WORLD ECONOMIC FORUM

COMMITTED TO IMPROVING THE STATE OF THE WORLD

White Paper

Digital Identity
On the Threshold of a Digital Identity Revolution

Davos-Klosters, Switzerland 23-26 January 2018

January 2018

REF 160118

Contents

On the threshold of a digital identity revolution

For individuals, legal entities and devices alike, a verifiable and trusted identity is necessary to interact and transact with others.

The concept of identity isn't new – for much of human history, we have used evolving credentials, from beads and wax seals to passports, ID cards and birth certificates, to prove who we are. The issues associated with identity proofing – fraud, stolen credentials and social exclusion – have challenged individuals throughout history. But, as the spheres in which we live and transact have grown, first geographically and now into the digital economy, the ways in which humans, devices and other entities interact are quickly evolving – and how we manage identity will have to change accordingly.

As we move into the Fourth Industrial Revolution and more transactions are conducted digitally, a digital representation of one's identity has become increasingly important; this applies to humans, devices, legal entities and beyond.

For humans, this proof of identity is a fundamental prerequisite to access critical services and participate in modern economic, social and political systems. For devices, their digital identity is critical in conducting transactions, especially as the devices will be able to transact relatively independent of humans in the near future.

For legal entities, the current state of identity management consists of inefficient manual processes that could benefit from new technologies and architecture to support digital growth. As the number of digital services, transactions and entities grows, it will be increasingly important to ensure the transactions take place in a secure and trusted network where each entity can be identified and authenticated.

Identity is the first step of every transaction between two or more parties. Over the ages, the majority of transactions between two identities has been mostly viewed in relation to the validation of a credential ("Is this genuine information?"), verification ("Does the information match the identity?") and authentication of an identity ("Does this human/thing match the identity? Are you really who you claim to be?"). These questions have not changed over time, only the methods have change.

This paper explores the challenges with current identity systems and the trends that will have significant impact on identity in the future.

Identity today is fractious

The advent of the internet catapulted us into the digital world and, for the past several decades, our identities have become more and more fractured and redundant with each new service provider and authority. Data related to our identities and the number of instances of our identities have proliferated to an unmanageable state. Think about your last move. How many different places did you need to update your address information? More fundamentally, think about how excluded from modern society you would be if you did not have any form of identity.

As digital forms of identity are required to conduct our lives, it is becoming clear that the current approach to identity and identity proofing is incompatible with the way we transact and behave across digital and physical worlds. The mandatory processes used to verify, authenticate and manage an identity throughout its life cycle are cumbersome and repetitive, requiring manual data reconciliation and validation processes in the background.

For individuals, this fragmented process leads to daily frustrations with countless usernames, forgotten passwords, ID documents and time wasted waiting to be verified and authenticated to complete a task such as gaining access to a building, boarding a plane, getting a job, etc. Challenges cited by individuals in both developed and developing country contexts include:

- **Limits to portability and acceptability –** "Recognized" identity differs widely among countries, organizations and contexts. Broadly, the issue arises as a result of a lack of trust between identity regimes and systems. As a result, individuals end up with thousands of digital and physical credentials for each service.
- **Social and financial inclusion** – For those who have no form of officially recognized identity, access to essential services as well as social and financial inclusion is extremely difficult or impossible.
- **Inability to manage data** – Globally, individuals have no ability to manage or know which entity has what parts of their data, where it is, how long the entity has access to the data, and who is monetizing that data.
- **Sharing of personal identification information –** Individuals have limited ability to select the persona and specific data that they want to share depending on the context and the entity with whom they are interacting.
- **Not user-friendly** – Authentication processes (e.g. banking, utilities) are often tedious and repetitive and provide the same set of documents for each service, sometimes from the same organization.

Identity is an equally challenging problem for organizations. Most identity-related industry practices and standards are developed and implemented based on industry-specific contexts but, as the need for digital identity evolves, a number of common issues have been identified:

- **Existing identity regimes are often inefficient, costly but mandatory** (e.g. know-your-customer or KYC, border control, global trade).
- **Identity data are disparate, difficult to find and often inaccurate.**
- Most identity systems and data are **not typically interoperable**, requiring significant, duplicate investments – even within a single organization.
- **Data protection regulations are different country by country** and compliance is difficult and expensive to manage.
- **Large investments have been made** into these regimes globally; any changes would be highly disruptive.
- **To date, the primary focus on identity is on identification of humans**, most standards, systems and architecture for non-human identities range widely in terms of maturity, reusability, suitability and usability for legal entities, devices and beyond.

