Bio-digital convergence
- the hidden plan, yet in plain sight.
Top-down decision.
Why? How? With whom?

Dr. Geanina Hagimă

publications.gc.ca/site/eng/9.881083/publication.html

Government of Canada / Gouvernement du Canada

Search Canada.ca

Jobs | Immigration | Travel | Business | Benefits | Health | Taxes | More services

Home → How government works → Oversight → Communications → Government of Canada Publications → Browse publications

Exploring biodigital convergence : what happens when biology and digital technology merge?

https://publications.gc.ca/site/eng/9.881083/publication.html

What is biodigital convergence?

Biodigital convergence is the interactive combination, sometimes to the point of merging, of digital and biological technologies and systems. Policy Horizons is examining three ways in which this convergence is happening.

1 Full physical integration of biological and digital entities

Digital technology can be embedded in organisms, and biological components can exist as parts of digital technologies. The physical meshing, manipulating, and merging of the biological and digital are creating new hybrid forms of life and technology, each functioning in the tangible world, often with heightened capabilities.

2 Coevolution of biological and digital technologies

This type of biodigital convergence emerges when advances in one domain generate major advances in the other. The coevolution of biological and digital sciences and technologies enables progress in each domain that would be impossible otherwise. This could lead to biological and digital technologies that are developed as integrated or complementary systems.

https://publications.gc.ca/collections/collection_2021/hpc-phc/PH4-185-2019-eng.pdf

UNIUNEA EUROPEANA
Fondul Social European

GUVERNUL ROMÂNIEI
Ministerul Dezvoltării Regionale
și Administrației Publice

PODCA
INOVAȚIE ÎN ADMINISTRAȚIE

Instrumente Structurale
2007-2013

PORTAL LEGISLATIV

ACASĂ | DESPRE PROIECT | FACILITĂȚI OFERITE | LEGĂTURI UTILE | GDPR

CUPRINS

Forme act
Forma consolidata
+ istoric consolidări

LEGE nr. 293 din 3 noiembrie 2022

pentru prevenirea și combaterea cancerului

EMITENT PARLAMENTUL ROMÂNIEI

Publicat în MONITORUL OFICIAL nr. 1077 din 8 noiembrie 2022

https://legislatie.just.ro/Public/DetaliiDocumentAfis/261246

Noul Parteneriat pentru medicina personalizată, care urmează să fie înființat în 2023 și finanțat în cadrul programului Orizont Europa, va identifica prioritățile pentru cercetare și educație în medicina personalizată, va sprijini proiectele de cercetare privind prevenirea, diagnosticul și tratamentul cancerului și va face recomandări pentru lansarea abordărilor medicale personalizate în practica medicală zilnică. Ca acțiune pregătitoare pentru parteneriat, Comisia Europeană va stabili o foaie de parcurs către prevenția personalizată, identificând lacunele din cercetare și inovare, și va sprijini o abordare pentru cartografierea tuturor anomaliilor biologice cunoscute care duc la susceptibilitatea la cancer, inclusiv a cancerelor ereditare.

Medicina personalizată va beneficia, de asemenea, de High-Performance Computing. Combinarea datelor de sănătate ale unei persoane cu monitorizarea în timp real prin dispozitive inteligente și farmacocinetică va constitui baza pentru crearea unui geamăn digital (digital twin) al fiecărei persoane. Acest lucru va valorifica potențialul abordărilor medicale personalizate și va spori strategiile de screening și prevenire, diagnosticele rapide și conceptele terapeutice individualizate.

Pe de altă parte, acest plan are în vedere o inițiativă prin care să se asigure accesul rapid la servicii de depistare, diagnosticare și tratament în cazul cancerelor pediatrice.

Personalised medicine will also benefit from **High-Performance Computing**. Combining an individual's health data with real-time monitoring through smart devices and pharmacokinetic will form the basis to create a digital twin (i.e. virtual representation) of each person. This will leverage the potential of personalised medicine approaches, and enhance targeted screening and prevention strategies, rapid diagnoses and individualised therapeutic concepts.

https://health.ec.europa.eu/document/download/26fc415a-1f28-4f5b-9bfa-54ea8bc32a3a_en

Standardization institutions

- **IEC International Electrotechnical Commission -** is an international standards organization that prepares and publishes **international standards for all electrical, electronic and related technologies** – collectively known as "electrotechnology". The **IEC cooperates closely with the International Organization for Standardization (ISO)** and the **International Telecommunication Union (ITU**). In addition, it works with several major standards development organizations, including the **IEEE** with which it signed a cooperation agreement in 2002, which was amended in 2008 to include joint development work.
- **IEEE Institute of Electrical and Electronics Engineers** - an American 501(c)(3) professional association for electrical engineering, electronics engineering, and other related disciplines.
- **ITU -International Telecommunication Union –**is a specialized agency of the United Nations responsible for many matters related to information and communication technologies. **The ITU promotes the shared global use of the radio spectrum, facilitates international cooperation in assigning satellite orbits, assists in developing and coordinating worldwide technical standards, and works to improve telecommunication infrastructure in the developing world.** It is also **active** in the areas of broadband Internet, optical communications (including optical fiber technologies), wireless technologies, aeronautical and maritime navigation, radio astronomy, satellite-based meteorology, TV broadcasting, amateur radio, and **next-generation networks**.

Standardul IEEE 1906.1: Nanocomunicațiile ca o nouă sursă de date

Editura: IEEE

Sebastian Canovas-Carrasco ; Antonio-Javier Garcia-Sanchez ; Joan Garcia-Haro Toți autorii

Abstract:

Comunicațiile la scară nanometrică reprezintă o nouă paradigmă care cuprinde toate acele preocupări legate de schimbul de informații între dispozitive la scară nanometrică. Este avută în vedere o infrastructură de rețea constând dintr-o cantitate imensă de nano-dispozitive pentru a asigura o transmisie de date robustă, fiabilă și coordonată. Acest lucru va permite o multitudine de aplicații și servicii viitoare în multe domenii de cercetare diferite, cum ar fi medicina personalizată, biologia sintetică, știința mediului sau industria, ceea ce va duce la progrese remarcabile și fără precedent. Standardul IEEE P1906.1 oferă un cadru conceptual și general pentru a stabili punctul de plecare pentru dezvoltările viitoare în rețelele de comunicații la scară nanometrică. Această lucrare trece în revistă cele mai recente recomandări IEEE P1906.1, observându-le principalele caracteristici atunci când sunt aplicate în zona de nanocomunicații electromagnetice (EM). Contribuim prin identificarea și discutarea principalelor deficiențe ale standardului, cărora trebuie să se dedice eforturi de cercetare ulterioare. De asemenea, oferim linii directoare interesante pentru focalizarea obiectului investigațiilor viitoare.

Publicat în: 2017 ITU Kaleidoscope: Challenges for a Data-Driven Society (ITU K)

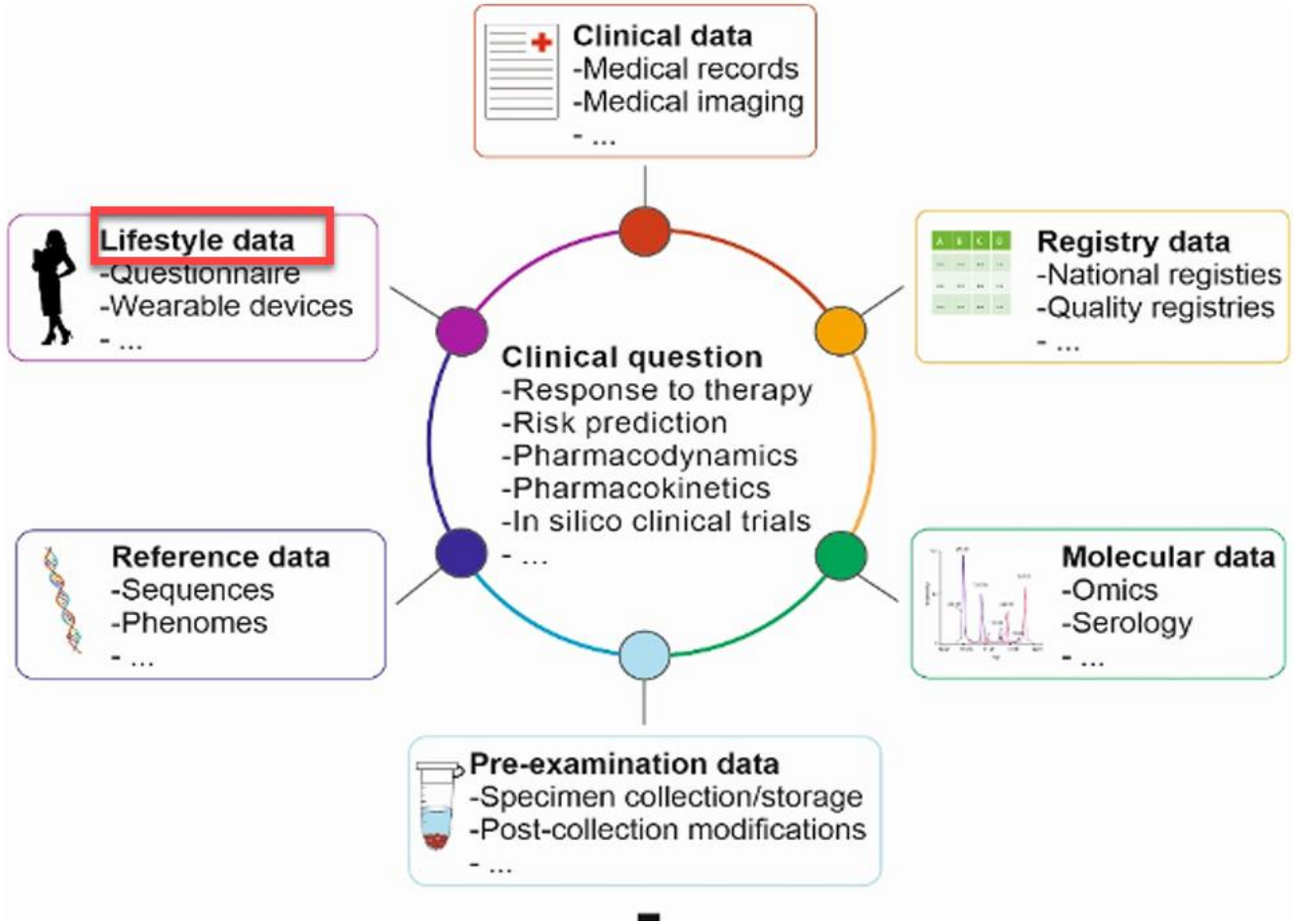
https://ieeexplore.ieee.org/document/8247001

Bio-digital convergence standardization opportunities IEC (2024-04-29)

3.3 Human digital twins/virtual human twins

3.3.1 Description

The human digital twin or virtual human twin (VHT) is an integrated multiscale, multi-time, and multi-discipline digital representation of quantitative human physiology and pathology that plays an important role for personalized medicine approaches. Its realization through



https://www.iec.ch/basecamp/bio-digital-convergence-standardization-opportunities

Bio-digital convergence standardization opportunities

2024-04-29

Available for download: English

Download Share Order paper copy

The term bio-digital convergence denotes the convergence of engineering, nanotechnology, biotechnology, information technology and cognitive science. While the concept is at least 20 years old, developments in the area have been turbocharged by the fast-paced changes and evolution of information and digital technologies.

Such multi-disciplinary solutions are key to tackling global environmental, governmental and societal challenges. Breakthroughs in biomedical devices, artificial organs and stem cell research have been vital to modern healthcare solutions. Agricultural bioengineering or genetic engineering of food helps address global challenges around hunger and economic welfare. Strides in environmental monitoring are crucial to managing clean air, water or soil. With a rapidly evolving technology landscape, it becomes imperative for standards around the area to co-evolve to ensure efficient progress.

https://www.iec.ch/basecamp/bio-digital-convergence-standardization-opportunities

Technology Report

Bio-digital convergence standardization opportunities

https://www.iec.ch/basecamp/bio-digital-convergence-standardization-opportunities

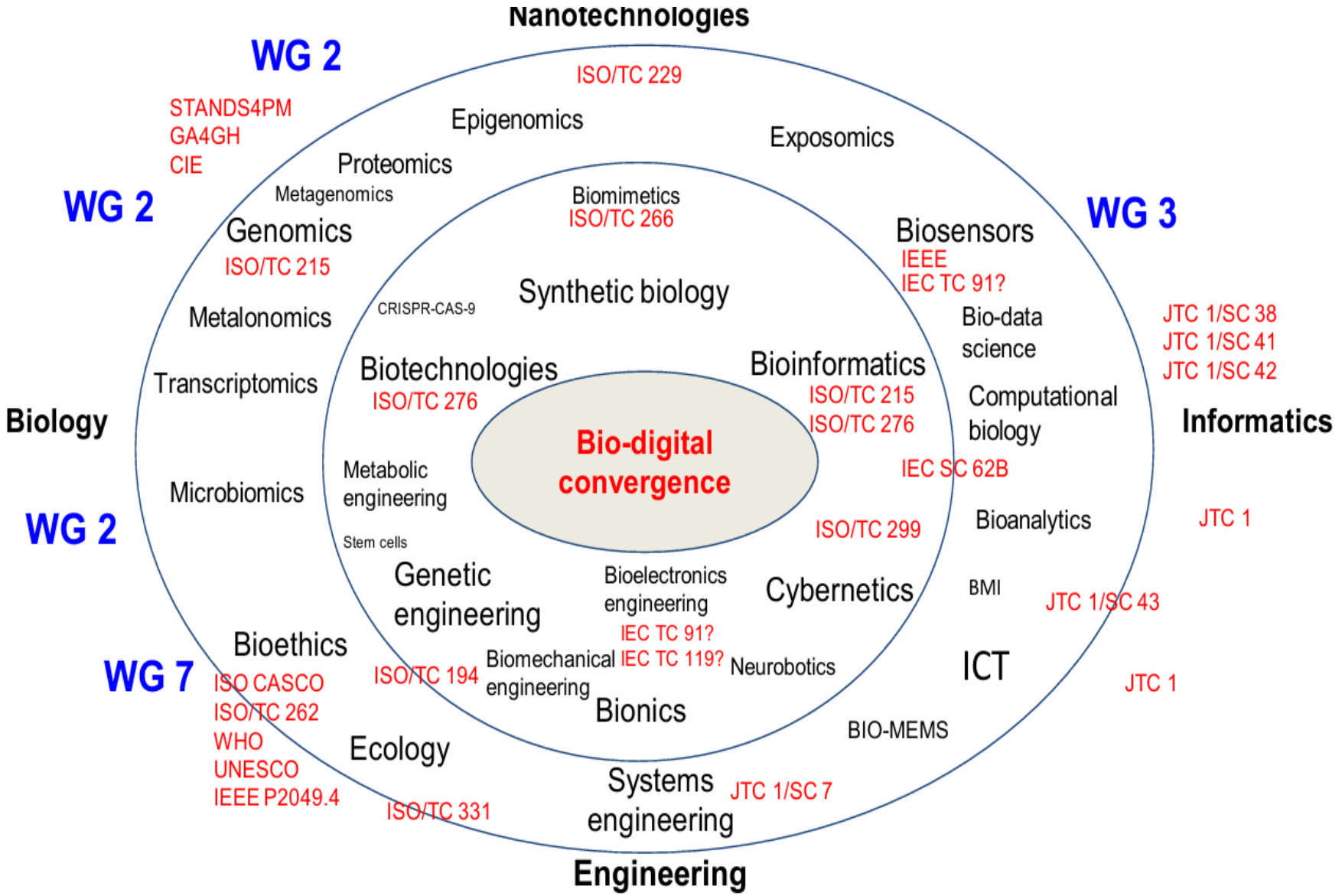


Figure 1 | Bio-digital convergence components

Bio-digital convergence standardization opportunities

https://www.iec.ch/basecamp/bio-digital-convergence-standardization-opportunities

