and policy-makers will have to carefully manage how human users interact with and are accountable for them. For example, home-based IoT devices increasingly enable instant purchases – presenting new vulnerabilities with simplified authentication methods (such as a button or a voice command). These links will need to be analysed to determine how non-human identity data should be protected.

- **Adopt privacy by design**. To reduce the possibility of humans meddling with identity systems, embed the principles of privacy by design, with regular follow-up privacy impact assessments.

- **Align proofing to risk**. To optimize the convenience/security trade-off and minimize the amount of data divulged unnecessarily, identity systems may include different procedures depending on a transaction's risk level. Opening or accessing a social media account, for example, may not require as much data or need to pass through as many authentication layers as opening or accessing a bank account.

2.2 Include the technology, industry, cultural and market landscape

- **Consider the context**. What individuals consider "private" depends on culture, personal values and the transaction, and it evolves over time. GDPR, for example, now considers public keys to be part of personally identifiable information (PII).

- **Don't just secure: protect**. Besides securing itself against cyber threats, a digital identity system must protect its users: it must have policies in place on the responsible use, sharing and management of data.

- **Embed flexibility and agility**. Identity systems today already face challenges in keeping up with the pace of technological change. These changes are set to accelerate. Flexible architecture and agile development are critical for identity systems to remain relevant.

- **Apply data-protection principles to non-humans**. Devices and other legal entities increasingly have digital identities and related data whose exposure or misuse could harm both individuals and organizations. Certain animals and natural resources – such as endangered species that face the threat of poaching – may also need to have their identities protected, too.

- **Transparency and education**. Users should be able to understand, through transparency and education, what happens when they share their data: who uses it, how they use it and for what purpose. Education must be more than fine print. It should be clear and engaging enough to overcome potential user apathy.

- **Work with the IoT**. Millions of connected devices are already in homes and offices with billions more to come. They all have digital identities that connect to individuals and organizations – creating an interoperability, management and security challenge. Digital identity systems will need to manage such devices seamlessly and securely across their life cycles. AI and data analytics can help protect the devices, their users, the industrial infrastructure of which they are part, and responsible parties.

- **Test new ecosystems**. The ecosystem partners identified above will likely cross sectors and geographies, creating a much larger and more diverse ecosystem than those of past identity systems. Pilots should be conducted to test interoperability as needed.

2.3 Determine the right archetype

- **Look at value, context and the ecosystem**. When considering archetypes for a given identity system, start by identifying individuals and ecosystem partners, and what they need and value (see above), then look at their socioeconomic, political and technological context, including connectivity and access.

- **Be ready for existing archetypes to evolve**. Hybrid versions of the three archetypes identified in Chapter 2 are emerging. Government-owned and managed systems will likely continue to dominate large-scale digital identity systems, but the environment in which counterparties operate is evolving. Mutual recognition among different systems may prove increasingly important.

- **Prepare new governance and operating models**. As digital identity archetypes increasingly involve larger ecosystems, rather than isolated operations, designers will need new models for ownership, funding, intellectual property rights, liability and operations. The experience of consortia in other areas may serve as a model.

2.4 Include best practices for compliance and security

- **Design for resilience**. Digital identity systems may have tens of millions of users, as part of the complex ecosystem, when a major cyberattack comes. The system, including governance and operating models, must be able to withstand these challenges. Resilience includes flexibility: the ability to adapt to rapidly evolving threats and challenges, including the ever-evolving concept of "what is good" for individuals.

- **Secure the links**. It's not enough to secure the digital identity system's architecture and the data that it handles. Designers will have to plan to secure the inferences that the system generates, the history that it records, and the individual's connections to devices, legal entities and other users.

- **Set up and maintain a mechanism for redress**. Frameworks must not just record data accurately, but must also correct any errors that might enter later, either through natural evolution, data theft or mismanagement. With a mechanism to address inaccuracies and provide recourse if needed, digital identities can remain valid and trustworthy.

- **Embed independent oversight into legal frameworks**. Government regulations have an important role to play in ensuring privacy, but some government agencies may access data in ways that individuals do not approve of and that could cause discrimination. Independent oversight – such as privacy commissioners – can be part of the answer.

2.5 Mitigate risks and resolve trade-offs

- **Consider the sustainability/inclusion trade-off**. Digital identity systems must be financially and functionally sustainable to be effective, as discussed in Chapter 2. But too much emphasis on maximizing revenue may exclude users. Exclusive focus on today's functions and threats may come at the cost of flexibility to adapt to trends and expectations as they emerge. Designers may want to embed in business models the capacity for user subsidies (such as cost-free access) and the flexibility to change as needed.