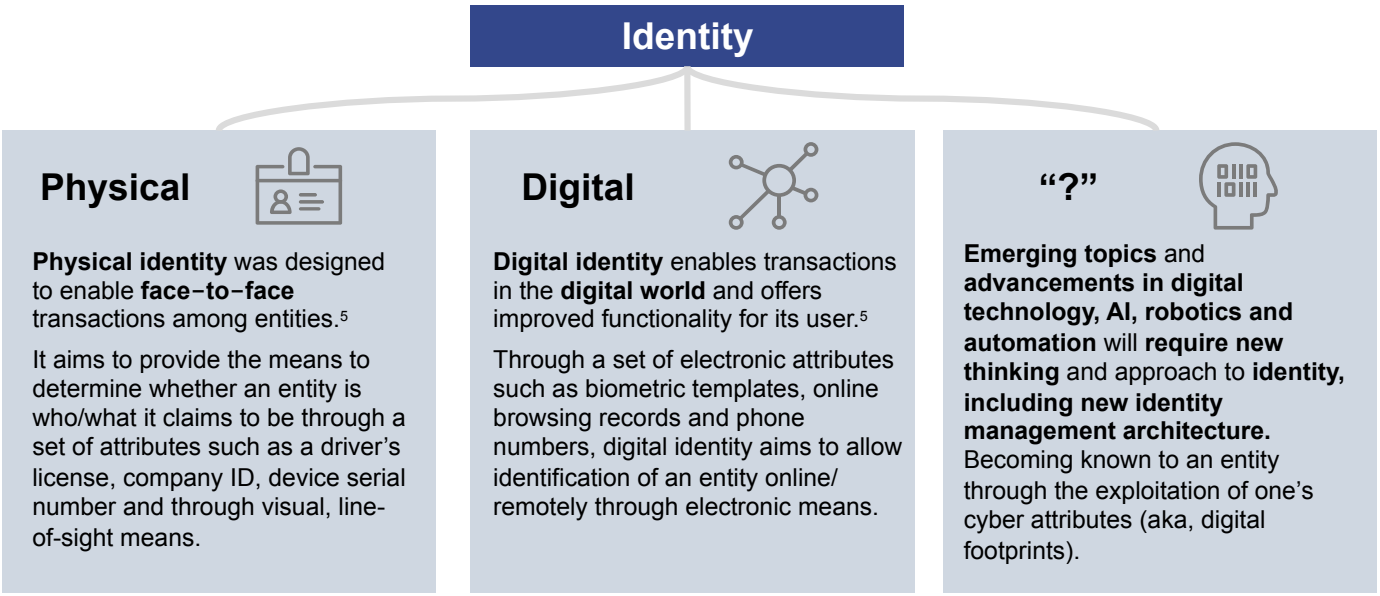
Our digital and physical selves are here to stay and there is new hope from emerging technologies to provide a better structure for identity. Change from our traditional means of creating and using an identity is required. It no longer makes sense to rely upon physical documents as the only mode given their fragility and inefficiency in a digital context.

What is digital identity?

Digital identity mechanisms offer the promise of greater efficiency, security and trust across industries and entities. From the provision of financial services to government-issued identification, digital identity enables transactions for the movement of people, funds, goods, data and other resources.

Just as instances of digital identity are fragmented, there are a number of different definitions for digital identity across human, legal entities and devices and "things" depending on context and industry. It is likely that, in the near future, a broader definition for digital identity will be required to address identity for virtual entities, AI "bots", robots and natural resources to enable a digital mechanism for identification and authentication to foster social and economic growth.

A selection of the most commonly used examples is listed below to demonstrate the differences found even in the most widely used definitions that form the foundation of most of today's identity regimes for people across financial services, travel and borders, public and humanitarian sectors.