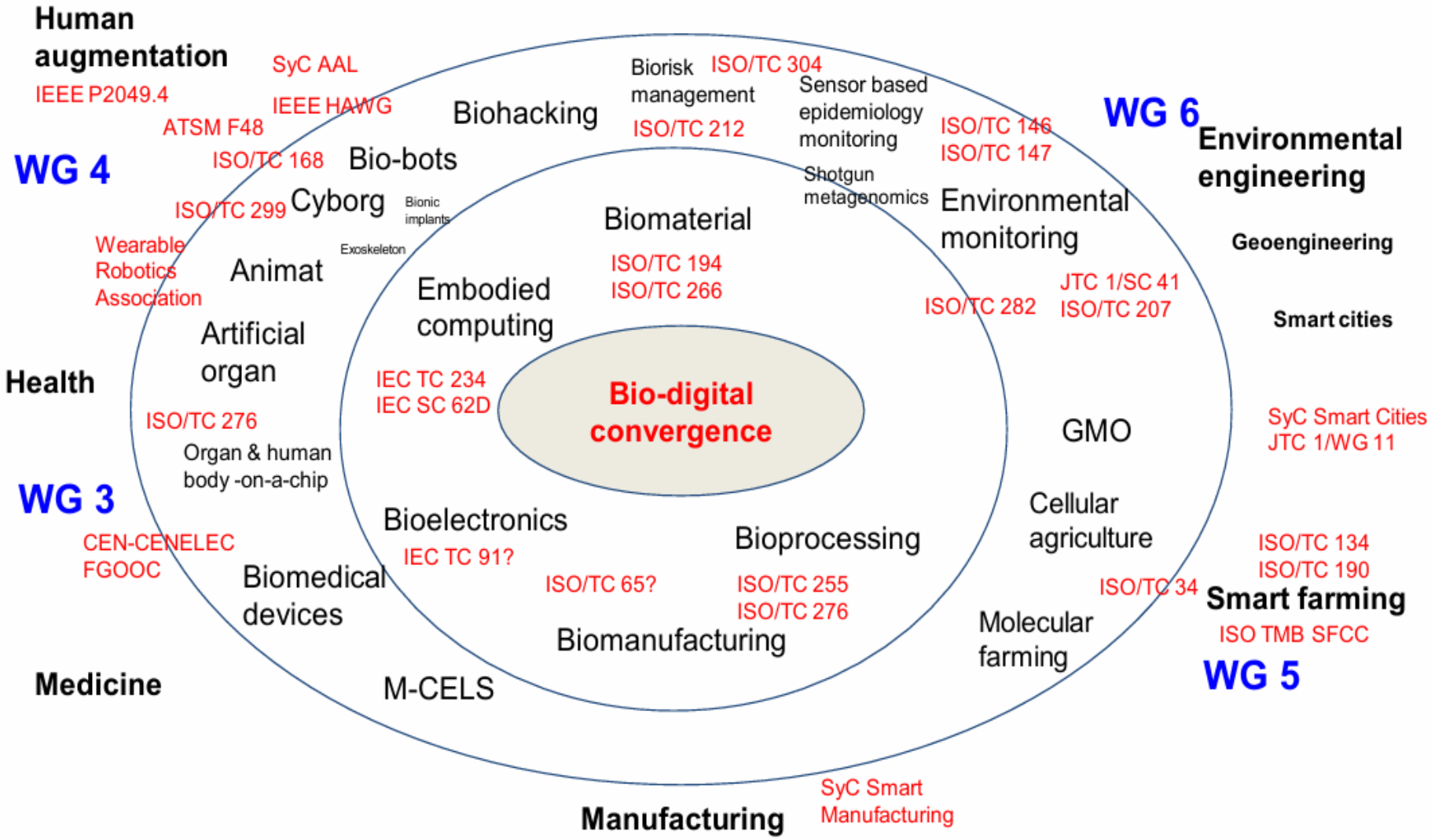


Figure 4 | Bio-digital convergence applications

Future Standards for Bio-digital – Convergence

UCL - University College London

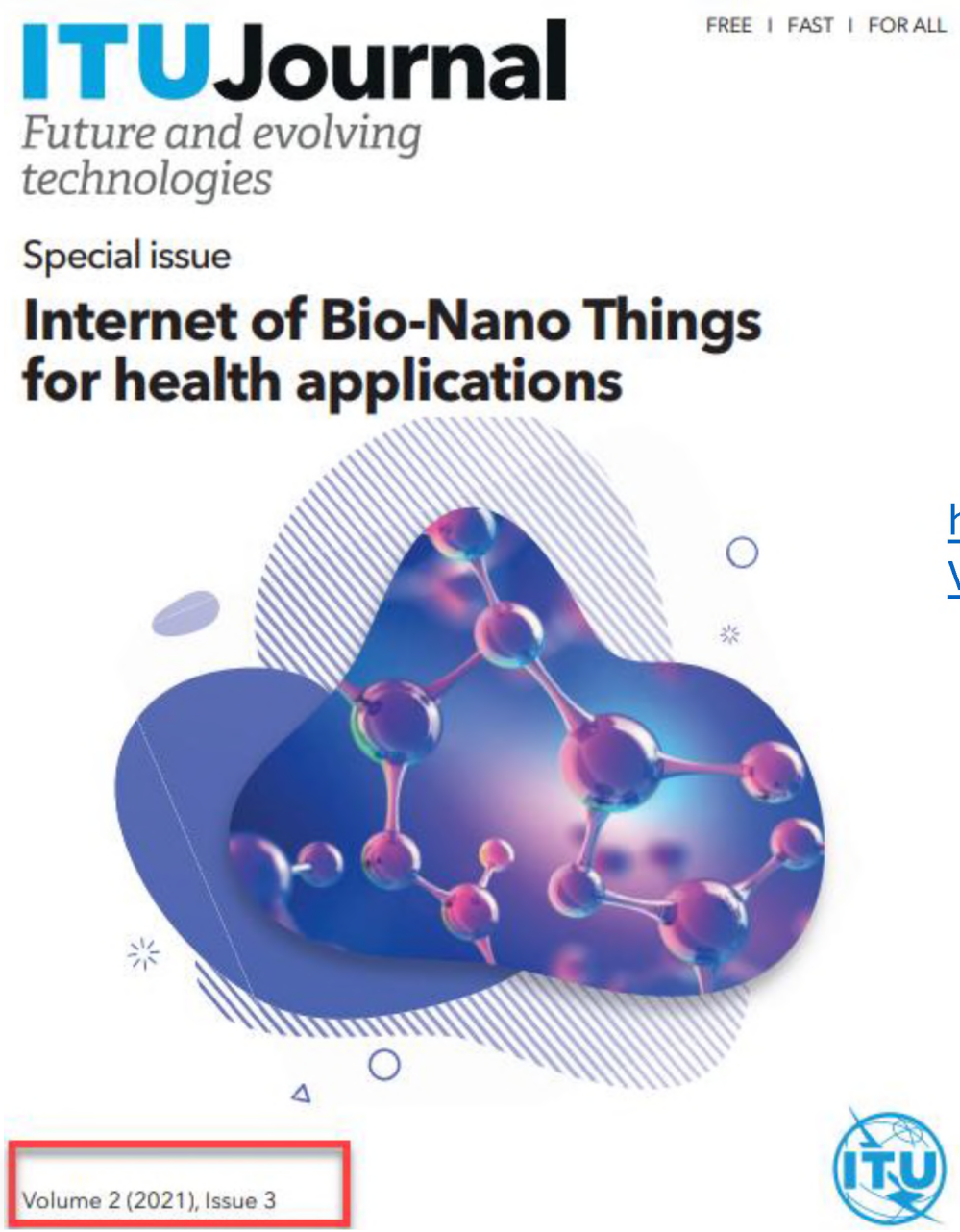
IEC SEG 12 established six Working Groups, each tasked with exploring critical issues related to bio-digital convergence in the current standardization landscape and identifying potential standardization opportunities. These Working Groups focus on the following areas:

- Working Group 1: Reverse Engineering of Living Systems (“WG1”)
- Working group 2: Life Systems and Bioengineering (“WG2”)
- Working group 3: Human Augmentation Technologies (“WG3”)
- Working group 4: Agricultural Bioengineering (“WG4”)
- Working group 5: Environmental Bioengineering (“WG5”)
- Ad-hoc Working Group: Bio-digital convergence ethical and societal considerations (“ahG7”)

https://www.ucl.ac.uk/steapp/sites/steapp/files/1_final_report_-_future_standards_for_bio-digital_convergence.pdf

https://www.itu.int/en/journal/j-fet/2021/003/Pages/default.aspx

- The **Terahertz (THz) band from 0.1 THz to 10 THz will be of paramount importance for wireless communications in the next decade**.
- In particular, **due to its abundant frequency resources,** the THz band will be a key to overcome the spectrum scarcity and capacity limitations inherent to current wireless systems.
- It is anticipated that THz band communications **will enable unprecedented applications both at the macro-scale and at the nano-scale**, ranging from high-speed satellite communications, ultra-high-capacity wireless fronthaul/backhaul in cellular networks, ultra-high-speed short-distance data transfer between devices, to inter/intra-chip communications and **instantaneous data exchange between nano-scale devices.**



https://www.itu.int/dms_pub/itu-s/opb/jnl/S-JNL-VOL2.ISSUE3-2021-PDF-E.pdf

National Science and Technology Council
Committee on Technology
Interagency Working Group on Nanoscience, Engineering and Technology (IWGN)

Nanotechnology Research Directions: IWGN Workshop Report

Vision for Nanotechnology R&D in the Next Decade

SEPTEMBER 1999

About the National Science and Technology Council

President Clinton established the National Science and Technology Council (NSTC) by Executive Order on November 23, 1993.

https://www.nano.gov/sites/default/files/IWGN_rd.pdf

There are numerous other potential applications of nanoscience to biology:

- Rapid, efficient **genome sequencing**, revolutionizing diagnostics and therapeutics
- **Effective and less expensive healthcare using remote and in-vivo devices**
- **New formulations and routes for drug delivery** that enormously broaden their therapeutic potential by effecting **delivery of new types of medicine to previously inaccessible sites in the body**
- More durable, **rejection-resistant artificial tissues and organs**
- **Sensor systems** that detect emerging disease in the body, which will shift the focus of patient care from **disease treatment to early detection and prevention**

Interagency Working Group on Nanoscience, Engineering and Technology (IWGN)

Chair: M.C. Roco, NSF
White House IWGN Co-chair: T.A. Kalil, Special Assistant to the President, W.H. Economic Council
Vice-chair: R. Trew, DOD
Executive Secretary: J.S. Murday, NRL
Members:

White House:	T.A. Kalil
OSTP:	K. Kirkpatrick
NSTC:	J. Porter
OMB:	D. Radzanowski
DOC:	P. Genther-Yoshida, M.P. Casassa (NIST), R.D. Shull (NIST)
DOD:	R. Trew, J.S. Murday (NRL), G.S. Pomrenke (AFOSR)
DOE:	I.L. Thomas, R. Price, B.G. Volintine
DOT:	R.R. John, A. Lacombe (Volpe Center)
DoTREAS:	E. Murphy
NASA:	S. Venneri, G.H. Mucklow, M. Meyyappan (NASA Ames), T. Krabach (JPL)
NIH:	J.A. Schloss, E. Kousvelari
NSF:	M.C. Roco, T.A. Weber, M.P. Henkart

Public Affairs Consultant: J. Canton

https://www.nano.gov/sites/default/files/IWGN_rd.pdf

WORLD ECONOMIC FORUM

COMMITTED TO IMPROVING THE STATE OF THE WORLD

The Fourth Industrial Revolution

During the summer of 2015, Professor Schwab proposed that the theme of Annual Meeting 2016 focus on the incredible speed and scale with which technology is disrupting all industries and economies around the world. Reflecting on the wealth of work by a wide range of experts on the impacts of digitisation and emerging technologies, including in depth work by the Forum itself, Schwab realised that these changes were of such a fundamental nature that they constitute nothing less than a new industrial revolution. This led to the World Economic Forum Annual meeting 2016 theme becoming "Mastering the Fourth Industrial Revolution", to a series of expert consultations in Abu Dhabi in November 2015 and to Professor Schwab writing in under three months a best-selling book on the dramatic ways in which technology, business and society are co-evolving.

The fourth industrial revolution describes a global transformation characterized by the convergence of digital, physical, and biological technologies. These technologies are influencing societies, economies and individuals in ways that are changing not just the world around us but the very idea of what it means to be human. The resulting transformation is historic in terms of its size, speed, and scope. This transformation is

https://www3.weforum.org/docs/Media/AM17/AM17_4IR.pdf

As powerful technologies such as artificial intelligence, advanced materials, augmented reality, 3D printing and new computing technologies become increasingly affordable and ultimately ubiquitous, they are altering the way we produce, consume, communicate, move, generate energy, and interact with one another. And given the new powers in genetic engineering and neurotechnologies, they may directly impact who we are and how we think and behave. The fundamental and global nature of this revolution also poses new threats related to the disruptions it may cause—affecting labor markets and the future of work, income inequality, and geopolitical security as well as social value systems and ethical frameworks.

Over the course of 2016, the Forum has deepened and extended its work on technology and society, and in October 2016 announced a new office, to open in San Francisco in February 2017: the World Economic Center for the Fourth Industrial Revolution. The Center will accelerate global cooperation for effectively and efficiently governing of the fourth industrial revolution, helping corporations, governments, civil society leaders, researchers and other stakeholders to realize the greatest positive societal impact from new technologies and scientific developments.

Unless we govern the fourth industrial revolution properly then its full economic and social potential will not be realised. As Gillian Hadfield, Professor of law and economics at the University of Southern California, argues, this means that rethinking how we make new rules is as important as deciding what rules we need. Governance is a sine qua non of economic and social progress: to be responsive and responsible in the fourth industrial revolution, during the course of 2017 leaders across all sectors need to work together to create agile governance models for an inclusive, prosperous, human-centred future.

https://www3.weforum.org/docs/Media/AM17/AM17_4IR.pdf

- A proof that the fourth industrial revolution **was not the demand of the people but the decision of organizations like the World Economic Forum**, and that Human Rights were violated.
- “And if we look at other **implications of the fourth industrial revolution**, I just want to mention the impact this revolution has on us. **It changes not only what we do, it changes us**. We create algorithms but algorithms can change us and our behavior. And we haven't really thoughts what it means. **But this again amplifies the fear of people who feel they are losing control,** and then of course they try to find protection in believing in, let's say, more populist approaches.”

2019 World Economic Forum Founder Klaus Schwab on the Fourth Industrial Revolution - https://www.youtube.com/live/CVIy3rjuKGY between minutes 21.16 - 23.06

WORLD ECONOMIC FORUM

COMMITTED TO IMPROVING THE STAT OF THE WORLD

Global Agenda

Top 10 Emerging Technologies of 2016

By the World Economic Forum's Meta-Council on Emerging Technologies

June 2016

https://www3.weforum.org/docs/GAC16_Top10_Emerging_Technologies_2016_report.pdf

Contents

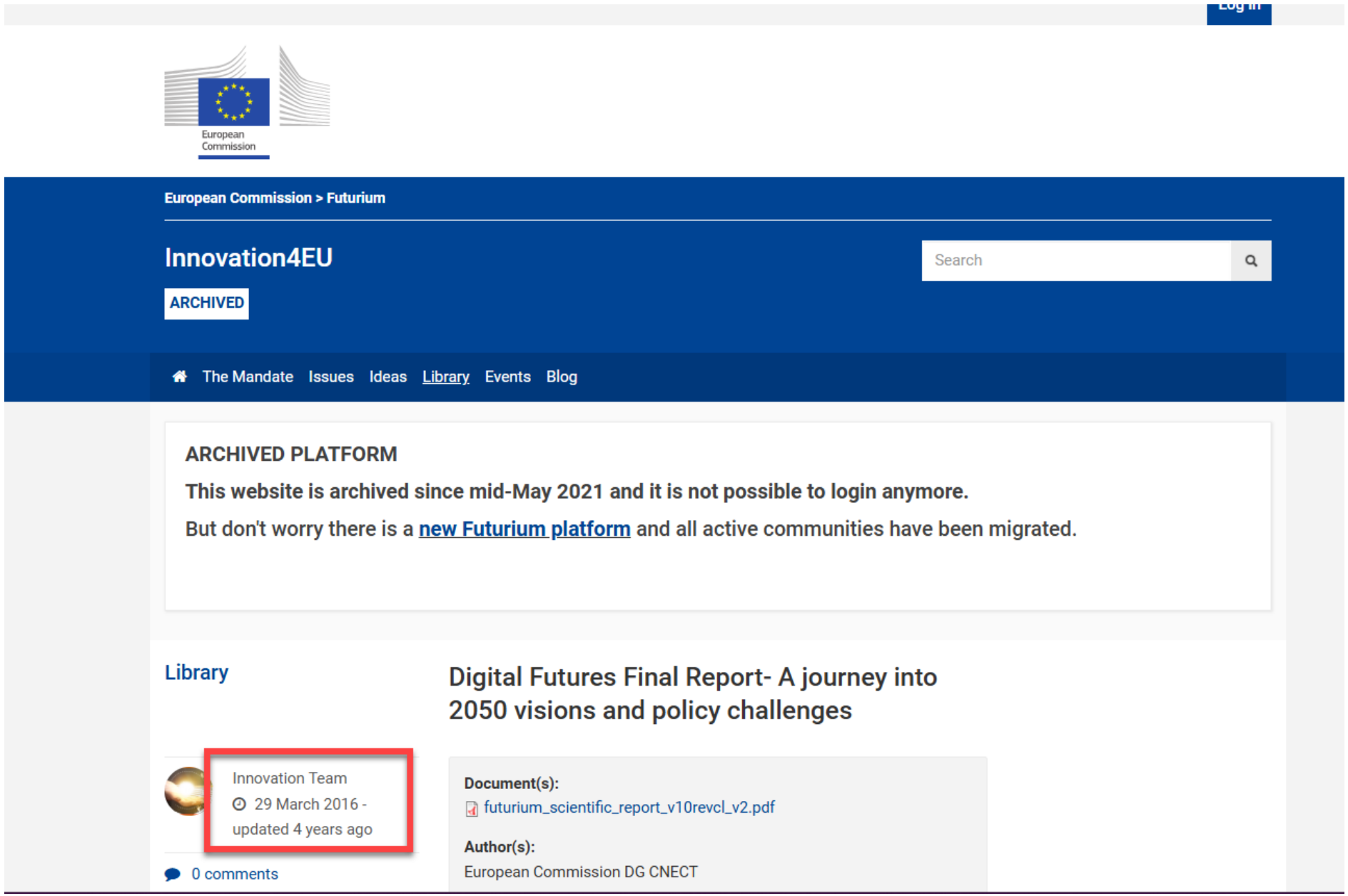
HEALTH AND HEALTHCARE SYSTEMS

Tracking how our bodies work could change our lives

Jun 4, 2020

https://www.weforum.org/stories/2020/06/internet-of-bodies-covid19-recovery-governance-health-data/

- We're entering the era of the "Internet of Bodies": collecting our physical data via a range of devices that can be implanted, swallowed or worn.
- The result is a huge amount of health-related data that could improve human wellbeing around the world, and prove crucial in fighting the COVID-19 pandemic.
- But a number of risks and challenges must be addressed to realize the potential of this technology, from privacy issues to practical hurdles.



https://ec.europa.eu/futurium/en/content/digital-futures-final-report-journey-2050-visions-and-policy-challenges.html

Directia generală Rețele de comunicații, conținut și tehnologie

Shape the Future

A trans-humanistic era

By 2050, a new form of human (a trans-human) will emerge, where ICTs and bio-medicine will fundamentally improve the human condition and greatly enhance human intellectual, physical, and psychological capacities.

The augmentation of human beings' cognitive and intellectual abilities through technological implants, such as memory and energy storage, will be possible.

Information and Communication Technology (ICT)

Long Term

Brain-to-Brain communication via implants

- Inter-personal communication will be mediated through technology capable of reading information from the brain (for instance through brain waves interpretation) and exchanging this information with other humans according to "trust" profiles.
- Data and information can be shared with other humans or machines through quantum communication links.
- Data will be received by brain implants and actuated instantaneously, i.e. the rational and emotional states of the originating human will be perceived by the receiving human(s) as if they are actually experienced. This will allow achieving the myth of telepathy.
- With increasingly reliable communication between multiple brains and bodies at the speed of quantum networks, thoughts will be instantaneously captured and shared between humans at a global level.

Genetically Enhanced Humans (GEH) will be the majority in the world

- With improved implant techniques and the creation of direct nerve connectors, body and sense enhancing implants are a common practice in 2050.
- They enhance the capabilities in normal functioning humans and provide normal or enhanced capabilities for impaired people. The visual implants make the blind see and the hearing implants make the deaf hear. Muscle implants make the weak stronger. Neural implants make the lame walk.
- GEH will be characterised by better senses and biological capabilities that are in so far prerogative of other species (e.g. speed, resistance, adaptation to extreme conditions, etc.).
- Following the philosophical path of trans-humanism, the augmentation of human's cognitive and intellectual abilities through technological implants, such as memory and energy storage, will be possible.

Enhancement option available that ensures effective treatment & management of chronic disease

- Nano devices and bio-computers provide life extending treatment.
- Nano-robots will help diagnosis and treatment of diseases at any age, including pre-birth surgery. They will be able to read from and write into our biology. They can also detect and destroy neoplasms, thus defeating cancer forever.
- Similar to nano-robots, bio-computers will be inoculated into the human body to perform complex tasks, for instance sensing and monitoring the status of organs or repairing tissues and organs in real-time, in-situ, at a micro and nano scale.

NBIC-convergence

- NBIC-convergence is the ongoing unification of nanotechnology, biotechnology, information technology and cognitive science.
- NBIC-convergence could allow us to enhance our intelligence, mobility, cognitive qualities or increase industrial productivity.