- **Build for the privacy/convenience trade-off**. To achieve a seamless, personalized, immersive digital experience, individuals often choose to reveal identity data. A powerful tool for choice is for designers to allow individuals to choose their own balance of privacy and convenience – including the right to be anonymous – with the support of education and transparency

- **Build procedures for liability**. Even the most secure systems are not invulnerable. Plan for how to assign responsibility in the case of fraud and consider digital identity insurance. Educate individuals, relying parties and other stakeholders about where to turn for redress should a compromise occur.

3. Iterate for future value

3.1 **Consider evolving needs to fight discrimination**. Your gender, age or ethnicity might not expose you to discrimination today, but it could if you move to another country in the future. Digital identity should be able to accommodate life changes while preventing discrimination. Minimizing the collection of data that could one day be abused for human rights violations, and empowering individuals to choose what data to divulge, can help.

3.2 **Prepare for challenges with legal entities, devices, natural resources and more**. Not every entity or object needs to have a digital identity, but more and more do. Many non-humans already have "digital twins", for example, especially in trade and supply-chain management. For people to use, trade, track, trace, operate, transact or manage on behalf of these entities, digital identity systems will need the right designs, scope and capabilities, and ecosystems will need regular iterations.

3.3 **Get ready for virtual entities, AI and more**. As AI and virtual entities grow in importance, identity systems will need the capacity to revisit their capabilities to spot AI bots that have assumed a user's identity. Identity systems will need to be able to assess whether such bots are acting with the user's consent. They will also need to outline the consequences and liability if an AI bot is hijacked.

3.4 **Consider new technologies' privacy implications**. Several new technologies could make it easier for individuals to manage their privacy and data with less friction, but they may bring additional challenges. Artificial Intelligence and blockchain will require careful considerations in architecture, design and regulations to ensure privacy.

Acknowledgements

The Forum would like to thank **Accenture** for their valuable support of this publication, which draws on the experiences and expertise of a number of organizations cooperating on the “good identity” agenda:

Contributors

Access Now
AirAsia
Airports Council International
Amadeus IT Group
Amazon Web Services Institute
Ark
AT&T
Averon
Baker McKenzie
Barclays
BCG Digital Ventures
Bharat Innovation Fund
Bill & Melinda Gates Foundation
CA Technologies
Caribou Digital
Cisco
Cloudera Foundation
Department of Internal Affairs, NZ
RealMe
Deutsche Bank
DFID
DIACC
European Commission
Evernym
Federal Public Service of Belgium
FIDO Alliance
Gemalto
Government of Australia
Government of New Zealand
Government of Estonia
globaliD
Gravity
Grow Asia
GSK
GSMA
HSBC
Hyperledger
IADB
ID2020
IEEE
International Committee of the Red Cross
International Telecommunication Union
Internet Identity Workshop
Juvo Mobile
Konux
Mastercard
McKinsey & Company
Mozilla
NetHope Inc.
New York University
Next ID Limited
Nokia
ObjectTech
Omidyar Network
One World Identity
Open Society Foundations
People-Centered Internet
PayPal
Royal Philips
SACAU
SAP
Secure Identity Alliance
Securiport
Sedicii
SICPA
Simprints
Sovrin Foundation
Spherity
Standard Chartered Bank
Swiss Re
Taqanu
Thomson Reuters
UNDP
UNHCR
University of California Berkeley
Venable
Visa
Vodafone
Western Union
World Bank
World Food Programme
World Identity Network
World Wide Web Foundation

Steering Group

Amanda Long, Director-General, Consumers International, United Kingdom
Ashok Vaswani, Chief Executive Officer – UK, Barclays, United Kingdom
Brett Solomon, Executive Director, Access Now, USA
Jeroen Tas, Chief Innovation and Strategy Officer, Royal Phillips, Netherlands
Lynn St Amour, Chief Executive Officer, Internet Matters, USA
Michael Gorriz, Group Chief Information Officer, Standard Chartered Bank, Singapore
Mitchell Baker, Executive Chairwoman of the Board, Mozilla Corporation, USA
Renée McKaskle, Chief Information Officer, Hitachi Vantara, USA
Sheri Rhodes, Chief Technology Officer, Western Union, USA

Project Team: World Economic Forum

Derek O’Halloran, Head – Future of Digital Economy and Society
Manju George, Head – Platform Services, Future of Digital Economy and Society

Project Advisers: Accenture

David B. Treat, Managing Director, Global Blockchain Lead
Christine Leong, Managing Director

We also extend our thanks to a number of colleagues at the World Economic Forum and Accenture for their contributions to this publication.