Organization	Publication	Definition of digital identity
NIST	*Special Publication 800-63-3 – Digital Identity Guidelines*	The unique representation of a subject engaged in an online transaction. A digital identity is always unique in the context of a digital service, but does not necessarily need to uniquely identify the subject in all contexts. In other words, accessing a digital service may not mean that the subject's real-life identity is known.[1]
ITU	*Telecommunication Standardization Sector of ITU Series X: Data Networks, Open System X 1252 Baseline identity management terms and definitions*	A digital representation of the information known about a specific individual, group or organization.[2]
World Bank Group, GSMA, Secure Identity Alliance	*Digital Identity: Towards Shared Principles for Public and Private Sector Cooperation*	A collection of electronically captured and stored identity attributes that uniquely describe a person within a given context and are used for electronic transactions.[3]
ENISA	*Managing Multiple Electronic Identities*	A set of attributes, represents an individual in a transaction.[4]
World Economic Forum	*A Blueprint for Digital Identity – The Role of Financial Institutions in Building Digital Identity*	Describes the purpose of digital identity; digital identity enables transactions in the digital world and offers improved functionality for its users.[5]

As part of this initiative, digital identity for humans, devices, legal entities and emerging areas such as artificial intelligence, digital entities and natural resources, across different industries and contexts, will be explored through discussions, including some key considerations:

- The principles, requirements and values of digital identity as it relates to specific industry and context for the future
- Existing standards, practices and architectures; their similarities, nuances, differences; what works well and what has not worked well and why
- Existing values and expectations of digital identity for the identity holders
- Critical processes associated with using a digital identity, especially authentication and identity proofing
- Operations for a digital identity regime across people, process and technologies for each ID holder group (people, things/devices, legal entities) and their respective components
- Future concepts of digital identity that would be beneficial socially and across different contexts/industries
- Impact of technology and architecture for digital identity in the future
- Challenges and risks associated with digital identity (e.g. privacy, ethical usage of data, security, ownership)

Why is digital identity important?

A recognized form of identity holds intrinsic value for the identity holder. Traditionally, it has been human-centric. It supports functions such as ownership and trust. It also enables the movement of people, goods, data, funds and other resources.

When entities need to create or authenticate the identity to fulfil the objectives of movements of resources, what is accepted and the mechanism by which an identity can be authenticated differ widely across cultures, countries, industries and context. The diagram below shows example cases for which identity proofing is required:

Examples Identities	People	Organizations	Governments & public sector	Connected Devices	'Things'	Virtual entities
Examples where identity proof is required	Employment e.g., background checks	Banking & insurance e.g., KYC	Getting an ID e.g., driving license	Social benefits & welfare	Goods in supply chain	Social Media
	Healthcare services	Making payments	Paying & collecting taxes	Trade finance	Forests & Wildlife tracking	Workforce management
	Border control	Telecom e.g., getting a mobile phone contract	Travel & hospitality	Paying & collecting taxes	Processes	Machine to machine

The process of identity verification touches almost every industry, making identity an essential element in every transaction and industry from people to supply chain. Digital identity can have a transformative effect on a number of sectors and entities as described in the following section.

Digital identity revolution, in the context of…

The humanitarian sector

Those living in developed countries often take their identities for granted; individuals typically have too many identities scattered across institutions. Near-universal coverage of "foundational" registries, including birth certificates and social security numbers, allows individuals relatively unfettered access to offline and online services.

However, the situation is very different in the developing world, where "foundational" registration remains limited and an estimated 1.1 billion people lack any form of officially recognized identification. These individuals are precluded from basic services. Furthermore, since these individuals do not officially "exist" in the systems, they are also at a greater risk of trafficking.

Within the humanitarian sector, the current refugee crisis and the unique needs of these displaced individuals highlight the limitations of – and potential for – digital identity. Sixty-five million individuals – more than at any other time in history – are displaced today due to conflict, drought, famine and other factors. These men, women and children lack the most basic services and rights: shelter, safety, food, etc. And yet, due to displacement, they are often unable to assert their identity, trustworthiness and right to services.[6]

An officially recognized identity is a basic human right, as recognized by the Universal Declaration on Human Rights. For refugees, the inability to prove their identity has profoundly harmful implications, as a verifiable identity answers not just "who are you?", but also "what rights do you have?" and the recognition of their existence. Empowerment of the individual is fundamental to their protection.

Lack of identification also hinders the organizations trying to serve these people. For policy-makers, it is difficult to accurately plan and budget for government services. For example, it is not uncommon to see reported immunization coverage rates beyond 100% in underperforming districts – indicating that existing government data is inaccurate.

Different government bodies, NGOs and private-sector organizations often provide specific services to the same group or closely overlapping populations. Regardless of whether the service provided is healthcare, food, shelter, education or financial support, each recipient needs to be registered, enrolled, vetted and authenticated when receiving these services.

The provision, verification and authentication of an identity is critical to each of the service providers, yet because each organization has historically developed proprietary identity systems, these capabilities and their operations are often duplicated and individuals are required to verify their identity with each service provider in turn. Moreover, these identity systems are costly to maintain and increasingly put the organizations at risk of data privacy and cybersecurity threats; this duplication also means greater risks.