We are in the era of the Fourth Industrial Revolution (4IR), which is characterized by the convergence and complementarity of emerging technology domains, including nanotechnology, biotechnology, new materials and advanced digital production technologies. Despite the challenges posed by the disruptive nature of these innovations—which are increasingly connecting objects, machines, people and the environment—the digital transformation presents opportunities for inclusive and sustainable development.

https://www.unido.org/sites/default/files/files/2021-11/Standards%20and%20Digital%20Transformation_Complete_2021.pdf

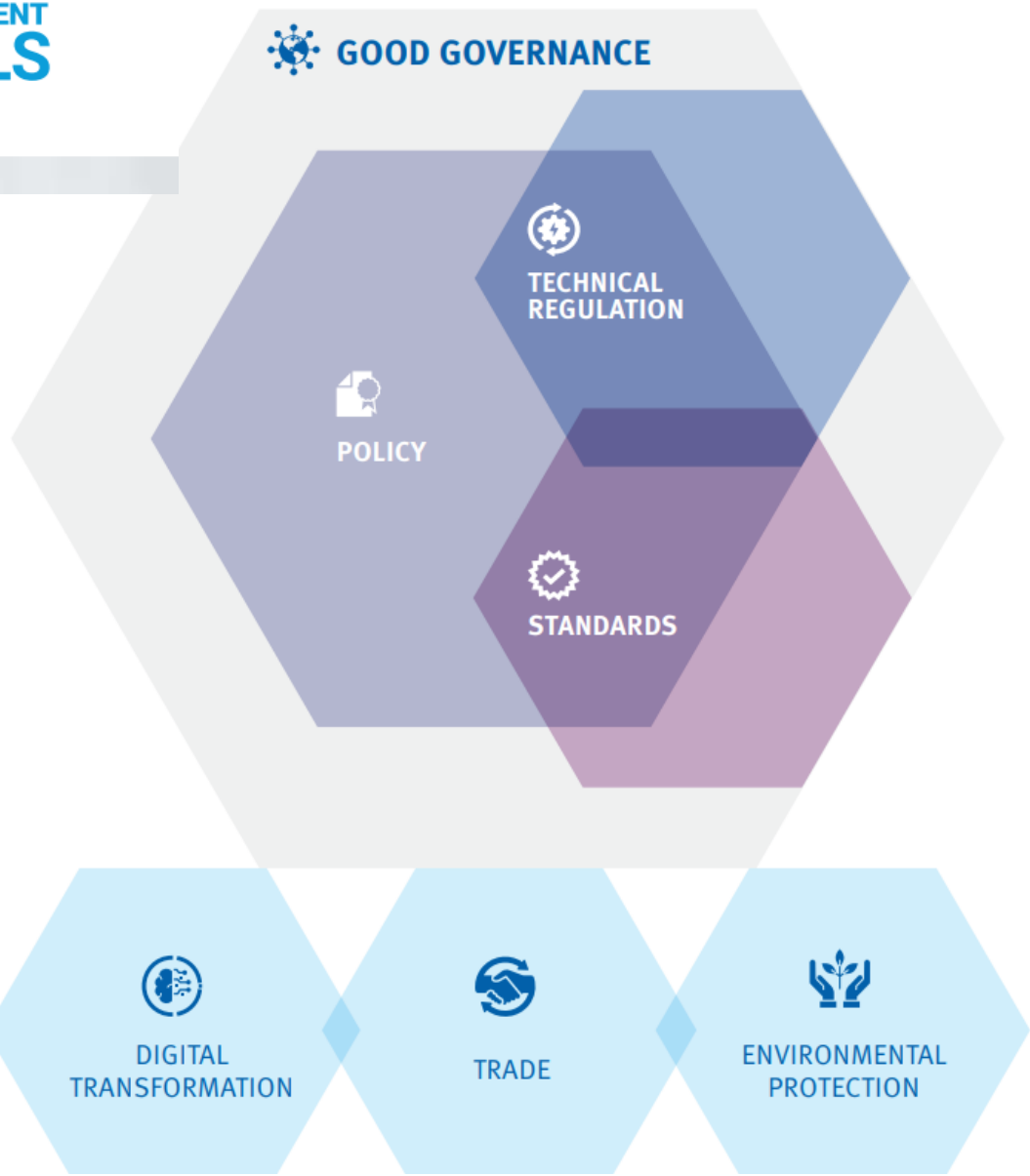
While revolutions and change have marked human development, what distinguishes the 4IR from previous industrial revolutions is the parallel technological breakthroughs within and across the digital, biological and physical spheres. The complexity and rapid pace of change of the 4IR also make the revolution distinctive. Moreover, the COVID-19 pandemic has been an unanticipated accelerator to the pace of change and structural shift towards the 4IR and the adoption of new technologies.

UNITED NATIONS
INDUSTRIAL DEVELOPMENT ORGANIZATION

SUSTAINABLE DEVELOPMENT GOALS

STANDARDS & DIGITAL TRANSFORMATION

GOOD GOVERNANCE IN A DIGITAL AGE



https://www.unido.org/sites/default/files/files/2021-11/Standards%20and%20Digital%20Transformation_Complete_2021.pdf

November 22, 2023

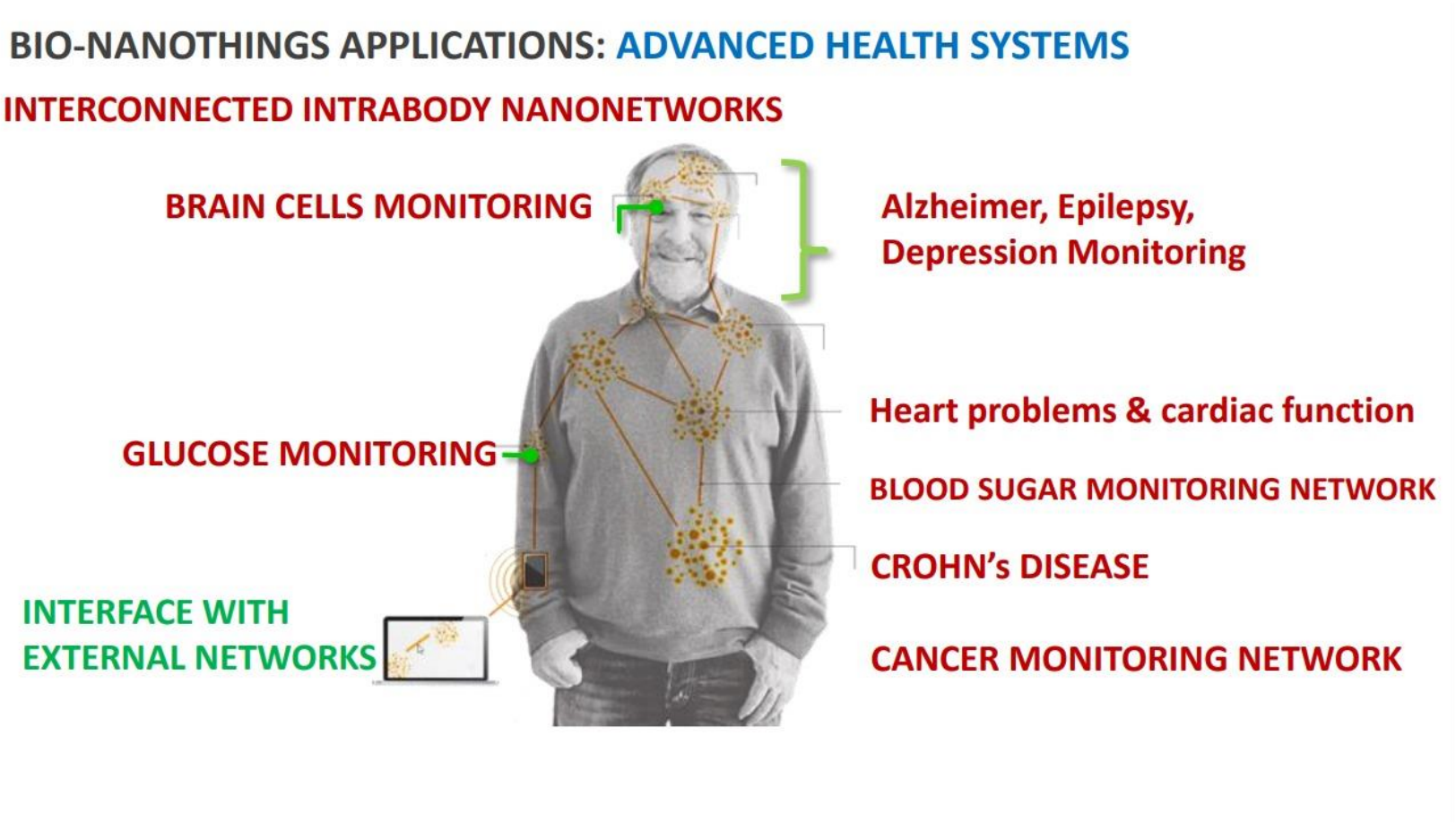
Nanotechnology \ Bio & Medicine

Networking nano-biosensors for wireless communication in the blood

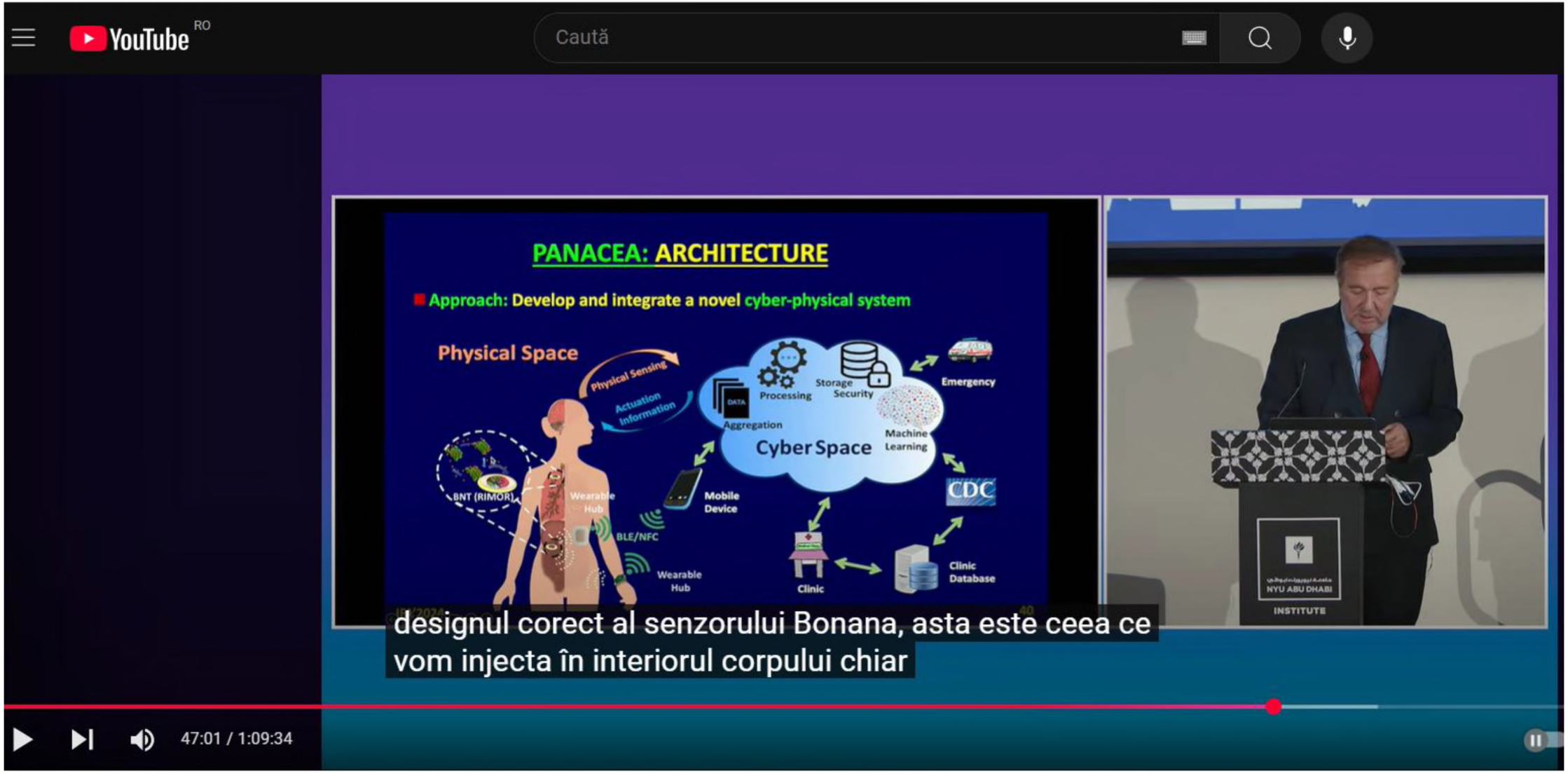
by Tanya Petersen , Ecole Polytechnique Federale de Lausanne

https://phys.org/news/2023-11-networking-nano-biosensors-wireless-communication-blood.amp

PANACEA: A Cyber-Physical System for Early Detection and Mitigation of Infections



https://www.itu.int/en/ITU-T/academia/kaleidoscope/2019/Documents/Presentations/Keynote%20speech_Ian_Akyildiz.pdf



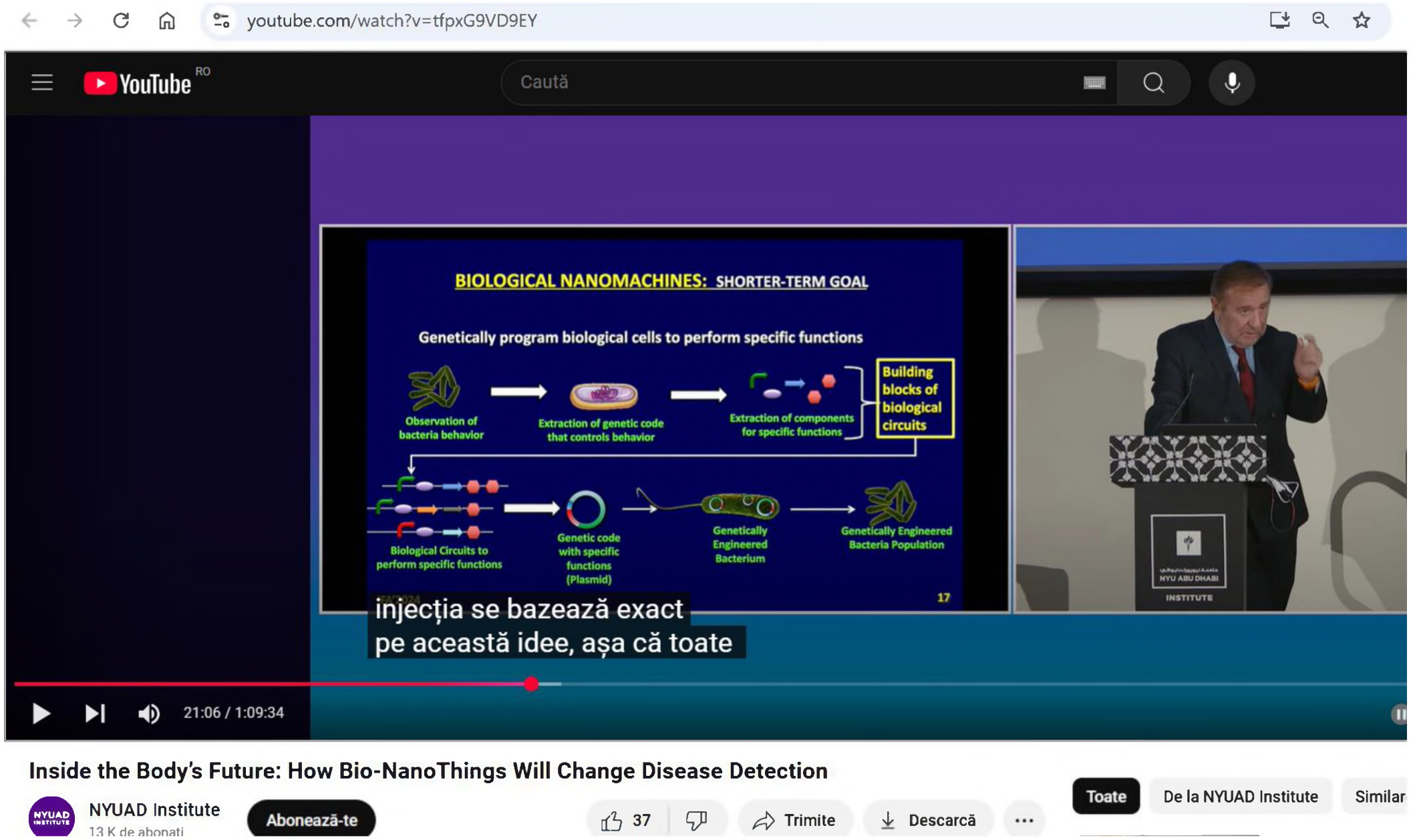
Inside the Body's Future: How Bio-NanoThings Will Change Disease Detection

NYUAD Institute
12,9 K de abonați
Abonează-te

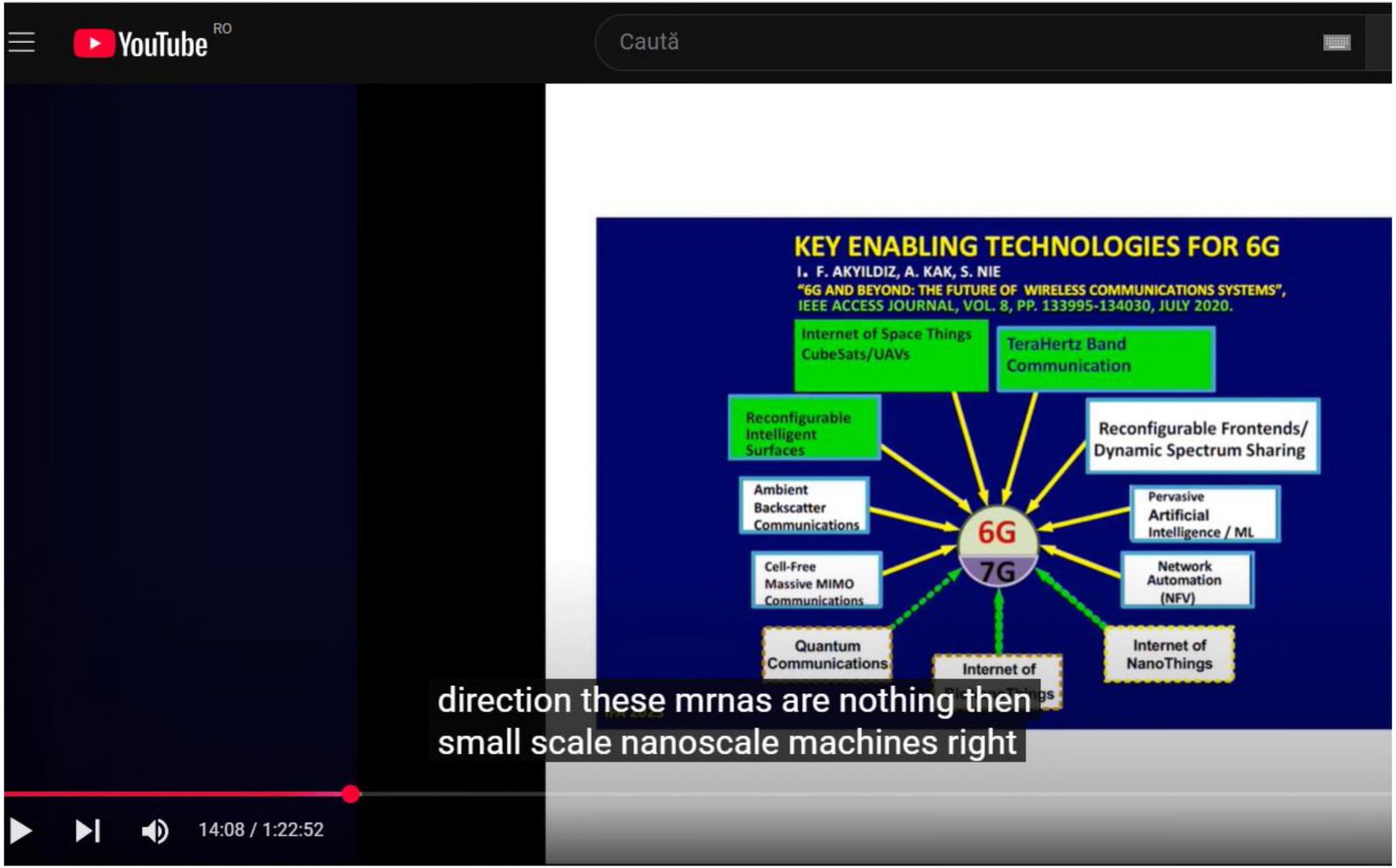
24 | Trimite | Descarcă | ...