For any inquiries, please contact Manju George, System Initiative on Digital Economy and Society, World Economic Forum, at Manju.george@weforum.org

Additional reading

Access Now, National Digital Identity Programmes: What's Next?, May 2018, https://www.accessnow.org/cms/assets/uploads/2018/06/Digital-Identity-Paper-2018-05.pdf

Ann Cavoukian, Privacy by Design – The 7 Foundational Principles
https://www.ryerson.ca/pbdce/certification/seven-foundational-principles-of-privacy-by-design/

Better Identity Coalition, Better Identity in America: A Blueprint for Policymakers, 2018, https://static1.squarespace.com/static/5a7b7a8490bade8a77c07789/t/5b4fe83b1ae6cfa99e58a05d/1531963453495/Better_Identity_Coalition+Blueprint+-+July+2018.pdf

Caribou Digital, Identities: New Practices in a Connected Age, 2017, https://www.identitiesproject.com/report/

China Daily, "Data for Mount Tai's ancient trees stored on digital ID cards", 2016, http://www.chinadaily.com.cn/china/2016-12/13/content_27651017.htm

Cloud Security Alliance, Identity and Access Management for the Internet of Things – Summary Guidance, 2016, https://cloudsecurityalliance.org/group/internet-of-things/

eIDAS, eIDAS Interoperability Architecture, 2015, https://joinup.ec.europa.eu/sites/default/files/document/2015-11/eidas_interoperability_architecture_v1.00.pdf

ETSI, SmartM2M; IoT LSP Use Cases and Standards Gap, 2016, https://www.etsi.org/deliver/etsi_tr/103300_103399/103376/01.01.01_60/tr_103376v010101p.pdf

European Union Agency for Network and Information Security (ENISA), Managing Multiple Identities, 2011, https://www.enisa.europa.eu/publications/mami

European Union Agency for Network and Information Security (ENISA), eIDAS: Overview on the Implementation and Uptake of Trust Services, 2018, https://www.enisa.europa.eu/publications/eidas-overview-on-the-implementation-and-uptake-of-trust-services

Gelb, Alan and Diofasi Metz, Anna, Identification Revolution: Can Digital ID be Harnessed for Development?, 2018, Center for Global Development: Washington, DC, https://www.cgdev.org/sites/default/files/identification-revolution-can-digital-id-be-harnessed-development-brief.pdf

Girão, João and Sama, Amardeo, NEC Laboratories Europe, Identities in the Future Internet of Things, 2009, https://www.researchgate.net/publication/226218872_Identities_in_the_Future_Internet_of_Things

Grassi, Paul, Garcia, Michael E. and Fenton, James L., NIST Special Publication 800-63-3: Digital Identity Guidelines, 2017, https://pages.nist.gov/800-63-3/sp800-63-3.html

GSMA, Access to Mobile Services and Proof-of-Identity: Global Policy Trends, Dependencies and Risks, 2018, https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2018/02/Access-to-Mobile-Services-and-Proof-of-Identity.pdf

GSMA, Enabling Access to Mobile Services for the Forcibly Displaced: Policy and Regulatory Considerations for Addressing Identity-Related Challenges in Humanitarian Contexts, 2017, https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2017/09/Policy-Note-FDPs-and-Mobile-Access.pdf

GSMA, Mobile Connect for Cross-Border Digital Services: Lessons Learned from the eIDAS Pilot, 2018, https://www.gsma.com/identity/wp-content/uploads/2018/02/MC-for-cross-border-digital-services_eIDAS_Feb2018-FINAL-web.pdf

Open Society Foundations and NAMATI, A Community-Based Practitioner's Guide: Documenting Citizenship and Other Forms of Legal Identity, 2018, https://www.opensocietyfoundations.org/sites/default/files/a-community-based-practitioners-guide-documenting-citizenship-and-other-forms-of-legal-identity-20180627.pdf

OECD, National Strategies and Policies for Digital Identity Management in OECD Countries, 2011, https://doi.org/10.1787/5kgdzvn5rfs2-en.