In a context of constrained funding for development and humanitarian work, this duplication of effort represents wasted resources. Given the numerous organizations providing supportive services, these individuals would benefit most from a digital identity that transcends organizational and national borders.

Perhaps because of the urgent and critical needs of crisis-affected populations, the humanitarian sector has emerged as a leader and advocate of establishing digital identity. UNHCR's work to empower refugees with a secure, portable digital identity fits within the broader agenda of the Sustainable Development Goals, and particularly with target 16.9 of the SDGs, which aims to "by 2030, provide legal identity for all, including birth registration."

> *"On October 2, 2017, the United Nations High Commissioner for Refugees, Mr Filippo Grandi, announced his vision for a digital identity for all refugees to increase their empowerment, inclusion, and protection, whilst also strengthening accountability and efficiency in humanitarian programme delivery and preventing and reducing statelessness."* [6]

The World Bank's ID4D programme has also taken a key leadership role in supporting developing country governments towards this goal:

> *"We believe that every person has the right to participate fully in their society and economy. Without proof of identity, people may be denied access to rights and services – they may be unable to open a bank account, attend school, collect benefits such as social security, seek legal protection, or otherwise engage in modern society. No one should face the indignity of exclusion, nor be denied the opportunity to realize their full potential, exercise their rights, or to share in progress. No one should be left behind."* [22]

Financial services

As both public and private organizations become more digitalized, financial institutions have acquired a unique edge in the digital identity space that enables them to drive identity systems and act as identity providers to public- and private-sector organizations. Substantial research and thinking have taken place on this topic specific to financial services, including the Forum's report *A Blueprint for Digital Identity – The Role of Financial Institutions in Building Digital Identity*. A number of concepts noted below leverage the content from this report.

Globally, the financial services industry has near-complete coverage of users (people, legal entities and assets) in developed economies[5] with global interconnected operations across multiple jurisdictions, giving them a structural advantage in enabling cross-jurisdictional identity transactions and systems.[5]

Financial institutions are one of very few types of institutions that can verify user information as they already perform this function for commercial and regulatory purposes.[5] People and legal entities in many countries already leverage documents from financial institutions as a form of identity to gain access to other services. This positions the sector as a prime candidate to act as trusted identity providers without extensive effort.

Despite this unique position, identity mechanisms and capabilities in the sector are still hampered by inefficiencies and costly manual processes (e.g. KYC). KYC is often conducted for the same entity multiple times as financial institutions are not designed to "trust" each other and their data. This repetition exists even within the same institution across different lines of business. Similarly, identity is not accepted and trusted across borders. Existing customers often find it difficult to open a bank account with the same institution in another country.

In some countries, financial institutions provide identity proofing services as they are trusted and/or more accessible by the consumers than governments. This is especially important in countries where changes in governments are frequent. Financial institutions often have greater longevity and accessibility. Some governments are leveraging the trust and accessibility of financial institutions to develop an identity ecosystem for the future. An example of this is the GOV.UK Verify initiative. Identity verification is performed by qualified and participating banks among other select institutions and underpins identity verification for this programme.[7]

Moreover, financial institutions' participation is often required for most transactions between entities, and they are established intermediaries in many transactions and therefore well-positioned to act as identity intermediaries.[5]

Financial institutions are also typically leaders in developing new systems and standards (e.g. Interac) that have been widely adopted and effectively used within the private sector.[5] The sector was also one of the first to make authentication more user-friendly and seamless through technologies like biometrics. Similarly, technologies such as blockchain are playing a role in changing identity architecture and addressing inefficiencies such as KYC.

Given the various market factors – including greater digitalization; increasing rates of security attacks and fraud; changes in customer expectations, incentives and behaviour, and the drive to offer more personalized services to customers – as well as its position of trust, the financial services sector could potentially revolutionize the future of identity services.

Travel and border control

Persistent security threats raise concerns for governments, the travel sector and the public. These threats cause numerous inefficiencies and impede the secure and seamless movement of legitimate travellers. As the world and the travel journey become more digitalized, digital identity will play a key role throughout the stages of the journey and enable authorities to accurately identify and authenticate travellers.