Toate | De la NYUAD Institute | Pentru tin

https://www.youtube.com/watch?v=tfpxG9VD9EY



https://www.youtube.com/watch?v=tfpxG9VD9EY



ARRC Seminar Series - Prof. Ian F. Akyildiz

https://www.youtube.com/watch?v=YAtQFkEg5-w

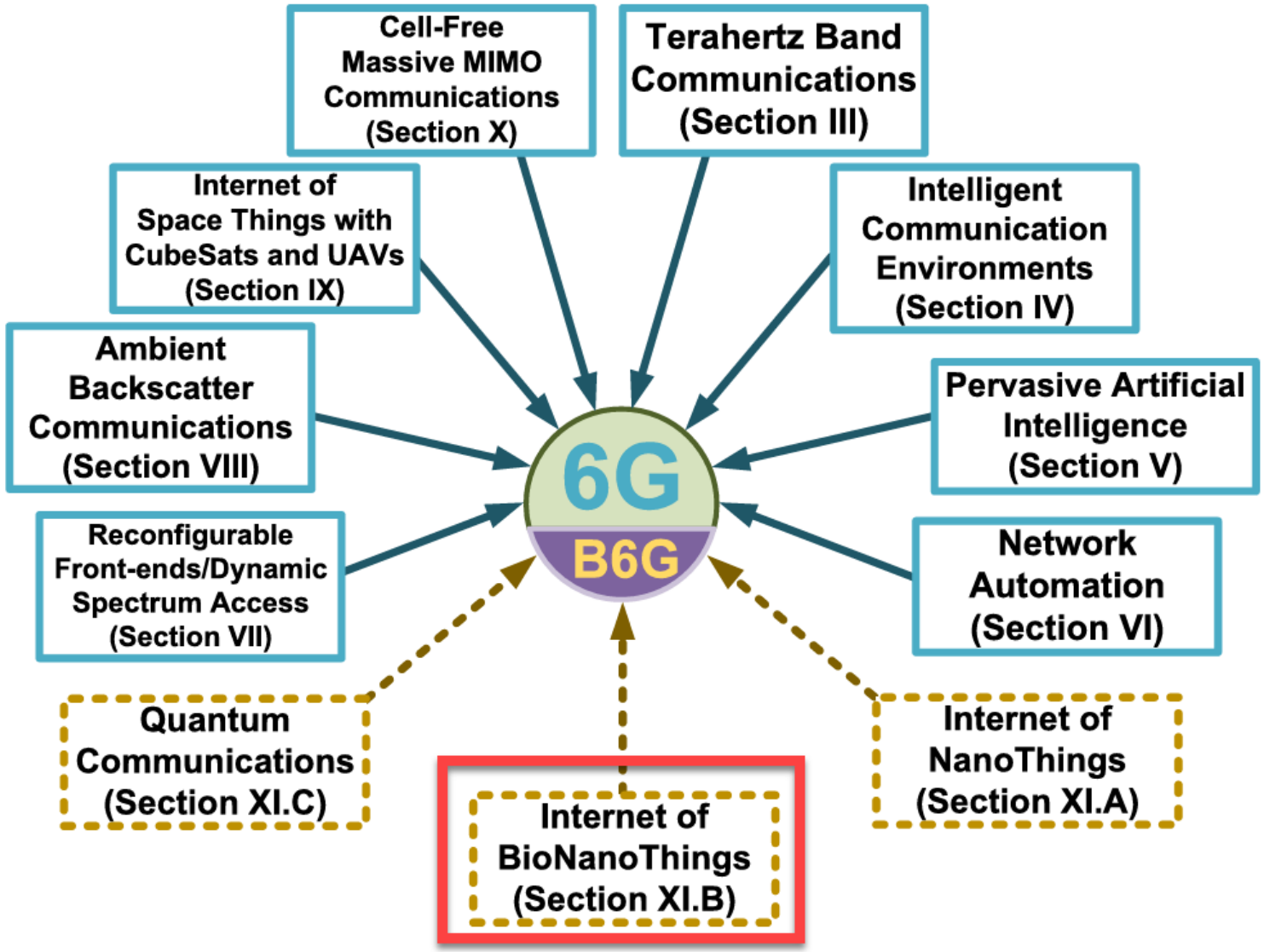


FIGURE 1. The envisioned key enabling technologies for 6G and beyond wireless communications systems.

https://ieeexplore.ieee.org/document/9145564

The internet of Bio-Nano things

Publisher: IEEE Cite This PDF

I. F. Akyildiz ; M. Pierobon ; S. Balasubramaniam ; Y. Koucheryavy All Authors

Abstract:

The Internet of Things (IoT) has become an important research topic in the last decade, where things refer to interconnected machines and objects with embedded computing capabilities employed to extend the Internet to many application domains. While research and development continue for general IoT devices, there are many application domains where very tiny, concealable, and non-intrusive Things are needed. The properties of recently studied nanomaterials, such as graphene, have inspired the concept of Internet of NanoThings (IoNT), based on the interconnection of nanoscale devices. Despite being an enabler for many applications, the artificial nature of IoNT devices can be detrimental where the deployment of NanoThings could result in unwanted effects on health or pollution. The novel paradigm of the Internet of Bio-Nano Things (IoBNT) is introduced in this paper by stemming from synthetic biology and nanotechnology tools that allow the engineering of biological embedded computing devices. Based on biological cells, and their functionalities in the biochemical domain, Bio-NanoThings promise to enable applications such as intra-body sensing and actuation networks, and environmental control of toxic agents and pollution. The IoBNT stands as a paradigm-shifting concept for communication and network engineering, where novel challenges are faced to develop efficient and safe techniques for the exchange of information, interaction, and networking within the biochemical domain, while enabling an interface to the electrical domain of the Internet.

Published in: IEEE Communications Magazine (Volume: 53 , Issue: 3, March 2015)

https://ieeexplore.ieee.org/document/7060516

MAC Protocol Selection and Performance Analysis in Wireless Body Area Networks

Publisher: IEEE Cite This PDF

Bhavana Alte ; Amarsinh Vidhate **All Authors**

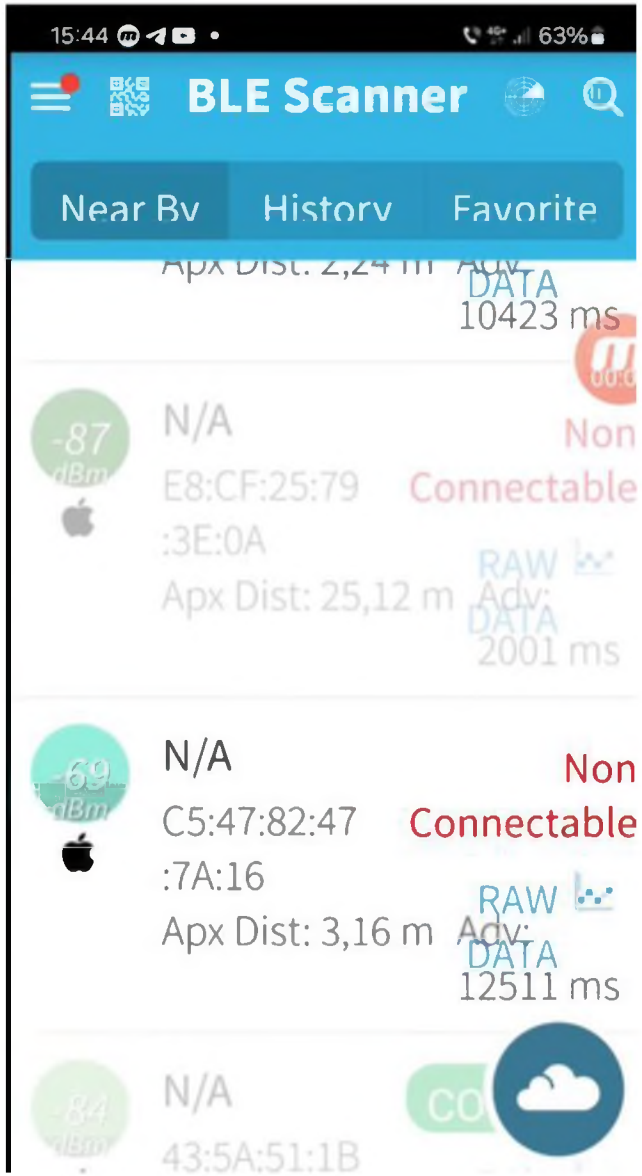
Abstract:

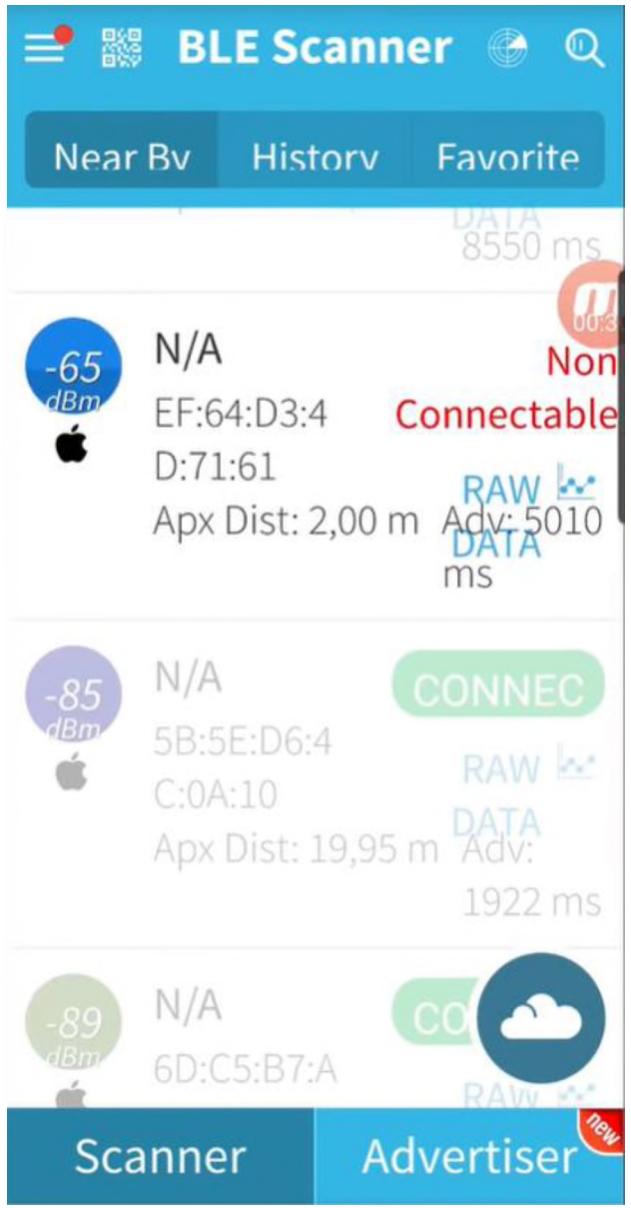
Over the last few decades, health monitoring systems based on wireless sensor networks have seen an exceptional surge in popularity. Wireless body area networks (WBANs) play a crucial role in enhancing the efficiency of medical services via a remote monitoring environment. Several small battery-operated implanted or wearable sensors in WBAN have many challenges in improving energy, quality, and operational performance. Prioritizing sensor nodes, selecting a sink node, and reducing control packet overheads are all ways to save energy while still handling emergency data, which has always been a significant problem for Wireless Body Area Networks (WBAN). Various researchers proposed a modified super-frame architecture of the MAC layer for efficient energy utilization, emergency traffic management, reliability, etc. In this paper, we have discussed significant observations of different MAC layers along modified super-frame architectures proposed by numerous researchers. Later, we provided comparative simulation observations of IEEE 802.15.4 and IEEE 802.15.6. By utilizing Guaranteed Time Slot (GTS) and polling mechanism, these results focus on providing decisive factors for selecting the acceptable MAC protocol in the medical context. Finally, we have provided a conclusion of our analysis for selecting the appropriate MAC protocol in WBAN.

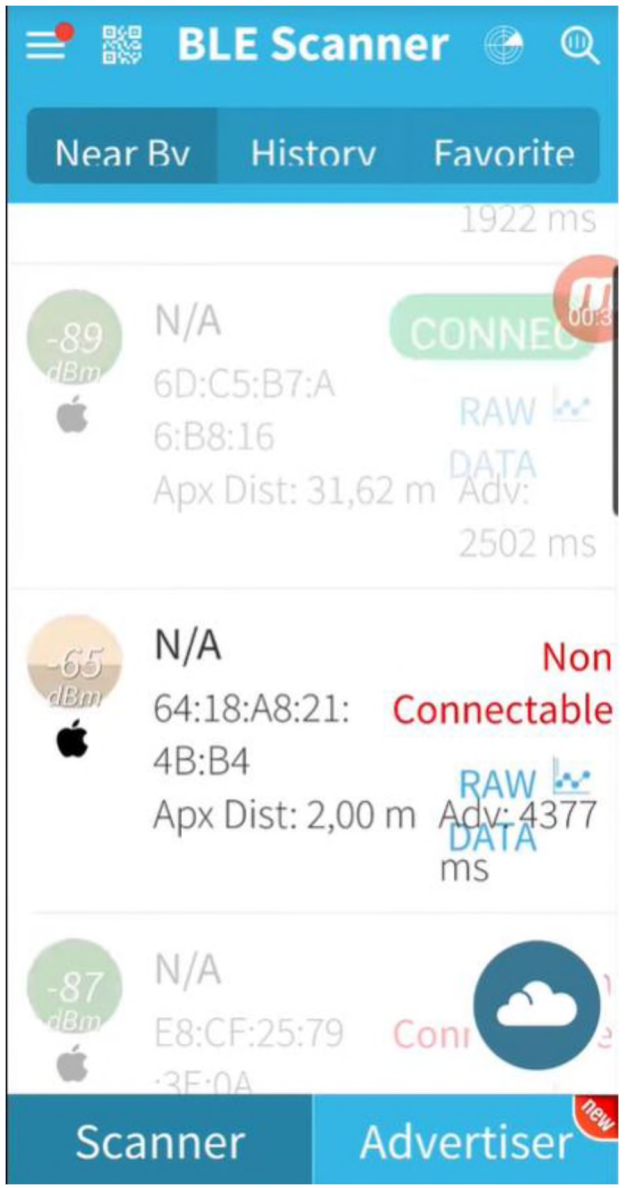
Published in: 2022 IEEE 2nd Mysore Sub Section International Conference (MysuruCon)

https://ieeexplore.ieee.org/document/9972349

Adrese MAC emise de persoanele de la saună





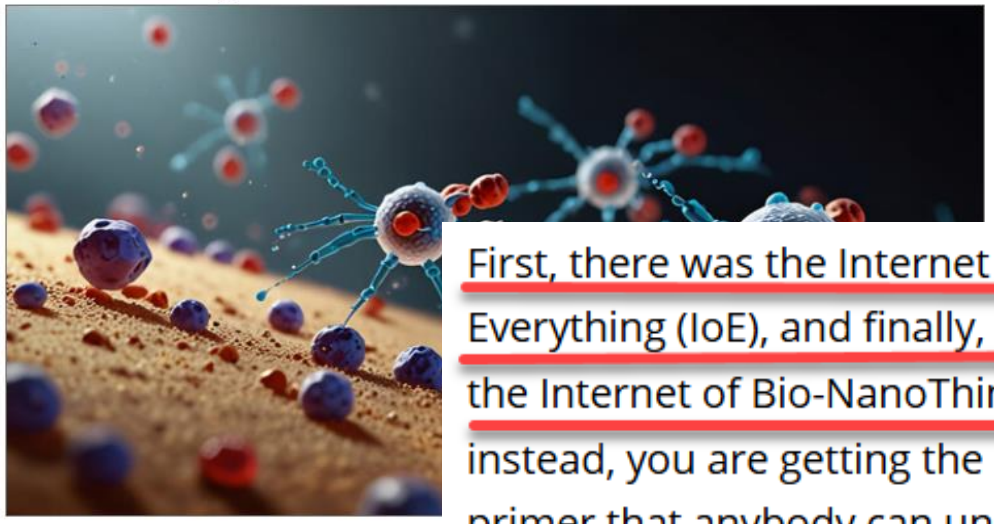


Children's Health Defense

CHD HOME DEFENDER NEWS CHD.TV RESOURCES COMMUNITY SCIE

ELECTROMAGNETIC RADIATION & WIRELESS • NEWS FROM AROUND THE WORLD
AUGUST 22, 2024

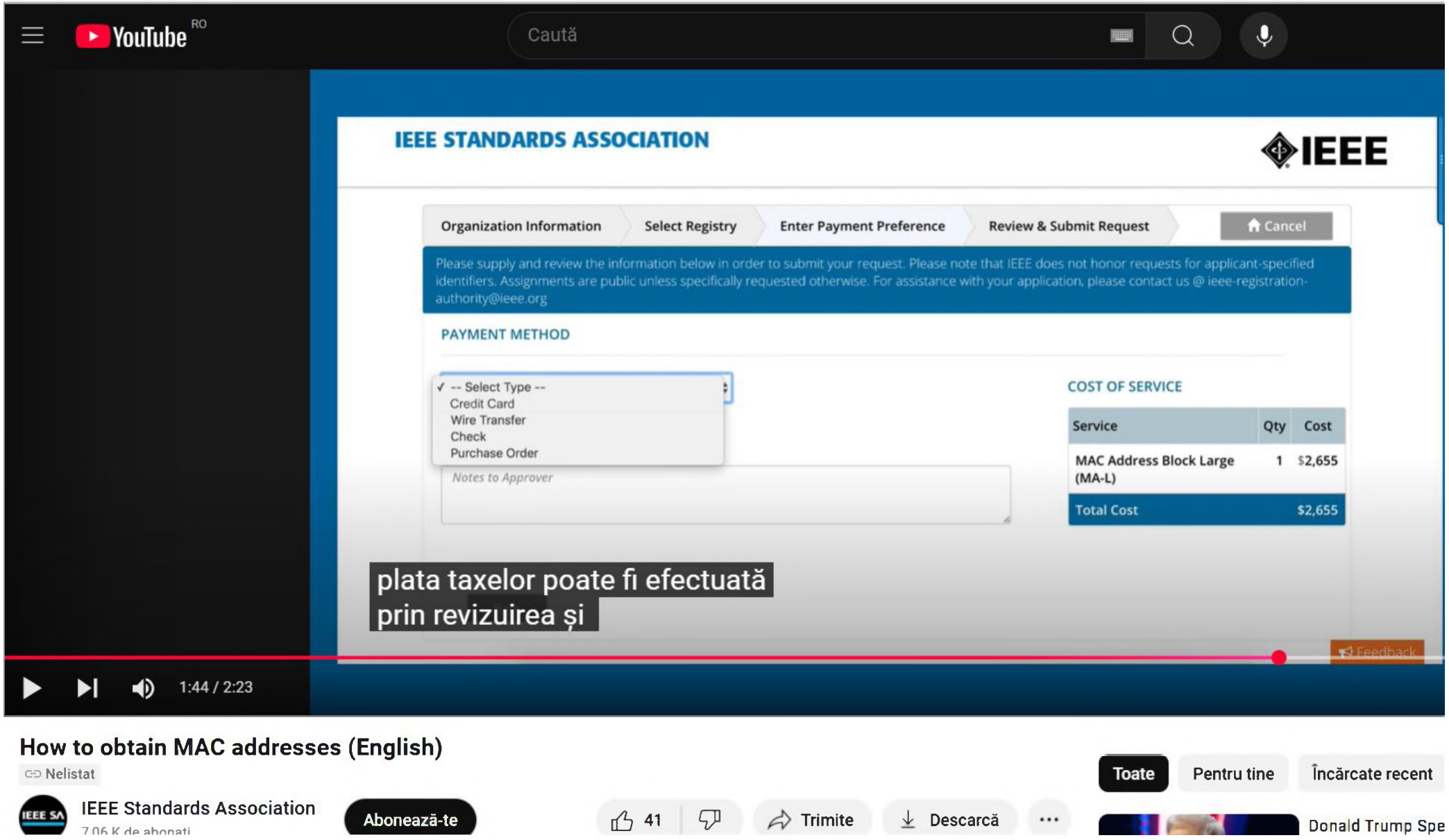
Under The Skin: The Internet Of Bio-NanoThings



First, there was the Internet of Things (IoT), then the Internet of Bodies (IoB), the Internet of Everything (IoE), and finally, Big Pharma and the military are going into your blood to construct the Internet of Bio-NanoThings (IoBNT). You might have hoped for the Internet of Nothing, but instead, you are getting the Internet Of Universal Skynet (IoUS). This paper from March 2015 is a primer that anybody can understand, including you. The IoBNT is the final building block of the surveillance network, bridging all living things from the biochemical domain into the electrical domain of the Internet.