OECD, Digital Identity Management for Natural Persons: Enabling Innovation and Trust in the Internet Economy – Guidance for Government Policy Makers, 2011, https://doi.org/10.1787/5kg1zqsm3pns-en

Omidyar Network, Digital Identity and Privacy, 2017, https://www.omidyar.com/sites/default/files/file_archive/Digital_Identity_POV_Oct17.pdf

Omidyar Network and Institute for the Future, Ethical OS: A Guide to Anticipating the Future Impact of Today's Technology, 2018, https://ethicalos.org/wp-content/uploads/2018/08/Ethical-OS-Toolkit-2.pdf

Oracle, Digital Twins for IoT Applications, 2017, http://www.oracle.com/us/solutions/internetofthings/digital-twins-for-iot-apps-wp-3491953.pdf

Privacy International, The Sustainable Development Goals, Identity, and Privacy: Does Their Implementation Risk Human Rights?, 29 August 2018, https://privacyinternational.org/feature/2237/sustainable-development-goals-identity-and-privacy-does-their-implementation-risk

Servida, Andrea, Demystifying the New eIDAS Framework: Regulation and Implementing Acts – Content, Intention & Impact, 2016, https://www.eema.org/wp-content/uploads/servida.pdf

UBS, Digital Identity, 2016, https://www.ubs.com/magazines/innovation/en/into-the-future/2016/who-will-we-be-in-a-digital-world.html

USAID, Identity in a Digital Age: Infrastructure for Inclusive Development, 2017, https://www.usaid.gov/sites/default/files/documents/15396/IDENTITY_IN_A_DIGITAL_AGE.pdf

W3C Draft Community Group Report, Decentralized Identifiers (DIDs) v0.11, 2018, https://w3c-ccg.github.io/did-spec/#motivations-for-dids

W3C Member submission, Web Thing Model, 2015, https://www.w3.org/Submission/wot-model/

World Bank Group, Principles on Identification for Sustainable Development: Toward the Digital Age, 2017, http://documents.worldbank.org/curated/en/213581486378184357/pdf/112614-REVISED-English-ID4D-IdentificationPrinciples-Folder-web-English-ID4D-IdentificationPrinciples.pdf

World Bank Group, Technical Standards for Digital Identity (draft for discussion), 2017, http://pubdocs.worldbank.org/en/579151515518705630/ID4D-Technical-Standards-for-Digital-Identity.pdf

World Bank Group, Technology Landscape for Digital Identification, 2018, http://pubdocs.worldbank.org/en/199411519691370495/ID4DTechnologyLandscape.pdf

World Bank Group: Global Partnership for Financial Inclusion (GPFI), G20 Digital Identity Onboarding, 2018, https://www.gpfi.org/sites/default/files/documents/G20_Digital_Identity_Onboarding_WBG_OECD.pdf

World Bank Group, GSMA and Secure Identity Alliance, Digital Identity: Towards Shared Principles for Public and Private Sector Cooperation, 2016, http://documents.worldbank.org/curated/en/600821469220400272/pdf/107201-WP-PUBLIC-WB-GSMA-SIADigitalIdentity-WEB.pdf

World Economic Forum, The Known Traveller: Unlocking the Potential of Digital Identity for Secure and Seamless Travel, 2018, http://www3.weforum.org/docs/WEF_The_Known_Traveller_Digital_Identity_Concept.pdf

World Economic Forum, A Blueprint for Digital Identity: The Role of Financial Institutions in Building Digital Identity, 2016, http://www3.weforum.org/docs/WEF_A_Blueprint_for_Digital_Identity.pdf