Cross-border travel is forecast to grow by 50% in the next decade and reach 1.8 billion international arrivals by 2030.[8] The number of people on the move today is unprecedented and the figures are expected to keep rising. Annual international arrivals rose from 25 million in the 1950s to 1.2 billion in 2015, and are expected to reach nearly 2 billion by 2030.[9]

We are simultaneously faced with a complex geopolitical landscape marked by a rise in both terrorism and e-terrorism, and a surge in populism and xenophobia. Together, they have the potential to reverse the growing freedoms acquired in previous decades by citizens to travel the world.[9]

As a result of these issues, the travel sector and travellers are facing increased risks and stringent privacy-infringing security requirements while operating at the limits of today's infrastructure capacity. At the current increasing pace, cross-border travel may exceed infrastructure capacity limits, leading to breakdown of processes, and industry and security deterioration.[23]

Particularly with air travel, the monetary and economic costs of the aviation security system are expected to reach unsustainable levels over the next 15-20 years[10] as the number of air travellers and air cargo continues to grow.[9] If no action is taken, this issue is expected to reach a tipping point, putting at risk potential future industry growth and causing the situation to deteriorate. However, digital innovations in travel security and Fourth Industrial Revolution technologies, if properly harnessed, can unlock significant change and value. Digital identity plays a key role in this change.

Security remains a central concern for stakeholders across the travel and tourism ecosystem.[11] The Fourth Industrial Revolution fuses the physical and digital worlds while revolutionizing the way global leaders think about security and global connectivity.[12] This has prompted a rise in border automation technology, enabling more-efficient processing of travellers at points of exit and entry.[23]

Beyond automation, technologies such as biometrics, cryptography, blockchain, AI and predictive analytics, and the proliferation of consumer mobile device capabilities, can make possible a complete redesign of traveller screening processes. These technologies can increase the ability to screen travellers in advance to clear low-risk travellers at a far faster rate, while accurately identifying high-risk individuals, maintaining traveller privacy and enabling a seamless experience.

Digital identity and the enabling technologies offer a promise of greater efficiency and security for the movement of people. Bringing the travel experience into the future will require active participation from stakeholders across the aviation, travel and tourism sector as well as governments around the world.

Connected devices

Smart devices – from mobile phones to wearables and smart home assistants, connected vehicles and healthcare devices – are becoming integral to our daily lives. Gartner estimates the number of connected things in use worldwide will reach 20.4 billion by 2020.[13] As we enter the Fourth Industrial Revolution, the complexity and number of connected devices transacting in the digital space will rise. Digital identity mechanisms will be of paramount importance for enabling trusted and secure transactions through these devices.

This will require scalable, reliable and secure methods of allocating, authenticating and managing human and machine identities throughout the life cycle of each connected entity.[27] Identity mechanisms need to evolve and scale to be capable of securely managing the identities of the anticipated billions of connected devices while enabling their usability.

These identity mechanisms must address the challenges of scalability, governance, privacy, domain space, complex devices and machine relationships, including multiple infrastructure and device ownership models, and different access management mechanisms for both real and virtual machines.[27]

Technologies and architecture are already transforming and developing our relationship with these devices. This includes cryptography, as chip manufacturers embrace the need for it and implement architectures that support hardware encryption, secure execution and embedded chip identifiers.[27]

Blockchain has the potential to be the backbone of internet of things (IoT) implementations in the future. Organizations are investing to develop IoT applicability for blockchain technology that will enable automated M2M communication and awareness while maintaining traceability, immutability and auditability of transactions performed by the device.

A number of standards (e.g. ISO, ITU-T, IEEE) are being developed across different areas in IoT with the hope that interoperability and alignment between business objectives and risks of IoT and associated challenges with identity would be considered. Alignment between industry, end users, standards organizations and regulators would need to play a role to ensure the technologies are properly leveraged to bring IoT to its potential.

Legal entities

Traditionally, identity systems and standards have been individual and human-centric. Although numerous systems exist to identify and authenticate legal entities, they vary across industries. These systems enable interoperability and transactions to take place between entities. Payment networks such as SWIFT, Visa and Mastercard provide a structure to manage identity for legal entities, including identifiers for every entity and transaction in the network, authentication protocols, and business and technical standards. Equivalent industry bodies, regulators, standards and structures are well established (e.g. travel industry and ICAO standards, IEEE for devices).

While the universal digital identity scheme for legal entities has yet to be established, a standard known as the Legal Entity Identifier (LEI) was developed as a response to the financial crisis of 2008 to address the gaps across quality, scope, accuracy and transparency of financial information.