There was no warning that nanotechnology of this sort was being pumped into your veins when you received a mRNA injectable from Pfizer or Moderna. Not a word from the government, Big Pharma, or the Military. There was no Informed Consent offered. The non-stop propaganda blared "Safe and Effective."

https://childrenshealthdefense.org/emr/under-the-skin-the-internet-of-bio-nanothings/



https://www.youtube.com/watch?v=0nlkxVfyxL4&t=86s
https://standards.ieee.org/products-programs/regauth/mac/

IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received September 2, 2018, accepted September 19, 2018, date of publication October 4, 2018, date of current version October 29, 2018.

Digital Object Identifier 10.1109/ACCESS.2018.2873825

Security in Wireless Body Area Networks: From In-Body to Off-Body Communications

MUHAMMAD USMAN[1], (Member, IEEE), MUHAMMAD RIZWAN ASGHAR[2], IMRAN SHAFIQUE ANSARI[3], (Member, IEEE), AND MARWA QARAQE[1]

[1]Division of Information and Computing Technology, College of Science and Engineering, Hamad Bin Khalifa University, Doha 34110, Qatar
[2]Department of Computer Science, The University of Auckland, Auckland 1142, New Zealand
[3]School of Engineering, University of Glasgow, Glasgow G12 8QQ, U.K.

Corresponding author: Muhammad Usman (musman@hbku.edu.qa)

The publication of this article was funded by the Qatar National Library.

https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8481660

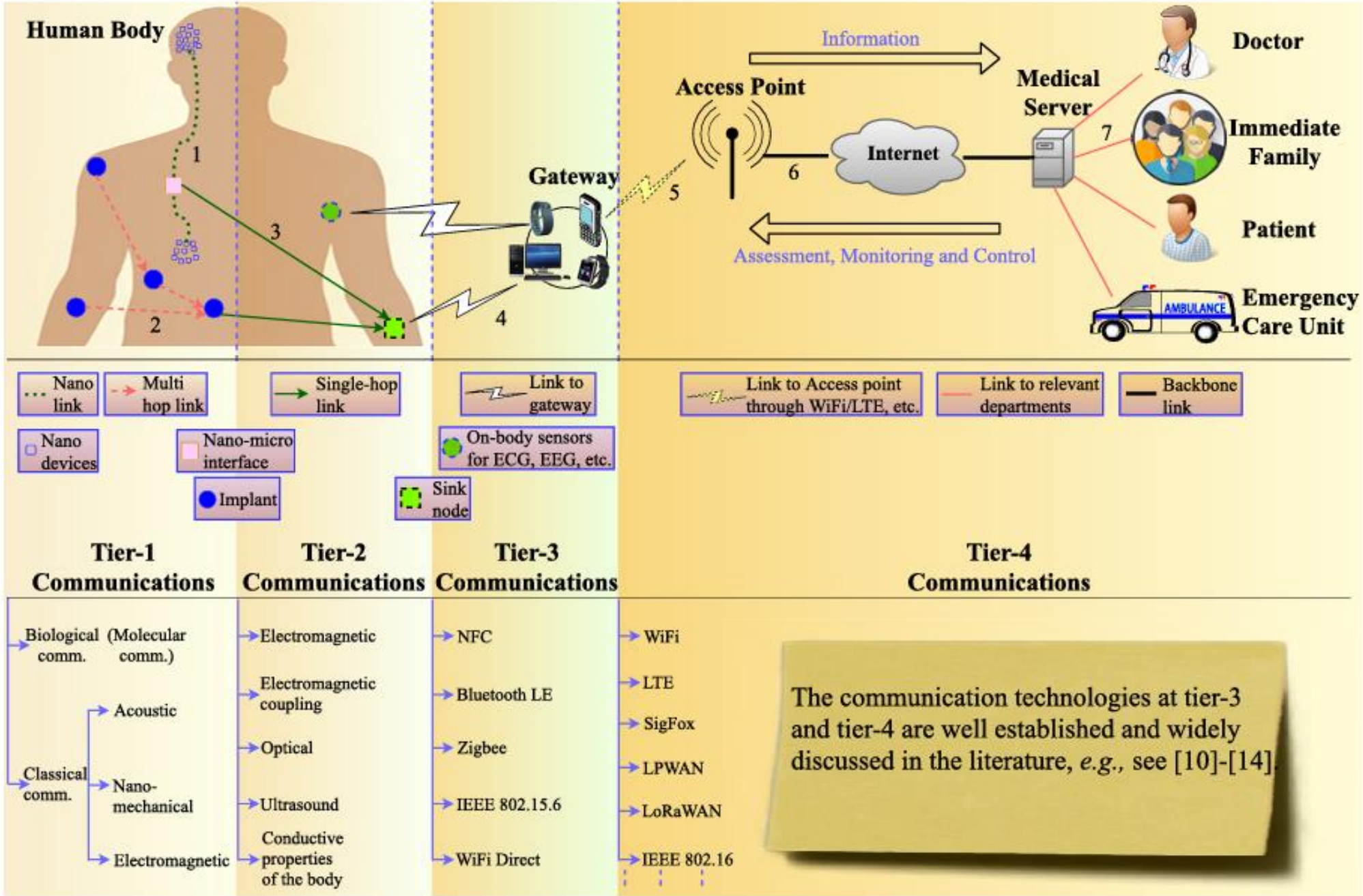
ABSTRACT Wireless body area networks (WBANs) play a vital role in shaping today's healthcare systems. Given the critical nature of a WBAN in one's health to automatically monitor and diagnose health issues, security and privacy of these healthcare systems need a special attention. In this paper, we first propose a novel four-tier architecture of remote health monitoring system and then identify the security requirements and challenges at each tier. We provide a concise survey of the literature aimed at improving the security and privacy of WBANs and then present a comprehensive overview of the problem. In particular, we stress that the inclusion of *in vivo* nano-networks in a remote healthcare monitoring system is imperative for its completeness. To this end, we elaborate on security threats and concerns in nano-networks and medical implants as well as we emphasize on presenting a holistic framework of an overall ecosystem for WBANs, which is essential to ensure end-to-end security. Lastly, we discuss some limitations of current WBANs.

- A. WBAN ARCHITECTURE
- In-body communications involve implants and nano-devices placed inside a human body. On-body communications involve the devices placed on the body such as wearables and other sensors for ECG, EEG, blood glucose, and blood pressure monitoring.
- Nano-devices: Nano-devices are one of the smallest entities in the healthcare ecosystem able to perform very basic functions at nano-scale, such as computing, data storage, sensing, actuation, and communications
- Nano-links: These are communication links between nano-devices and nano-micro interfaces.
- Nano-micro Interface: This interface connects nanodevices inside human body to a sink node, which finally connects them to off-body devices.
- Implant: This represents a medical device implanted inside human body for monitoring certain diseases, vital signs, or even biometric identification.
- Sink Node: Sink node acts like a data hub in WBANs that collects data from different in-body devices to relay it to the medical server and vice versa.

https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8481660

- On-body Sensors: This includes different sensors placed on the skin or inside clothes of a human body to measure and monitor different vital signs such as ECG, EEG, blood pressure, blood glucose, and blood oxygen level.
- Gateway: This represents a gateway device employed to connect the WBAN with the medical server. It can be a smartphone or any other device such as a computer or an Internet-of-Things (IoT) device that is directly connected to a base station using, e.g., 3G/4G.
- Access Point: This represents a cellular base station or a WiFi access point to route sensor's traffic to the medical server.
- Medical Server: This is a database, which stores all information of sensors for further actions and analysis of the data. It can include real-time monitoring of vital signs and virtual clinics wherein patients and physicians

https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8481660



https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8481660

> Comput Biol Med. 2021 Sep:136:104707. doi: 10.1016/j.compbiomed.2021.104707. Epub 2021 Jul 31.

Securing Bio-Cyber Interface for the Internet of Bio-Nano Things using Particle Swarm Optimization and Artificial Neural Networks based parameter profiling

Sidra Zafar [1], Mohsin Nazir [2], Aneeqa Sabah [3], Anca Delia Jurcut [4]

PMID: 34375900 DOI: 10.1016/j.compbiomed.2021.104707

Abstract

Internet of bio-nano things (IoBNT) is a novel communication paradigm where tiny, biocompatible and non-intrusive devices collect and sense biological signals from the environment and send them to data centers for processing through the internet. The concept of the IoBNT has stemmed from the combination of synthetic biology and nanotechnology tools which enable the fabrication of biological computing devices called Bio-nano things. Bio-nano things are nanoscale (1-100 nm) devices that are ideal for in vivo applications, where non-intrusive devices can reach hard-to-access areas of the human body (such as deep inside the tissue) to collect biological information. Bio-nano things work collaboratively in the form of a network called nanonetwork. The interconnection of the biological world and the cyber world of the Internet is made possible by a powerful hybrid device called Bio Cyber Interface. Bio Cyber Interface translates biochemical signals from in-body nanonetworks into electromagnetic signals and vice versa. Bio Cyber Interface can be designed using several technologies. In this paper, we have selected bio field-effect transistor (BioFET) technology, due to its characteristics of being fast, low-cost, and simple The main concern in this work is the security of IoBNT, which must be the preliminary requirement, especially for healthcare applications of IoBNT.

https://www.sciencedirect.com/science/article/abs/pii/S0010482521005011?via%3Dihub

Security of Wireless Body Area Networks for Healthcare Applications: Comparison between ETSI and IEEE Approaches

Publisher: IEEE Cite This PDF

Giacomo Borghini ; Stefano Caputo ; Lorenzo Mucchi ; Adnan Rashid ; Sara Jayousi ; Matti Hämäläinen All Authors

Abstract:

Wireless Body Area Network (WBAN) is vulnerable to various security threats including both active and passive attacks. It is important to implement effective security measures to mitigate these threats and ensure the security requirements of medical information transmitted over WBANs. In this paper, a comparison of the security features of different standards suitable for WBANs are presented. The various security protocols, made by different global standard organizations, such as the Institute of Electrical and Electronic Engineers (IEEE) and European Telecommunications Standards Institute (ETSI), for WBAN, are analyzed. Moreover, it also presented their current work in the context of WBAN security and what their future directions are.

Published in: 2023 IEEE 17th International Symposium on Medical Information and Communication Technology (ISMICT)

Date of Conference: 10-12 May 2023

DOI: 10.1109/ISMICT58261.2023.10152140

Date Added to IEEE *Xplore*: 20 June 2023

Publisher: IEEE

https://ieeexplore.ieee.org/document/10152140

1. NAME OF THE MEDICINAL PRODUCT

ENGERIX B 10 micrograms/0.5 ml
Suspension for injection
Hepatitis B recombinant vaccine, adsorbed

SUMMARY OF PRODUCT CHARACTERISTICS

5. PHARMACOLOGICAL PROPERTIES

5.1. Pharmacodynamic properties

ENGERIX B, hepatitis B vaccine is a sterile suspension containing the purified major surface antigen of the virus manufactured by recombinant DNA technology, adsorbed onto aluminium hydroxide.

The antigen is produced by culture of genetically-engineered yeast cells (Saccharomyces cerevisiae) which carry the gene which codes for the major surface antigen of the hepatitis B virus (HBV). This hepatitis B surface antigen (HBsAg) expressed in yeast cells is purified by several physico-chemical steps.

The HBsAg assembles spontaneously, in the absence of chemical treatment, into spherical particles of 20 nm in average diameter containing non-glycosylated HBsAg polypeptides and a lipid matrix consisting mainly of phospholipids. Extensive tests have demonstrated that these particles display the characteristic properties of natural HBsAg.

https://www.ema.europa.eu/en/documents/referral/engerix-b-article-30-referral-summary-product-characteristics_en.pdf

WIKIPEDIA
The Free Encyclopedia

Search Wikipedia | Search

Fractal antenna

10 langua

ıide

antennas

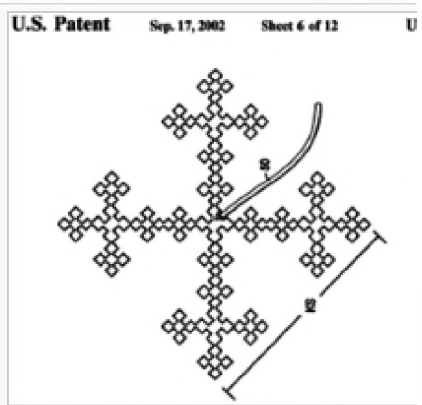
ariance and
ıations

Article Talk | Read Edit View history T

From Wikipedia, the free encyclopedia

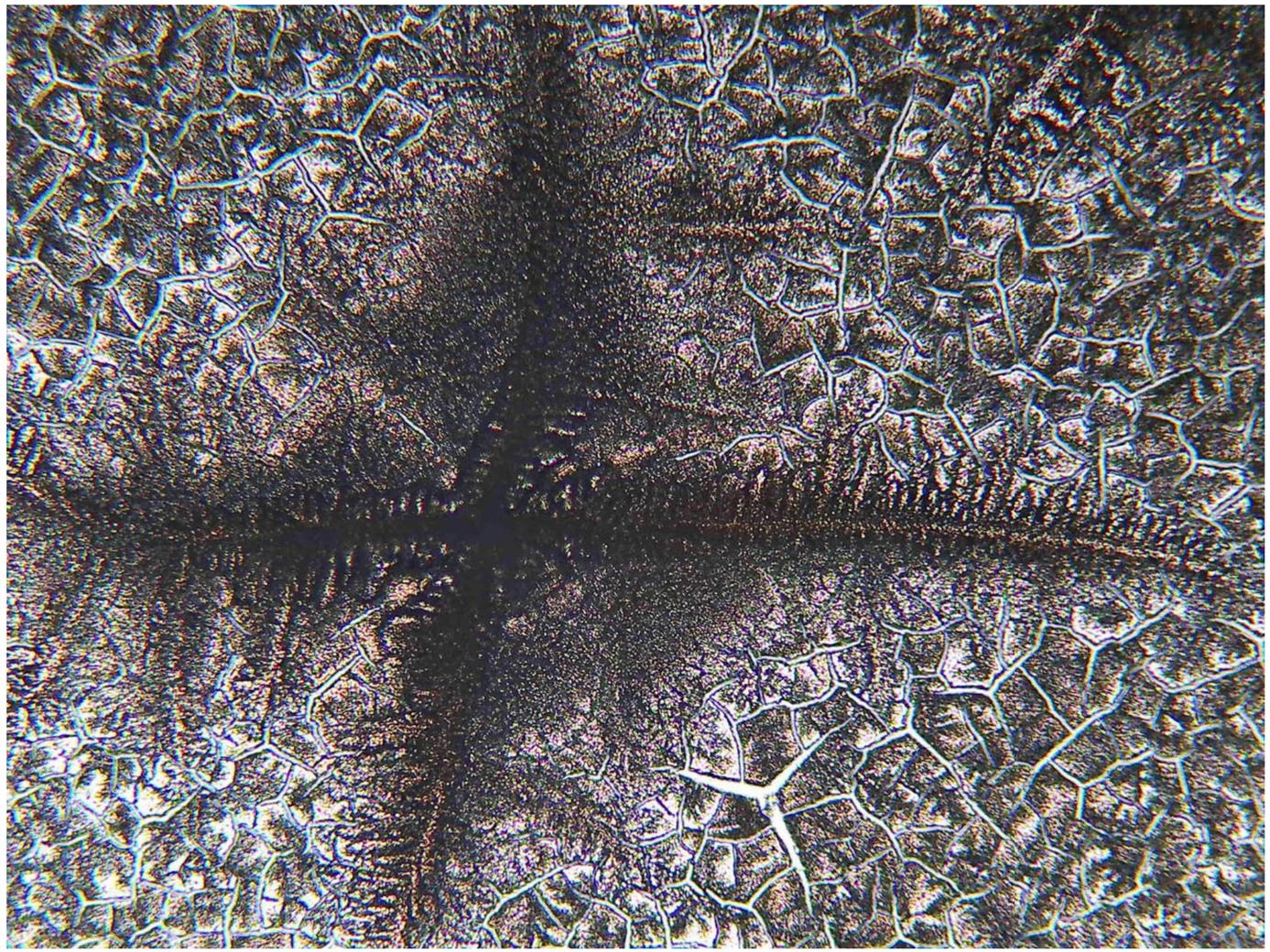
A **fractal antenna** is an antenna that uses a fractal, self-similar design to maximize the effective length, or increase the perimeter (on inside sections or the outer structure), of material that can receive or transmit electromagnetic radiation within a given total surface area or volume.

Such fractal antennas are also referred to as multilevel and space filling curves, but the key aspect lies in their repetition of a motif over two or more scale sizes,[3] or "iterations". For this reason, fractal antennas are very compact, multiband or wideband, and have useful applications in cellular telephone and microwave communications. A fractal antenna's response differs markedly from traditional antenna designs, in that it is capable of operating with good-to-excellent performance at many different frequencies simultaneously. Normally, standard antennas have to be "cut" for the frequency for which they are to be used—and thus the standard antennas only work well at that frequency.