Endnotes

1. Le Bras, Tom, “Online Overload – It’s Worse Than You Thought”, 2015, https://blog.dashlane.com/infographic-online-overload-its-worse-than-you-thought/ (accessed 10/9/2018).
2. UN General Assembly, Global Indicator Framework for the Sustainable Development Goals and Targets of the 2030 Agenda for Sustainable Development, A/RES/71/313, https://unstats.un.org/sdgs/indicators/Global%20Indicator%20Framework%20after%20refinement_Eng.pdf (accessed 10/9/2018).
3. World Economic Forum, Internet for All: A Framework for Accelerating Internet Access and Adoption, 2016. http://www3.weforum.org/docs/WEF_Internet_for_All_Framework_Accelerating_Internet_Access_Adoption_report_2016.pdf (accessed 10/9/2018).
4. eIDAS Regulation: Regulation (EU) No 910/2014 of the European Parliament and of the Council, 2014, https://www.eid.as/Regulation#preamble (accessed 10/9/2018).
5. ICAO, Machine Readable Travel Documents, Seventh Edition, 2015, https://www.icao.int/publications/Documents/9303_p3_cons_en.pdf (accessed 10/9/2018).
6. Finansiell ID-Teknik BID AB, “This Is BankID”, 2018, https://www.bankid.com/en/om-bankid/detta-ar-bankid (accessed 10/9/2018).
7. Patel, Neel V., “Malta Pilots Blockchain-Based Credentials Program”, 2018, IEEE Spectrum, https://spectrum.ieee.org/tech-talk/computing/networks/malta-pilots-blockchainbased-credentials-program (accessed 10/9/2018).
8. Finansiell ID-Teknik BID AB, “This is BankID”, 2018.
9. Malik, Tariq, “Technology in the Service of Development: The NADRA Story”, 2014, https://www.cgdev.org/publication/ft/technology-service-development-nadra-story (accessed 10/9/2018).
10. UNHCR, “Biometric Identity Management System”, 2015, http://www.unhcr.org/550c304c9.pdf (accessed 10/9/2018).
11. PRIMES: Bi-monthly update covering UNHCR’s rollout and continued use of biometrics systems in April and May; contact primes@unhcr.org for more information.
12. Irkliewskij , Mikel and Raia, Alexander, Pay-As-You-Go and the Internet of Things: Driving a New Wave of Financial Inclusion in the Developing World, 2018, https://newsroom.mastercard.com/wp-content/uploads/2018/05/180652_MC_PAYG_Whitepp_9.pdf (accessed 10/9/2018).
13. Unique Identification Authority of India, “AADHAAR Dashboard”, accessed July 2018, https://uidai.gov.in/aadhaar_dashboard/index.php (accessed 10/9/2018).
14. GSMA, SK Telecom – Operator Cooperation in South Korea Has Created a Successful Identity Solution, 2017, https://www.gsma.com/identity/wp-content/uploads/2017/09/mc_skt_case_08_17.pdf (accessed 10/9/2018).
15. Huh, Ian, “T-Authentication by SK Telecom: How We Enabled Win-Win authentication Business Model”, 2017, https://www.gsma.com/identity/wp-content/uploads/2017/03/T-Authentication-by-SK-Telecom-Updated.pdf (accessed 11/9/2018).
16. UN Office of the High Commissioner for Human Rights, “The Right to Privacy in the Digital Age”, https://www.ohchr.org/EN/Issues/DigitalAge/Pages/DigitalAgeIndex.aspx (accessed 10/9/2018).
17. European Commission, “What Are My Rights?”, https://ec.europa.eu/info/law/law-topic/data-protection/reform/rights-citizens/my-rights/what-are-my-rights_en (accessed 10/9/2018).
18. Gemalto, “eGov Strategy: Belgium’s Case (November 2016 update)”, 2016, https://www.gemalto.com/govt/inspired/belgium (accessed 10/9/2018).
19. Enterprise Estonia, e-Estonia Guide, https://e-estonia.com/wp-content/uploads/eas-eestonia-vihik-a5-180404-view.pdf (accessed 10/9/2018).
20. Ghelen, Tom, “How Blockchain Revolutionizes Identity Management”, 2018, https://www.accenture-insights.nl/en-us/articles/how-blockchain-will-revolutionize-identity-management (accessed 10/9/2018).
21. Gemalto, “Gemalto Brings Secure, Multi-Factor Authentication to Belgium’s Pioneering National Mobile Identity Scheme Itsme®”, 2018, https://www.gemalto.com/press/pages/gemalto-brings-secure-multi-factor-authentication-to-belgium-s-pioneering-national-mobile-identity-scheme-itsme.aspx (accessed 10/9/2018).
22. Itsme, “Log into Websites and Apps Quickly and Securely”, 2017, https://www.itsme.be/en/blog/log-into-websites-and-apps-quickly-and-securely (accessed 10/9/2018).

WORLD
ECONOMIC
FORUM

COMMITTED TO
IMPROVING THE STATE
OF THE WORLD

The World Economic Forum, committed to improving the state of the world, is the International Organization for Public-Private Cooperation.

The Forum engages the foremost political, business and other leaders of society to shape global, regional and industry agendas.

World Economic Forum
91–93 route de la Capite
CH-1223 Cologny/Geneva
Switzerland

Tel.: +41 (0) 22 869 1212
Fax: +41 (0) 22 786 2744

contact@weforum.org
www.weforum.org