The ISO 17442:2012 Financial Services Legal Entity Identifier standard defines a “legal entity” as a legal person or structure that is organized under the laws of any jurisdiction. It includes, but is not limited to, unique parties that are legally or financially responsible for the performance of financial transactions or have the legal right in their jurisdiction to enter independently into legal contracts, regardless of whether they are incorporated or constituted in some other way (e.g. trust, partnership, contractual). It excludes natural persons, but includes governmental organizations and supra-nationals).[15]

An LEI is unique to each legal entity and is associated with a standard set of attributes that represent the specific legal entity. A trusted source of truth supported by the Global Legal Entity Identifier Foundation (GLEIF) provides access to trusted information about legal entities. Regulators have benefited from improved compliance and increased access to trusted information.

To take one example, more-efficient digital identity regimes for legal entities are needed in trade finance. In any trade transaction, there are multiple parties throughout the supply chain; each party needs to be onboarded with a bank and public authorities (e.g. tax or customs authorities) in order to transact. Numerous paper-based documents are involved in onboarding and throughout the transaction (e.g. certificate of incorporation, bank guarantees, export licences). Each entity, delegate and document must be verified and authenticated multiple times by multiple parties, which is costly, opaque and inefficient.

Similar to human identities, the lack of trust between systems and parties is a core issue in the ecosystem. Data sent from one system to another is not trusted and must be validated. This creates the need for repetitive but critical validation, authentication and reconciliation processes. With a more transparent and “trusted” architecture to manage identities of legal entities, these inefficiencies could be reduced.

LEI is certainly a potential foundation that can be leveraged beyond compliance. One of the goals of the LEI system is to provide reliable identity information to permit unique identification of legal entities worldwide, in financial services and beyond (e.g. supply chain applications).[5] The LEI is intended to become the link between all other identifier systems (e.g. KYC systems, business register codes).[5] LEI has the potential to be leveraged in blockchain/distributed

ledger applications as an identity label for trading financial instruments or managing LEI creation and administration itself.[16]

As we enter the Fourth Industrial Revolution, the expectations of how we transact digitally in the consumer environment will transfer to legal entities. Paper-based, manual processing systems are ripe for change. Emerging technologies, such as blockchain and robotics, are already transforming operations and transactions between legal entities. Legal entities will require digital identities to leverage these technologies to increase efficiency, productivity, cost-effectiveness and transparency.

Sustainable supply chain

Green trade, which includes things like renewable energy, sustainable materials and low-carbon transport, is rising in political and economic importance and has a global market of $1 trillion a year.[18] At the same time, the *Sustainability Consortium 2016 Impact Report* found that the majority of manufacturers have limited visibility into the sustainability of their supply chains.[19] To improve the sustainability or "greening" of global supply chains requires traceability and transparency.

- **Traceability** is necessary to track hazardous products and materials, assign and allocate responsibilities, and monitor compliance with environmental and sustainability protocols.
- **Transparency** is essential for achieving credibility, legitimacy, accurate risk management and fairness, and to avoid "green-washing" – misinformation provided by companies to appear more environmentally responsible than they really are – or moving polluting activities to developing countries.[20]

To trace products and materials, an identifier is required. Today, there are numerous definitions and approaches to manage identifiers depending on the product, context and point in the supply chain.

The introduction of RFIDs (radio-frequency identification) allows organizations to create a digital history down to the individual product level. This mechanism provides an identity to the individual product and thus enables it to be traced across its life cycle. This has been a game-changer in verifying the authenticity and sustainability performance of goods as they move through the supply chain.

A digital identity for all actors, goods and places in a supply chain, established provenance and a means of traceability throughout all touchpoints along the supply chain are essential to assure products like timber, pharmaceuticals, fish, coffee, etc. have been ethically sourced and follow sustainability protocols. By establishing an interoperable digital identity across contexts, efficiency gains can be made by allowing linkages to KYC, inventory management and traditional legacy systems.

Additionally, paired with technologies such as blockchain, all actors along the supply chain are visible and accountable. This greater transparency has the potential to mitigate risks, reduce costs and open access to a broader range of the market.

Most companies now recognize that a sustainable supply chain is no longer just an optional nice-to-have – it's a business imperative, critical to the success of the organization as a whole. In 2010, when Accenture surveyed more than 700 members of the United Nations Global Compact on sustainable business practices, 96% of CEOs stated that sustainability should be integrated into all aspects of strategy and operations; and 88% of CEOs surveyed singled out the supply chain as an area of specific importance.