An example of a fractal antenna: a space-filling curv called a "Minkowski Island"["Minkowski fractal"[2]

https://en.wikipedia.org/wiki/Fractal_antenna



1. NAME OF THE MEDICINAL PRODUCT

Gardasil 9 suspension for injection.
Gardasil 9 suspension for injection in a pre-filled syringe.
Human Papillomavirus 9-valent Vaccine (Recombinant, adsorbed)

2. QUALITATIVE AND QUANTITATIVE COMPOSITION

1 dose (0.5 ml) contains approximately:

Human Papillomavirus[1] Type 6 L1 protein[2,3]	30 micrograms
Human Papillomavirus[1] Type 11 L1 protein[2,3]	40 micrograms
Human Papillomavirus[1] Type 16 L1 protein[2,3]	60 micrograms
Human Papillomavirus[1] Type 18 L1 protein[2,3]	40 micrograms
Human Papillomavirus[1] Type 31 L1 protein[2,3]	20 micrograms
Human Papillomavirus[1] Type 33 L1 protein[2,3]	20 micrograms
Human Papillomavirus[1] Type 45 L1 protein[2,3]	20 micrograms
Human Papillomavirus[1] Type 52 L1 protein[2,3]	20 micrograms
Human Papillomavirus[1] Type 58 L1 protein[2,3]	20 micrograms

[1]Human Papillomavirus = HPV.
[2]L1 protein in the form of virus-like particles produced in yeast cells (*Saccharomyces cerevisiae* CANADE 3C-5 (Strain 1895)) by recombinant DNA technology.
[3]Adsorbed on amorphous aluminium hydroxyphosphate sulfate adjuvant (0.5 milligrams Al).

https://www.ema.europa.eu/en/documents/product-information/gardasil-9-epar-product-information_en.pdf

ITU Journal on Future and Evolving Technologies, Volume 5, Issue 2, June 2024

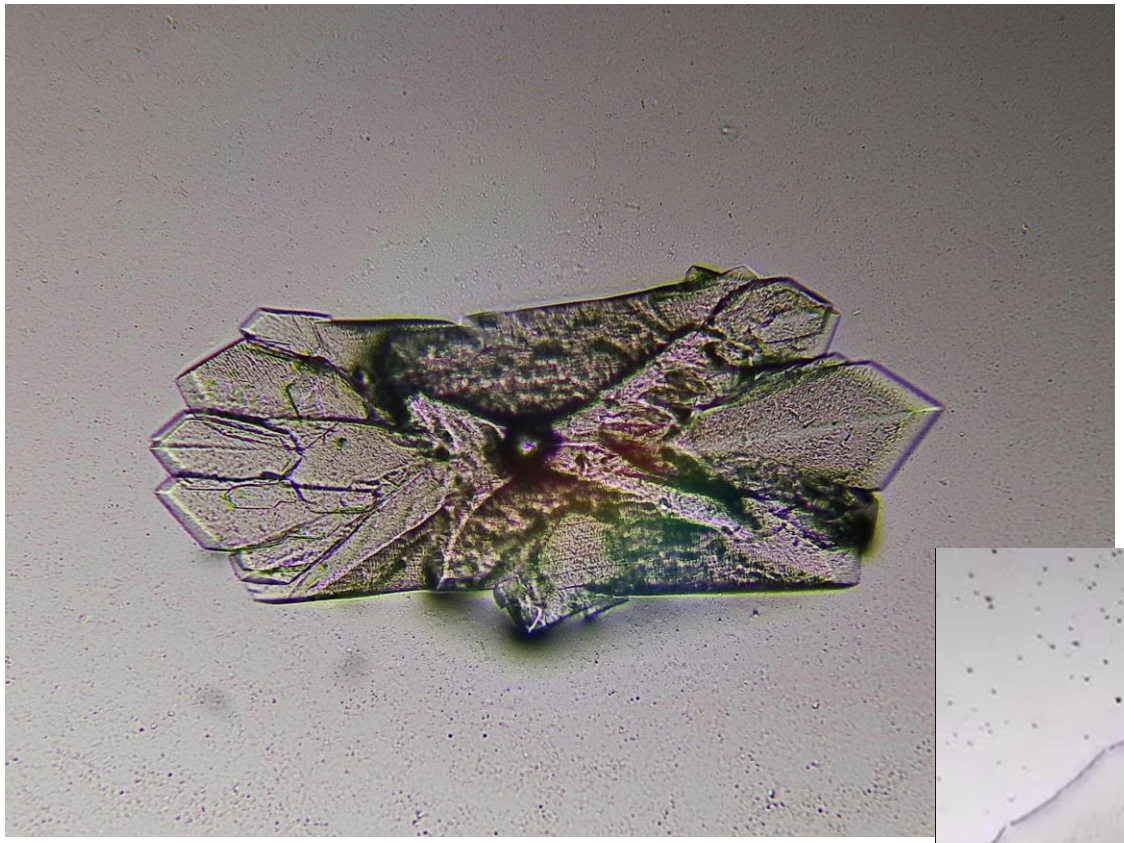
FUTURE SATELLITE COMMUNICATIONS: SATELLITE CONSTELLATIONS AND CONNECTIVITY FROM SPACE

Hazer Inaltekin[1], Mark Bowyer[2], Iain B. Collings[1], Gunes Karabulut Kurt[3], Walid Saad[4], Phil Whiting[1]
[1]Macquarie University, [2]Airbus UK, [3]Polytechnique Montreal, [4]Virginia Tech

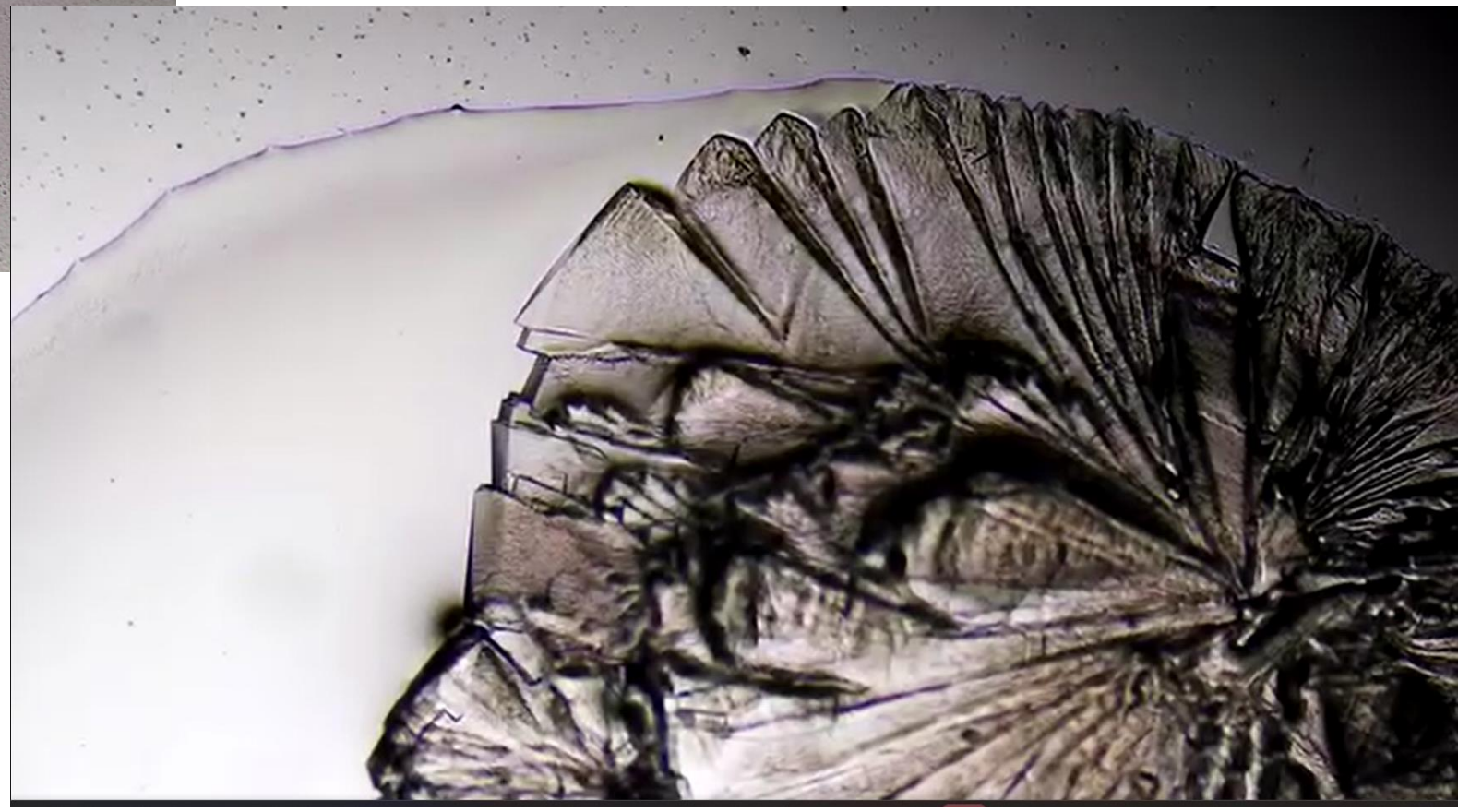
NOTE: Corresponding author: Hazer Inaltekin, hazer.inaltekin@mq.edu.au

Abstract – *Satellite communications is currently undergoing a massive growth, with a rapid expansion in Low Earth Orbit (LEO) networks, and a range of new satellite technologies. Until very recently, satellite communication systems and terrestrial 5/6G wireless networks have been complementary distinct entities. There is now the opportunity to bring these networks together and deliver an integrated global coverage multi-service network. Achieving this will require solving some key research challenges, and leveraging new technologies including high frequency phased-array antennas, onboard processing, dynamic beam hopping, physical layer signal processing algorithms, transmission waveforms, and adaptive inter-satellite links and routing. By integrating seamlessly with terrestrial 5/6G networks and low altitude flying access points, future satellite networks promise to deliver universal connectivity on a global scale, overcoming geographical limitations. In this special issue, we focus on the future of satellite communications, exploring topics ranging from beam hopping and design to space routing and THz satellite communications. Our aim is to shed light on the potential of these emerging technologies and their role in reshaping the landscape of global connectivity.*

https://www.itu.int/dms_pub/itu-s/opb/jnl/S-JNL-VOL5.ISSUE2-2024-A20-PDF-E.pdf



Crystallization model of Comirnaty Omicron and Moderna vaccine droplets



NEUROTECHNOLOGIES FOR BRAIN-MACHINE INTERFACING

https://standards.ieee.org/industry-connections/activities/neurotechnologies-for-brain-machine-interfacing/

About the Activity

The goal of this program is to bring together diverse stakeholders across neurotechnologies, research institutions, industry and government agencies to identify and address gaps in the existing standards for Brain-Machine Interfacing (BMI)/Brain Computer Interface (BCI) based solutions.

Next Steps

View the ICAID (PDF)

https://unesdoc.unesco.org/ark:/48223/pf0000383559

https://unesdoc.unesco.org/search/N-EXPLORE-90ec54c0-bf2d-4f15-a655-a71489709fa1

Roco, Mihail C. <mroco@nsf.gov> 8 ian. 2024, 18:08

către eu

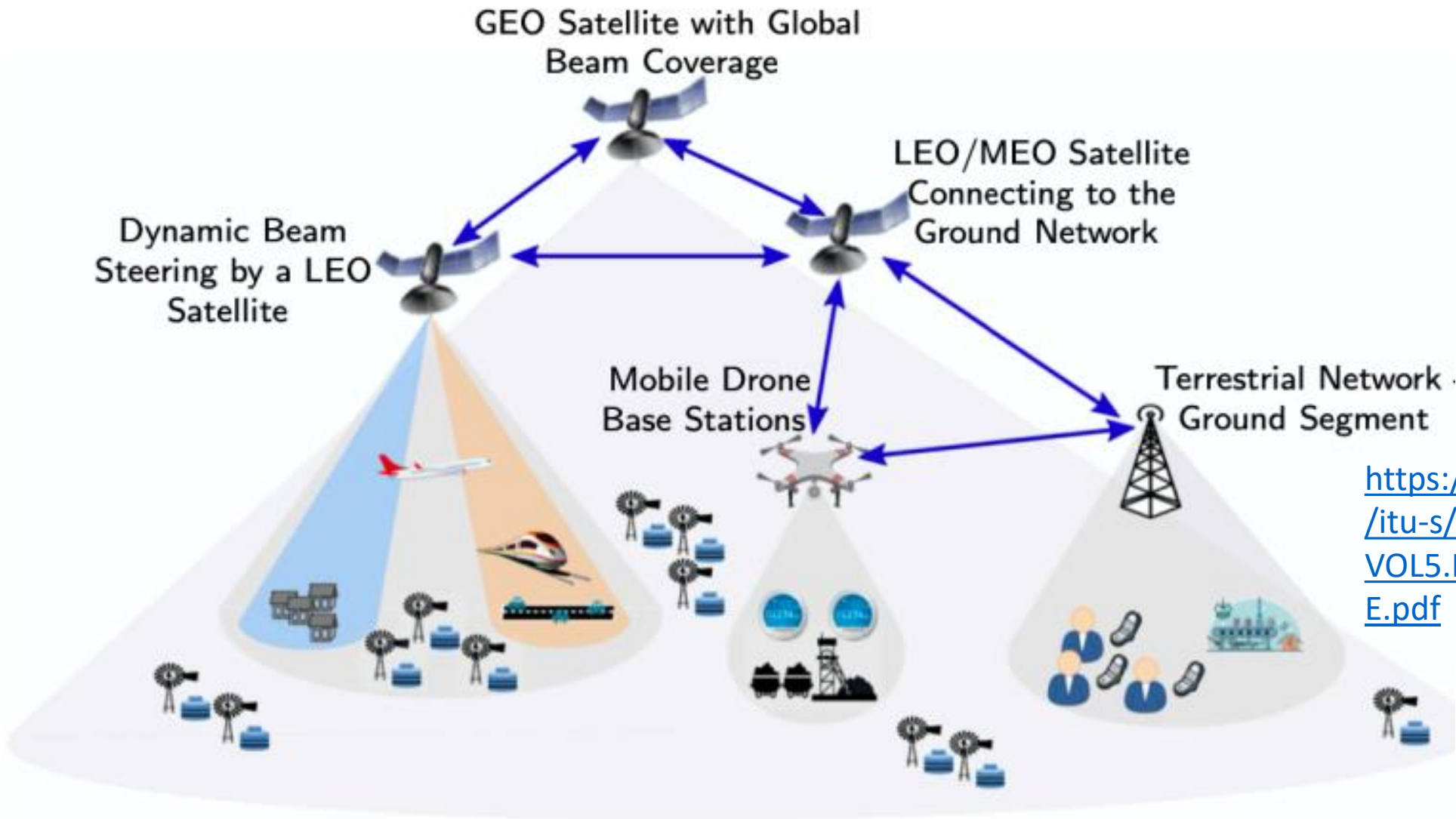
Dr. Geanina Hagimă,

I have received your e-mail with your comments and personal opinions on nanoscale science and engineering.

The National Nanotechnology Initiative is a science-based project and program where societal implications, including environmental and health effects, have been addressed from its beginning. All natural and man-made objects are built from atoms and molecules and have a nanostructure at the first level of organization of atoms. Nanostructure are encountered in every material object or organism, and by itself is not dangerous. Understanding and properly using nanoscale science and engineering makes the world better in a fundamental way. Combating possible misuses of nanotechnology must be addressed in each application. The general concerns must be addressed by researchers and manufacturers, and for specific product concerns it is the primarily responsibility of those making the new specific products to investigate. The regulatory framework is affected by political factors in each country and region. For example, the vaccine manufacturers must address the efficacy and safety of their products.

I am not involved directly in medical research applications and I am not able to address your suggestions. If there are concerns of governance of nanotechnology in Europe, please consider writing to the EU/EC or local industry.

Sincerely,
Mihail Roco
NSF



https://www.itu.int/dms_pub/itu-s/opb/jnl/S-JNL-VOL5.ISSUE2-2024-A20-PDF-E.pdf

Fig. 1 – A multi-layer space network integrated with terrestrial and low-altitude drone base stations.

ITU Journal on Future and Evolving Technologies, Volume 5, Issue 2, June 2024

A STUDY ON THz COMMUNICATIONS BETWEEN LOW EARTH ORBIT CONSTELLATIONS AND EARTH STATIONS

Estephania Flores Aguilar[1] and Gunes Karabulut-Kurt[1]
[1]Polytechnique Montréal, 2500 Chem. de Polytechnique, Montréal, QC H3T 1J4, Canada

NOTE: Corresponding author: Estephania Flores, estephania.flores-aguilar@polymtl.ca

Abstract – *A non-terrestrial system that uses Terahertz (THz) frequencies is a potential solution to achieving equal access to the Internet worldwide. This paper describes a non-terrestrial system that consists of a Low Earth Orbit (LEO) constellation, Earth Stations in Motion (ESIMs) and standard Earth stations. We examine the effects of rain, fog, clouds and atmospheric gases for this non-terrestrial system for frequencies between 100-300 GHz. The research findings suggest that the frequency bands between 102 - 109.5 GHz are rather suitable for communication between Earth stations and satellites, including ESIMs, reaching in a critical scenario uplink data rates of up to 2.6 Gbits/s with 0.5 GHz of bandwidth or up to 12 Gbits/s with 5 GHz of bandwidth in uplink. For the downlink, we can reach up to 6 Mbits/s with a transmitted power of 29 dBW, but if we increase the power transmitted by satellites, it is possible to reach up to 25 Gbits/s with 2.5GHz of bandwidth. Under clear, blue-sky conditions, we can achieve a maximum data rate of 17.3 Gbits/s for downlink and uplink. For inter-satellite links (communications between satellites in the same orbit or between different orbits), the frequency bands between 111.8 – 114.25 GHz, 116 – 123 GHz, 174.5 – 182 GHz, 185 – 190 GHz are viable, offering speeds from 1.5 to 2.51 Gbits/s when using a uniform rectangular array with 625 radiating elements. This research provides new findings from the amalgamation of existing literature, which is crucial for the future allocation of optimal frequencies between 100 - 300 GHz for satellite services.*

https://www.itu.int/dms_pub/itu-s/opb/jnl/S-JNL-VOL5.ISSUE2-2024-A19-PDF-E.pdf ,
https://www.itu.int/en/journal/j-fet/Pages/default.aspx

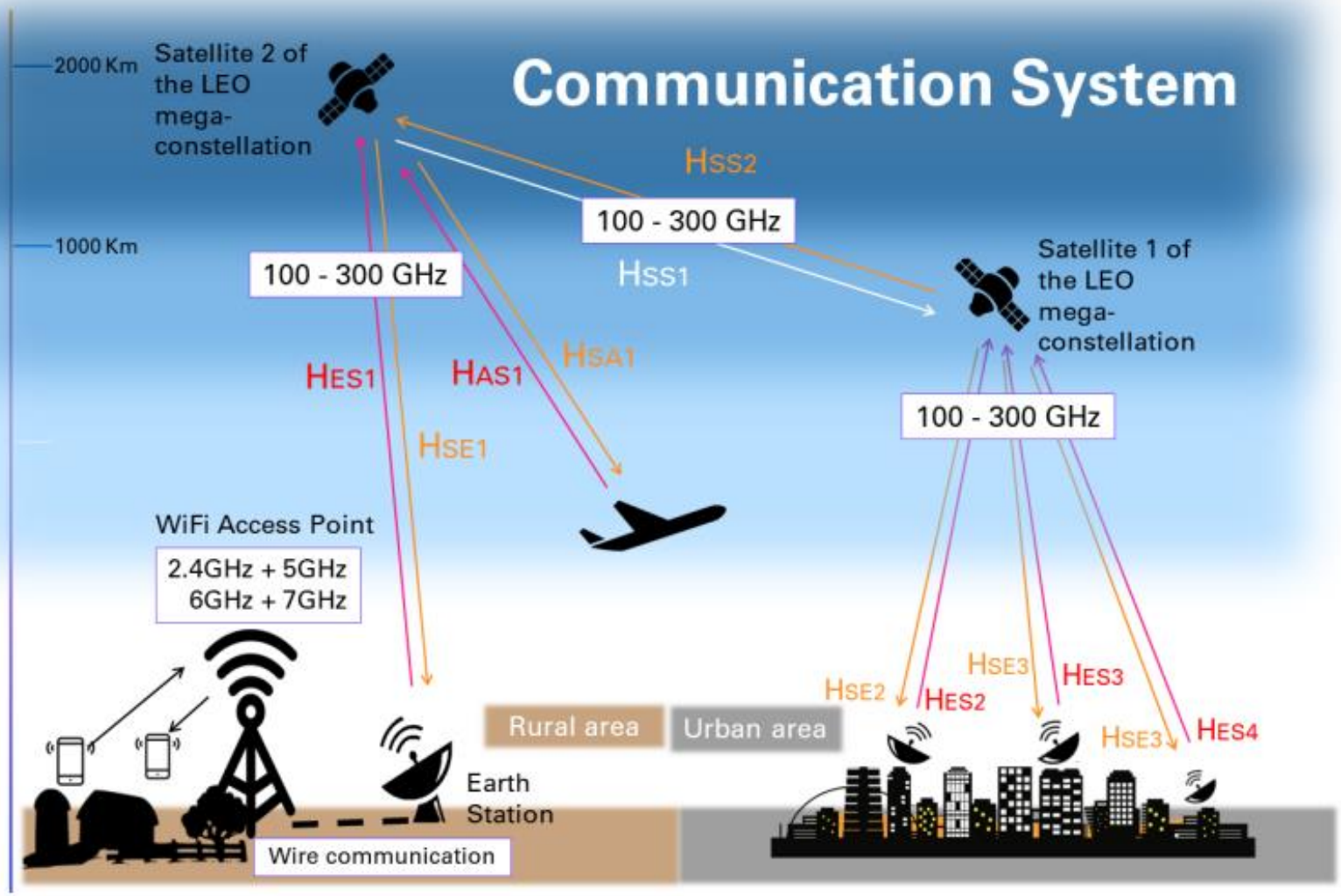


Fig. 1 – An overview of the considered communication system

A STUDY ON THz COMMUNICATIONS BETWEEN LOW EARTH ORBIT CONSTELLATIONS AND EARTH STATIONS

https://www.itu.int/dms_pub/itu-s/opb/jnl/S-JNL-VOL5.ISSUE2-2024-A19-PDF-E.pdf ,
https://www.itu.int/en/journal/j-fet/Pages/default.aspx