Yet, only 54% of those CEOs affirmed that they had achieved supply chain sustainability. Other evidence strongly suggests that their suppliers are still serious sustainability laggards.[21]

Digital identity, especially combined with blockchain, can provide organizations with a means to manage their supply chain to achieve and demonstrate greater sustainability performance. This greater transparency can, in turn, help to change the way consumers are incentivized to use green goods and services. Together, this can ultimately provide the means by which we bring together humans and technology to shape and change the behaviours necessary to protect our environment.

Risks and key points for consideration

While digital identity is critical for social inclusion and growth in the future, it is also a topic that must be considered responsibly and ethically. Answering the question 'Who we are' can be fraught with risks for many people. For those that are fleeing conflict and persecution, they might not want to reveal their identity. Options for those not wanting to have a digital identity or those that want to share only parts of their identities (e.g. different personas in different context) or only share relevant identity data for specific purposes must be considered. For digital identity regimes to be effective, considerations must be made for the edge use cases and exceptions, in order to be truly universal and ubiquitous.

Providing control back to the digital identity owner needs to be considered, it enables the individual to decide who should have access to what data and for how long. The emerging trend for self-declared or managed identity is gaining momentum. While in principle the concept for the identity owner managing and fully controlling their identity is being considered in some developed countries and technology sector, for the majority of the world, the trust anchors for digital identities are still the same as the physical world. While these trust anchors may change in the future, the existing strong trust anchors (e.g. government authorities, banks etc.) are not disappearing. They are likely to remain the trust anchors for identities both digital and physical. The need for delegation and custodianship of digital identity and its management will remain a requirement.

People are often more at ease sharing identity data digitally than they are physically. Social media and networks are a good example of this where these are deemed to be highly trusted by consumers as they provide a valued service despite the extensive amount of identity information used. However, the sense of anonymity in the digital world is not always robust and the level of segregation between physical and digital are often not as well defined as we would like to believe. Identity fraud is an indication that digital identities breaches can have a significant impact on our physical lives. Consumers need to be educated and trained to understand that actions in the digital world have direct impact in the physical world, as our digital identity is primarily a representation of 'who we are' physically.

Values, principles, requirements and key questions in consolidating a fractured identity landscape

It is clear that the key trends affecting digital identity will impact every industry and entity type. This is all the more reason to develop a cohesive, well-considered approach to digital identity across industries so that the leaders of organizations can understand its importance and support each other in the adoption of global digital identity efforts. Numerous efforts are taking place in this space with many different standards; and new standards are emerging as well as countless new technology solution providers and rapidly changing architecture forces from the market.

To consolidate the efforts and make sense of digital identity such that a central voice emerges from the numerous studies, solution players, states and organizations, regulators need to work together to form the future of digital identity.

As we embark on this initiative, one key step is to think about the principles of digital identity. What must organizations do and why? What should they avoid based on previous mistakes? What elements are common across organizations, and which parts will be revolutionized by new technology and architecture? What are the requirements and principles of digital identity?

The principles noted below include ID4D digital identity principles developed specifically for people from the perspective of state-issued identity. These principles are a robust starting point for considering identity regimes for the future and what principles, requirements and value digital identity would be required to follow in the context of people.

World Bank ID4D Principles on Identification for Sustainable Development include:

Inclusion: Universal coverage and accessibility	– Ensuring universal coverage for individuals from birth to death, free from discrimination – Removing barriers to access and usage, and disparities in the availability of information and technology
Design: Robust, secure, responsive, and sustainable	– Establishing a robust – unique, secure and accurate – identity – Creating a platform that is interoperable and responsive to the needs of various users – Using open standards and ensuring vendor and technology neutrality – Protecting user privacy and control through system design – Planning for financial and operational sustainability without compromising accessibility
Governance: Building trust by protecting privacy and user rights	– Safeguarding data privacy, security and user rights through a comprehensive legal and regulatory framework – Establishing clear institutional mandates and accountability – Enforcing legal and trust frameworks though independent oversight and adjudication of grievances

About the Digital Identity initiative

The World Economic Forum seeks to ensure the existence of a digital mechanism for identity authentication that fosters opportunity; enables a system for persons, devices and entities; and supports the movement of individuals, funds, goods, data and other resources.

This initiative aims to shape the next chapter in identity through understanding and defining a framework, basic principles and requirements for digital identity regimes. The initiative will also provide a platform to facilitate and frame tailored multistakeholder conversations across sectors, industries and geographies; and set the foundation for a digital mechanism that fosters growth and opportunity by addressing key questions about the impact of digital identity on the movement of individuals, funds, goods, data and other resources in the digital economy and society.