Our Common Agenda
Policy Brief 7

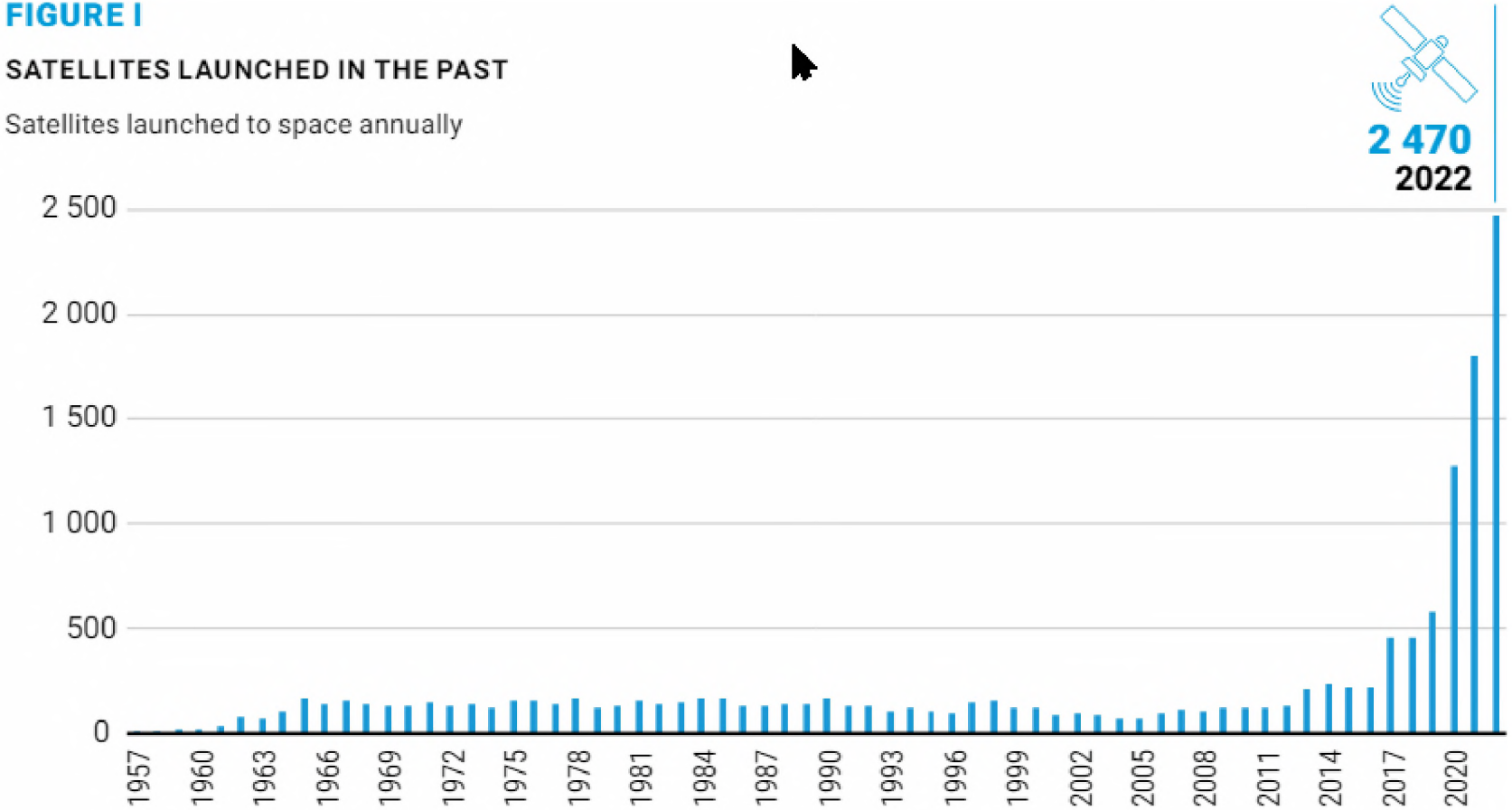
For All Humanity – the Future of Outer Space Governance

MAY 2023

FIGURE I

SATELLITES LAUNCHED IN THE PAST

Satellites launched to space annually



https://www.un.org/sites/un2.un.org/files/our-common-agenda-policy-brief-outer-space-en.pdf

Our Common Agenda
Policy Brief 7

For All Humanity – the Future of Outer Space Governance

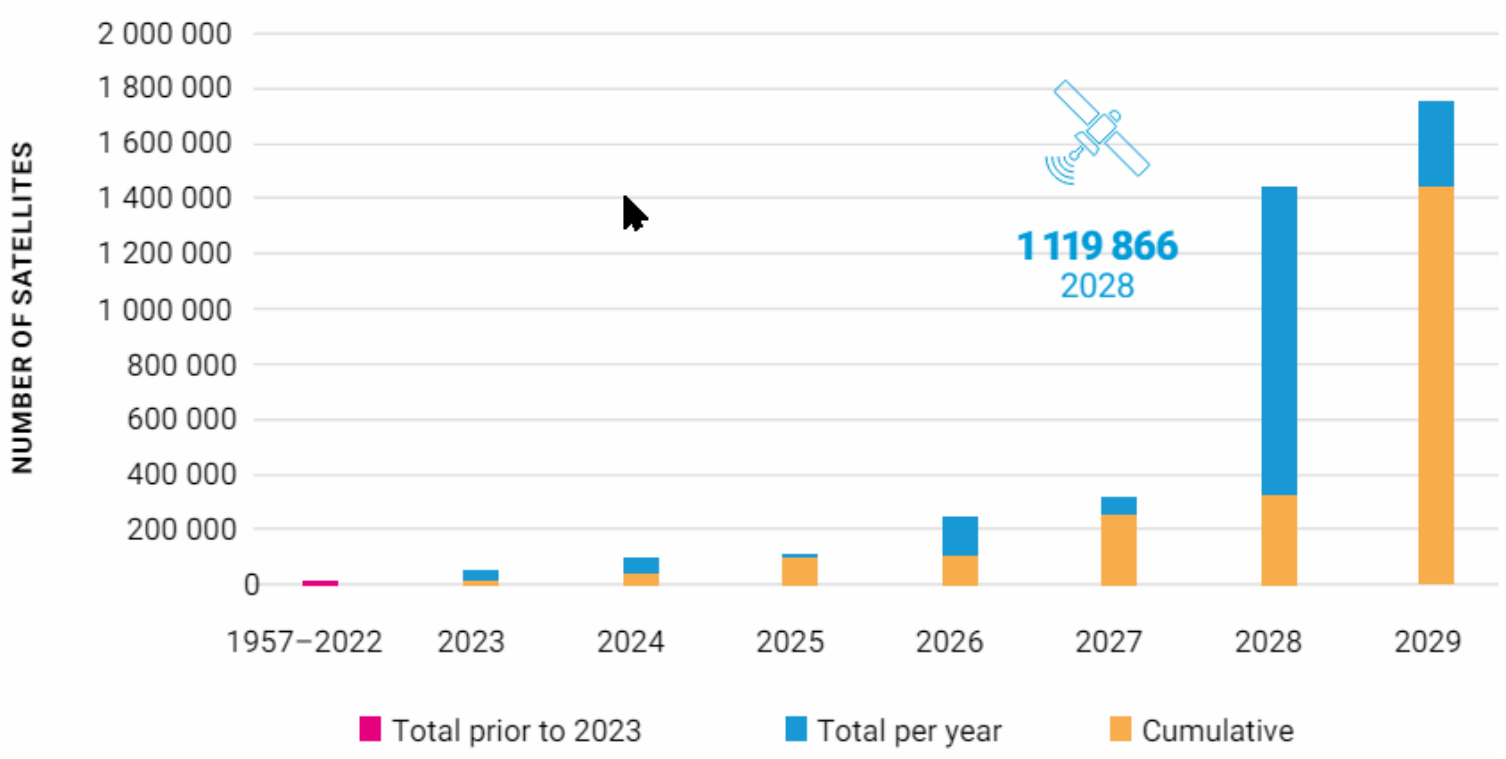
MAY 2023

https://www.un.org/sites/un2.un.org/files/our-common-agenda-policy-brief-outer-space-en.pdf

SATELLITES REGISTERED TO LAUNCH IN THE FUTURE

Number of non-geostationary satellites for which states have registered radio frequecies with the International Telecommunication Union (by year and cummulative)

For past launches, see figure I.



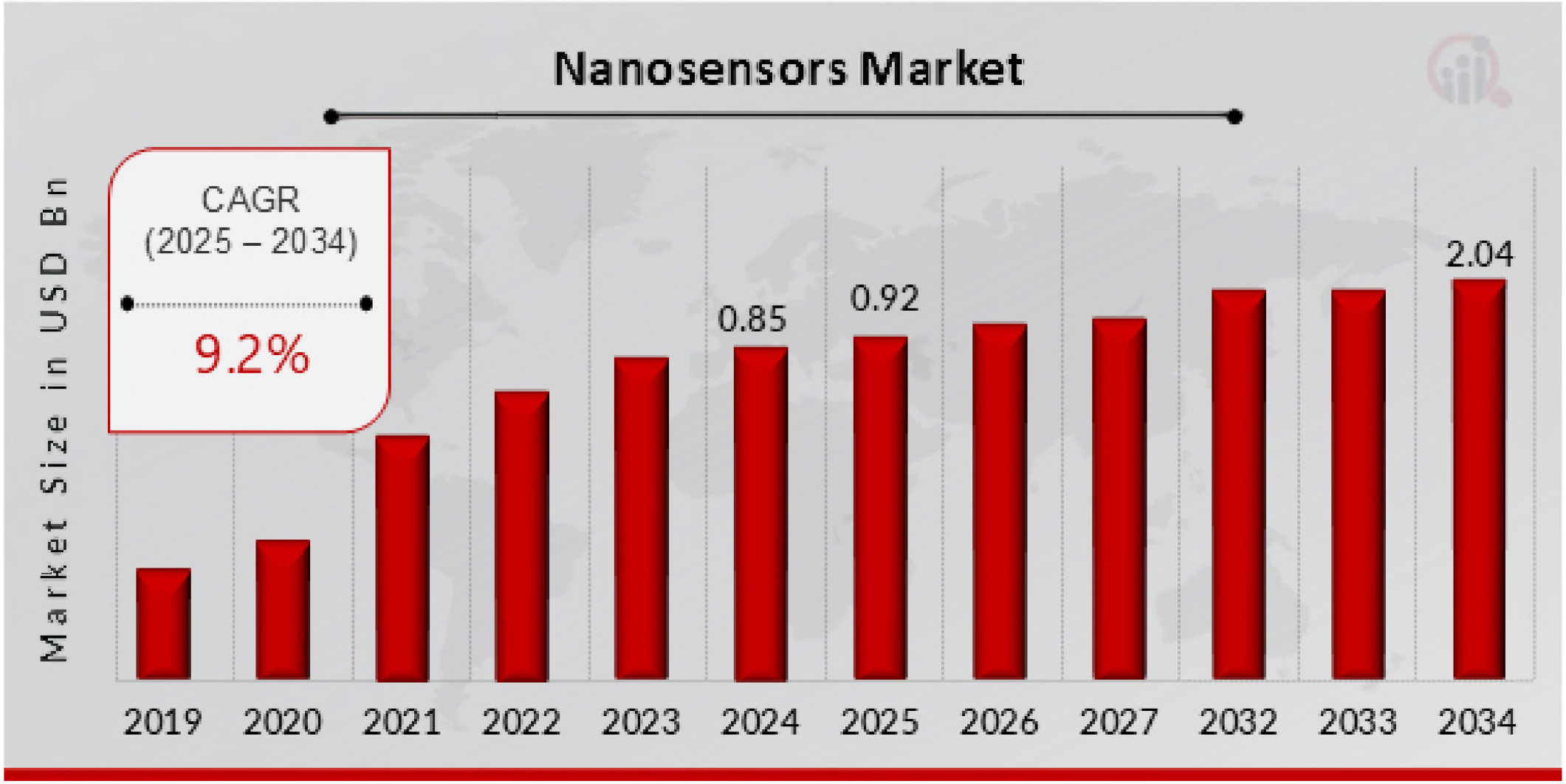
Global Body Area Network Market Outlook (2022 to 2032)

The **global body area network market** is predicted to grow at a robust **CAGR of 22.3%**. It is estimated to be valued at about **US$ 229.8 Bn** by 2032, going up from **US$ 24.6 Bn** in 2021.

Attributes	Details
Body Area Network Market Size (2021)	US$ 24.6 Bn
Body Area Network Market Value (2022)	US$ 30.8 Bn
Body Area Network Market Value (2032)	US$ 229.8 Bn
Body Area Network Market Growth Rate (2022 to 2032)	22.3%
Market Share of Top 5	68.6%

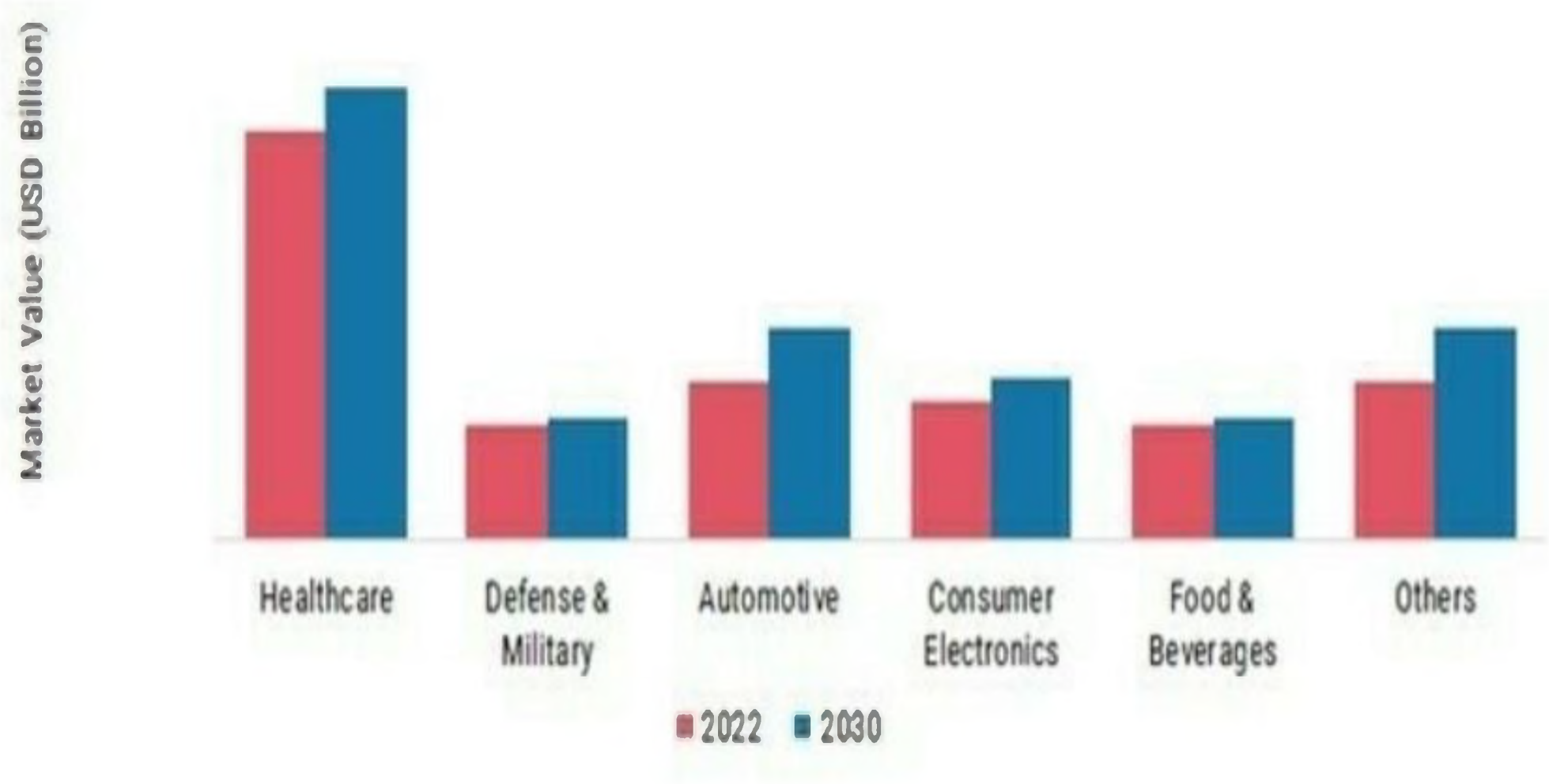
https://www.factmr.com/report/body-area-network-market

https://dataintelo.com/report/global-wireless-body-area-network-market



https://www.marketresearchfuture.com/reports/nanosensors-market-1117

Figura 2: Piața globală a senzorilor NANO, după aplicație, 2022 și 2030 (miliard USD)



https://www.marketresearchfuture.com/reports/nanosensors-market-1117

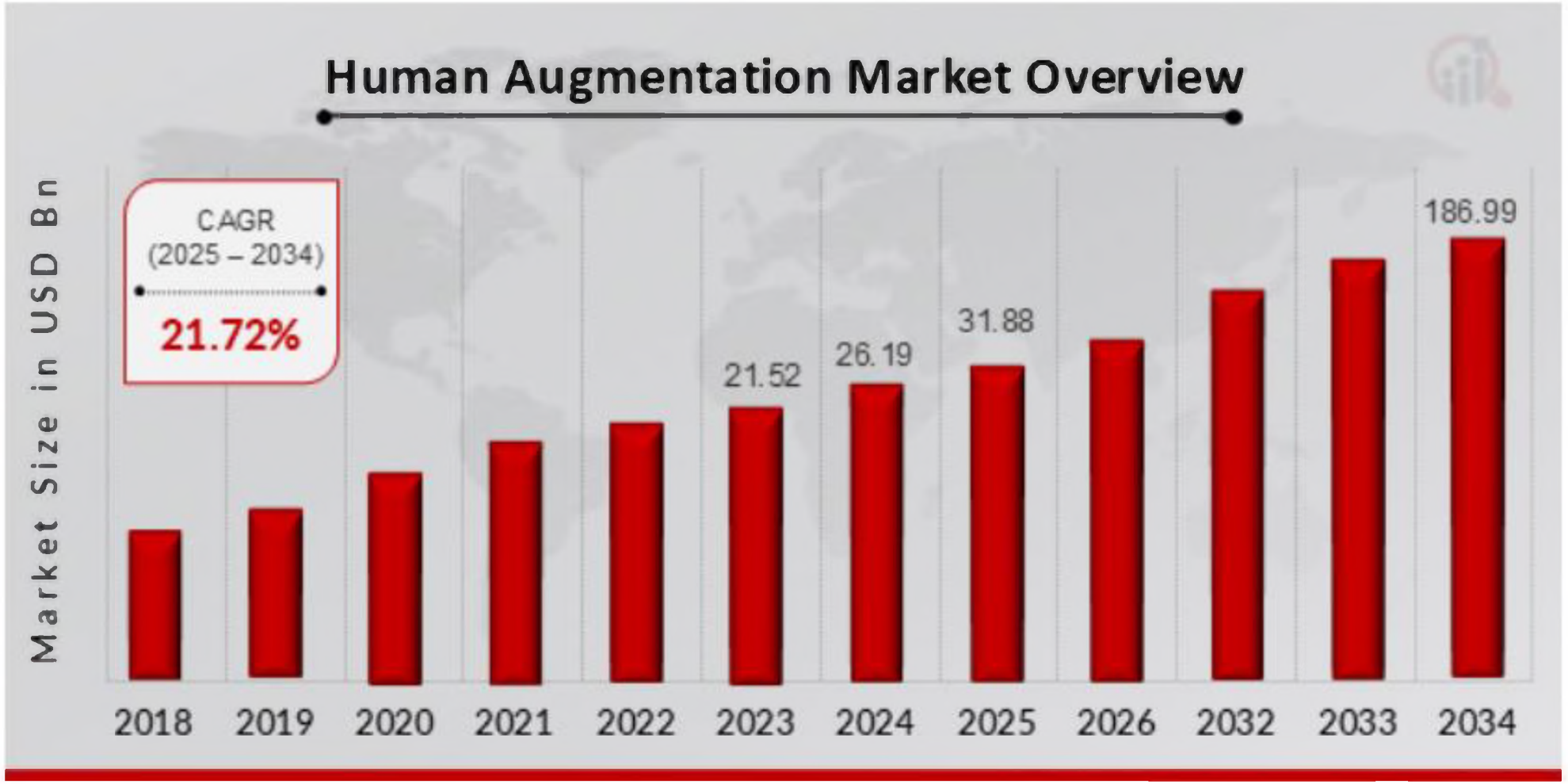
Human Augmentation Market Overview

Human Augmentation Market is projected to grow from **USD 31.88 billion** in 2025 to **USD 186.99 billion** by 2034, exhibiting a compound annual growth rate **(CAGR) of 21.72%** during the forecast period (2025 - 2034). Additionally, the market size for Human Augmentation Market was valued at USD 26.19 billion in 2024.