We welcome any additional thoughts, suggestions and contributions on digital identity that could help further our mission. Please reach out with any suggestions digitalidentity@weforum.org

Endnotes

The following sources have been used for definitions quotes, definitions and concepts.

1. http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-3.pdf
2. https://www.itu.int/SG-CP/example_docs/ITU-T-REC/ITU-T-REC_E.pdf
3. https://openknowledge.worldbank.org/bitstream/handle/10986/24920/Digital0identi0e0sector0cooperation.pdf?sequence=1&isAllowed=y
4. https://www.enisa.europa.eu/publications/mami/at_download/fullReport
5. A Blueprint for Digital Identity – The Role of Financial Institutions in Building Digital http://www3.weforum.org/docs/WEF_A_Blueprint_for_Digital_Identity.pdf
6. http://www.unhcr.org/blogs/id2020-and-unhcr-host-joint-workshop-on-digital-identity/)
7. https://www.gov.uk/government/publications/introducing-govuk-verify/introducing-govuk-verify
8. UNWTO. UNWTO World Tourism Barometer – Advance Release January 2017. UNWTO. [Online] January 2017. [Cited: October 18, 2017.] http://cf.cdn.unwto.org/sites/all/files/pdf/unwto_barom17_01_january_excerpt_.pdf. Air travel on a whole is expected to double from 3.8 billion air travellers recorded in 2016 to 7.2 billion air travellers in 2035. IATA http://www.iata.org/pressroom/pr/Pages/2016-10-18-02.aspx
9. http://www3.weforum.org/docs/IP/2017/MO/WEF_ATT_DigitalBorders_WhitePaper.pdf
10. Gillen, David and Morrison, William. Aviation security: Costing, pricing, finance and performance. s.l.: Elsevier, 2015.
11. World Economic Forum. Digital Transformation Initiative: Aviation, Travel and Tourism Industry. Geneva: World Economic Forum, 2017. REF 060117.
12. World Economic Forum. The Fourth Industrial Revolution, what it means and how to respond. s.l.: World Economic Forum, 2016
13. https://www.gartner.com/newsroom/id/3598917
14. Global Legal Entity Identifier Foundation https://www.gleif.org/en/
15. The ISO 17442:2012 Financial Services Legal Entity Identifier standard https://www.iso.org/obp/ui/#iso:std:iso:17442:ed-1:v1:en
16. Identifier Verification: Evaluation of Blockchain and Alternative Technologies http://www.efinancelab.de/fileadmin/documents/conferences/herbsttagung2016/presentations/16_2016-09-01_eFinanceLab-presentation_blockchain_V1.2_final_1800-1815.pdf
17. http://www.tradefacilitation.org/
18. http://www.uscib.org/coalition-for-green-trade-endorses-wtos-environmental-goods-agreement-ud-4779
19. https://www.sustainabilityconsortium.org/wp-content/2016-impact-report/
20. OECD, WTO and World Bank Group. 2014. “Global Value Chains: Challenges, Opportunities and Implications for Policy.” G20 Australia.
21. https://www.accenture.com/us-en/insight-outlook-why-sustainable-supply-chain-is-good-business
22. http://pubdocs.worldbank.org/en/200361509656712342/web-English-ID4D-IdentificationPrinciples.pdf
23. World Economic Forum, Shaping the Future of Security in Travel Insight Report: Known Traveller Digital Identity Concept
24. World Economic Forum, Digital Borders Enabling a secure, seamless and personalized journey
25. World Economic Forum, Digital Transformation Initiative Aviation, Travel and Tourism Industry
26. Accenture, Security Call to Action: Preparing for the Internet of Things https://www.accenture.com/t20160719T011940Z__w__/us-en/_acnmedia/Accenture/Conversion-Assets/Microsites/Documents22/Accenture-Security-Call-to-Action-IOT.pdf#zoom=50
27. Accenture, The Challenges of Identity Management in the IoT Report

Acknowledgments

World Economic Forum, Shaping the Future of Digital Economy and Society System Initiative
Derek O'Halloran, Head of Digital Economy and Society System Initiative
Manju George, Head of Platform Services and Public-Private Cooperation
Daniel Dobrygowski, Project Lead
Justine Moscatello, Community Specialist

Accenture (Project Advisor)
David Treat, Managing Director USA
Christine Leong, Managing Director USA
Yevgeniy Bakhir, Digital Identity Consulting Manager USA

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