The increasing adoption of wearable devices in the fitness sector and the growing demand for human augmentation technologies are the key market drivers enhancing market growth.

https://www.marketresearchfuture.com/reports/human-augmentation-market-5043

Figure 1: Human Augmentation Market Size, 2025-2034 (USD Billion)



https://www.marketresearchfuture.com/reports/human-augmentation-market-5043

UNITED NATIONS
INDUSTRIAL DEVELOPMENT ORGANIZATION

SUSTAINABLE DEVELOPMENT GOALS

STANDARDS & DIGITAL TRANSFORMATION

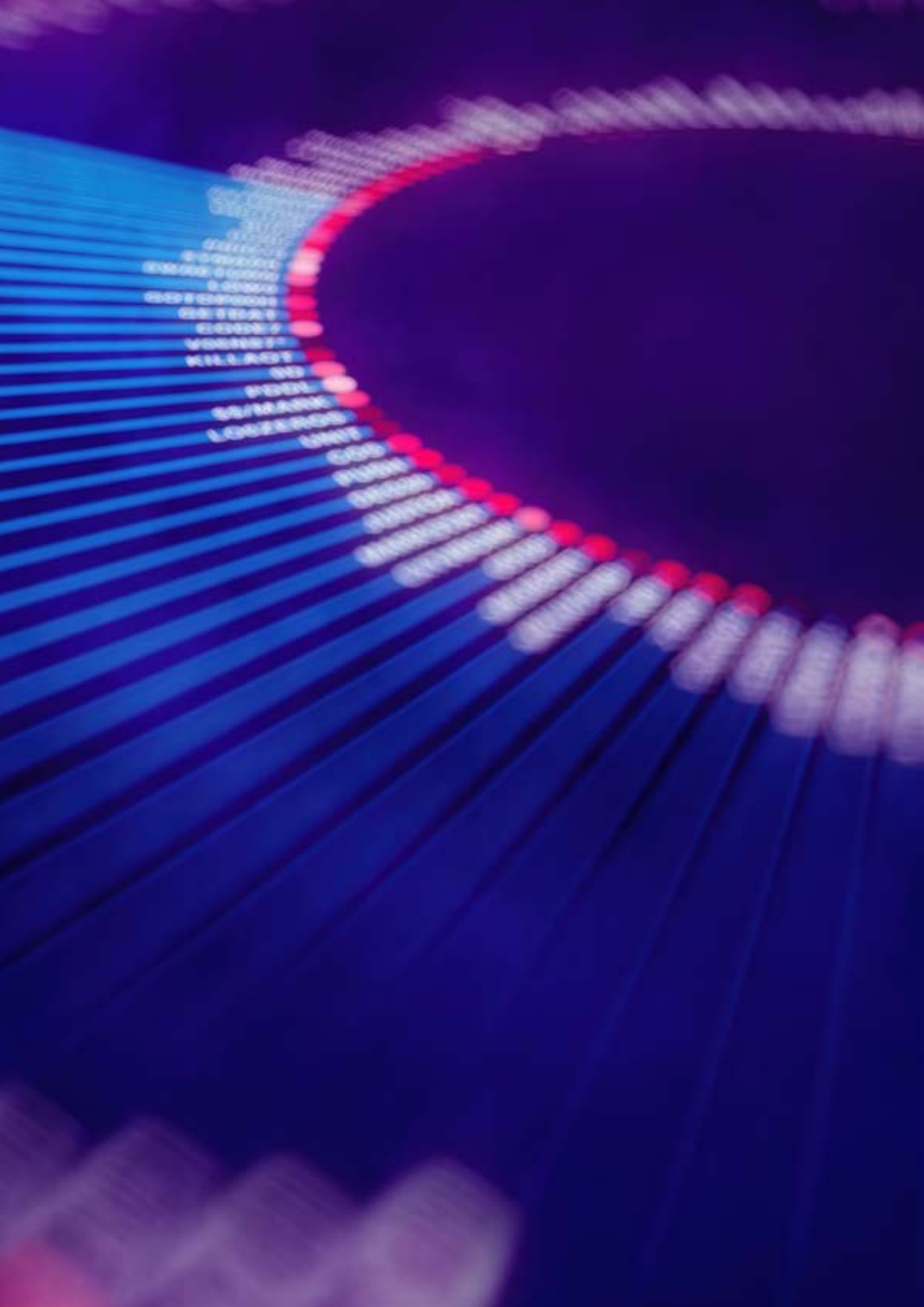
GOOD GOVERNANCE IN A DIGITAL AGE

UNITED NATIONS
INDUSTRIAL DEVELOPMENT ORGANIZATION

STANDARDS & DIGITAL TRANSFORMATION

GOOD GOVERNANCE IN A DIGITAL AGE

Table of Contents



ACKNOWLEDGEMENTS

This publication has been prepared by the United Nations Industrial Development Organization (UNIDO) under the overall guidance of Mr. Bernardo Calzadilla-Sarmiento, Managing Director of the Directorate of Digitalization, Technology and Agri-Business. Technical inputs were coordinated by Ms. Dorina Nati, Industrial Development Expert, UNIDO. The publication is based on the work of Ms. Ruth Hillary and Ms. Sandra Camargo, with important comments received by Mr. Glenn Bosmans. We acknowledge the valuable contribution and support of several members of the UNIDO core team: Mr. Marco Kamiya, Mr. Alejandro Rivera Rojas, Mr. Juan Pablo Davila, Mr. Cong Wu, Mr. Darren Gleeson, Ms. Rebeca Gallardo Gomez, Mr. Nora Dei-Anang, Mr. Xiao Su and Mr. Jinfeng Mu.

This publication was edited by Ms. Brigitt Roveti. Design and layout was developed by Ms. Radhika Nathwani.

DISCLAIMER

Foreword

Standards have an essential role in the digital transformation process, offering numerous benefits and opportunities for digital technologies to shape the future for the better. They can provide global, transnational, multidisciplinary and potentially rapid solutions to current and future technological and societal challenges derived from digital technologies as they set minimum requirements in terms of safety, security, reliability, efficiency, interoperability and trust.

For over 50 years, the United Nations Industrial Development Organization (UNIDO), the specialized United Nations agency mandated to promote inclusive and sustainable industrial development has supported the establishment and upgrading of standards and conformity assessment structures worldwide.

Developing economies can compete on global markets and participate in international value chains when they can demonstrate compliance with quality requirements and trade rules. With existing commercial opportunities, UNIDO is applying its expertise to support its developing member states to address these issues. It does this by working with governments to establish a Quality Infrastructure system, which covers the essential aspects of policy, institutions, service providers, and the value-added use of international standards and conformity assessment procedures.

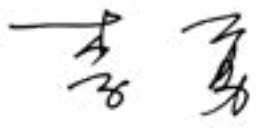
UNIDO is a strong proponent of the use of standards to support the achievement of the United Nations 2030 Agenda for Sustainable Development and Sustainable Development Goals (SDGs) through the enhancement of prosperity and the well-being of people, and for the preservation of the planet. To this end, UNIDO engages in all stages of the standardization process, from advocacy and pre-standardization; standardization; dissemination and implementation; to outreach and global partnerships.

Quality Infrastructure, and standards in particular will grow in importance and prominence as the global community continues to mobilize resources and efforts to respond to the Decade of Action that calls for the acceleration of sustainable solutions to address global social, economic and environmental challenges.

The ongoing digital transformation is being molded to support the three pillars of sustainability—people, planet and prosperity—in line with the SDGs for the benefit of society. The digitalization process provides possibilities to overcome the spatial and social barriers as digital technologies enables new inclusive and sustainable production methods and business models.

With inclusion and sustainability in mind, this publication serves to provide an overview of the digital transformation and the role of standards in digital transformation governance. It also calls the standard-setting community to act to help leverage the opportunities offered by digital technologies to contribute to the Decade of Action towards the achievement of the 2030 Agenda for Sustainable Development.

UNIDO is fully committed to doing its part to support standardization for digital technologies and continue its engagement with developing countries to achieve sustainability and prosperity for all.



LI Yong, UNIDO Director General

List of Abbreviations

4IR	Fourth Industrial Revolution
ADP	Advanced Digital Production
AI	Artificial Intelligence
AM	Additive Manufacturing
AMT	Additive Manufacturing Technology
ARSO	African Organisation for Standardisation
ASTM	American Society for Testing and Materials
CAA	Civil Aviation Authorities
CAD	Computer-aided Design
CEN	European Committee for Standardization
CENELEC	European Committee for Electrotechnical Standardization
CO_2	Carbon dioxide
COPANT	The Pan American Standards Commission
DLT	Distributed Ledger Technology
ETSI	European Telecommunications Standards Institute
EU	European Union
EUOS	European Union Observatory for ICT Standardisation
GDPR	General Data Protection Regulation
GPS	Global Positioning System
GQSP	Global Quality and Standards Programme
HMI	Human–machine Interface
IoT	Internet of Things
IIOT	Industrial Internet of Things
ICT	Information and Communication Technology
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
IIC	Industrial Internet Consortium
IP	Intellectual Property
IPR	Intellectual Property Rights
ISO	International Organization for Standardization
ITU	International Telecommunication Union

JC	Joint Committee
JTC	Joint Technical Committee
ML	Machine Learning
NGO	Non-governmental Organization
NGGP	Namib Green Gold Processing (Pty) Ltd
NIST	National Institute of Standards and Technology
NSB	National Standards Body
NSO	National Standards Organization
OECD	Organization for Economic Cooperation and Development
OEE	Overall Equipment Effectiveness
PII	Personally Identifiable Information
PSDO	Partner Standards Development Organisation
QA	Quality Assurance
QI	Quality Infrastructure
QP	Quality Policy
QMS	Quality Management System
SA	Standards Association
SASAM	Support Action for Standardisation in Additive Manufacturing
SC	Sub Committee
SDGs	Sustainable Development Goals
SDO	Standards Development Organization
SSO	Standard Setting Organization
STEM	Science, technology, engineering and mathematics
TIPPSS	Trust, Identity, Privacy, Protection, Safety, Security
UAS	Unmanned Aircraft System
UAV	Unmanned Autonomous Vehicle
UN	United Nations
UNIDO	United Nations Industrial Development Organization
WEF	World Economic Forum
WHO	World Health Organization
WSN	Wireless Sensor Networks

Executive Summary

We are in the era of the Fourth Industrial Revolution (4IR), which is characterized by the convergence and complementarity of emerging technology domains, including nanotechnology, biotechnology, new materials and advanced digital production technologies. Despite the challenges posed by the disruptive nature of these innovations—which are increasingly connecting objects, machines, people and the environment—the digital transformation presents opportunities for inclusive and sustainable development.

This publication describes the digital transformation process and provides insights into its key drivers and the implications for sustainable development, particularly for the five dimensions addressed by the Sustainable Development Goals (SDGs)—people, prosperity, planet, peace (governance) and partnerships.

While revolutions and change have marked human development, what distinguishes the 4IR from previous industrial revolutions is the parallel technological breakthroughs within and across the digital, biological and physical spheres. The complexity and rapid pace of change of the 4IR also make the revolution distinctive. Moreover, the COVID-19 pandemic has been an unanticipated accelerator to the pace of change and structural shift towards the 4IR and the adoption of new technologies.

The SDGs sit at the heart of the 2030 Agenda for Sustainable Development and guide global, regional and national development endeavours until 2030. Their achievement will be significantly impacted by the rapid change brought about by digital transformation to production, the economy, the environment and society. The digital transformation is in full swing and although little mention is made to it or digital technologies in the 2030 Agenda,, it has the potential to be shaped to promote sustainability for the benefit of all parts of society.

Standards can play a crucial role in shaping the digital transformation process, offering benefits and opportunities for digital technologies, complementing regulations and contributing to digital transformation governance. In the context of digital transformation, the timely and harmonized adoption of standards can promote interoperability, productivity and innovation, and ensure the successful scale-up of solutions to be implemented globally.

Digital technologies and the new business models of digital transformation do not fit easily into the traditional regulatory framework regulators use to intervene in markets. Former modes of governance, which are largely reactive in nature, will prove to be ineffective in the era of advanced digital transformation. Governance rules and regulatory approaches for new technology and processes of innovation need to be more agile, flexible and resilient.

Even though the world has witnessed a rise of standard-setting activities related to digital technologies in recent years, it still falls short to meet the needs of producers, consumers and regulators and remains fragmentally concentrated at the national level, leaving room for international exploitation and harmonization.

A comprehensive review of the international landscape was undertaken for seven of the most-trending digital technologies of the 4IR, namely artificial intelligence and big data, blockchain/distributed ledger technology, Internet of Things, robotics, 3D printing and unmanned aircraft systems. While standardization reflects the different features and scope of impacts of 4IR technologies, this publication identifies the essential criteria to consider when developing standards for digital transformation worldwide.

The rapid and extensive adoption of digital technologies and their far-reaching pervasive impact on people, their prosperity and the planet also suggest a core set of distinct principles is needed to guide standards developed for digital transformation governance. These principles include trustworthiness, inclusiveness, sustainability, interoperability, safety and security, data privacy, and international collaboration.

In addition to these principles, unlocking the potential of standards to contribute to digital transformation governance requires standards developers to consider, inter alia, strategic planning, objectivity, creditability and transparency in their work. As this decade is critical for the planet and its people, this publication is a call to action to all stakeholders in the development of regulations and standards to consider the outlined principles in their work in order to leverage the opportunities offered by digital technologies and thereby contribute to sustainable development for the benefit of all people and the planet.

PART 1: **CONTEXT**

INTRODUCTION

The world is in the midst of the Fourth Industrial Revolution (4IR) powered by digital technologies that are transforming society, economies and the environment. These digital technologies are being integrated into all organizational areas, fundamentally changing how organizations operate and deliver value to customers or stakeholders—a process referred to as digital transformation. Increasingly connecting objects, machines, people and the environment, the disruptive nature of the technological innovations shaping the digital transformation makes it difficult to plan for and anticipate the future.[1] What is clear is that the seismic shift that the digital transformation brings has major implications for sustainable development.

Timely and harmonized standards can play a pivotal role in shaping the digital transformation process, complementing regulations and contributing to digital transformation governance. Standards can facilitate the ongoing digitalization of industry by promoting compatibility and interoperability between products and processes, while guaranteeing minimum levels of quality and safety. Furthermore, standards can serve as accelerators of change as they promote innovation and the uptake and quality of new digital technologies.

This publication describes digital transformation, its key drivers and the implications for three of the Sustainable Development Goal (SDG) pillars—people, prosperity and planet. It also highlights the role of standards in digital transformation governance (peace) as well as the importance of global collaboration (partnerships). A comprehensive review of the international standards landscape was undertaken for seven of the most-trending digital technologies of the 4IR, namely: artificial intelligence (AI) and big data, blockchain/distributed ledger technology (DLT), Internet of Things (IoT), robotics, 3D printing, and unmanned aircraft systems (UAS). While standardization reflects the different features and scope of impacts of 4IR technologies, this publication identifies the essential criteria to consider when developing standards for digital transformation worldwide. Based on the review, further consideration is given to what good governance principles are necessary for guiding the development of standards in the digital technology landscape to ensure that the technologies are human-centered and aligned to the goals of sustainability.

> Sustainable development seeks to meet the needs and aspirations of the present without compromising the ability to meet those of the future. Far from requiring the cessation of economic growth, it recognizes that the problems of poverty and underdevelopment cannot be solved unless we have a new era of growth in which developing countries play a large role and reap large benefits.

[1] The Enterprise Project 2021

CHANGING WORLD – THE FOURTH INDUSTRIAL REVOLUTION

Revolutions and change have marked human development. Agricultural societies were transformed by steam power in the first industrial revolution, beginning the movement of people from rural to urban settings. Steel, chemicals and electricity helped fuel mass production and accelerated urbanization in the second industrial revolution during the late 19th and early 20th centuries. Information technology saw the rise of the third industrial revolution in the latter half of the 20th century, characterized by digital electronics, computers, telecommunication and the Internet.

What distinguishes the Fourth Industrial Revolution (4IR) from previous industrial revolutions is the parallel technological breakthroughs within and across the digital, biological and physical spheres, with the process of convergence deepening as technologies continue to evolve. As highlighted by the World Economic Forum, "the unlimited possibilities presented by billions of people being connected by mobile devices will be multiplied by emerging technological breakthroughs in fields such as artificial intelligence, robotics, the Internet of Things, autonomous vehicles, 3-D printing, nanotechnology, biotechnology, materials science, energy storage, and quantum computing."

The complexity and exponential pace of change of the 4IR also make the revolution unique compared to previous industrial revolutions. Moreover, the COVID-19 pandemic has acted as an unanticipated accelerator to the pace of change and structural shift towards the 4IR and the adoption of new technologies.

The 4IR is still being shaped. The digital technologies[2] that sit at its heart will irrevocably transform systems and, consequently, how people live, work and play, therefore, societies need to understand both the rewards and risks of the 4IR as technological advancement occurs every day. It is essential to ensure the new technologies in the digital, biological and physical worlds remain human-centered and serve society and the planet as a whole for the prosperity of all. A new concept bounding the 4IR is Society 5.0, i.e. a people-oriented society that balances economic advancement with resolving social problems by a system that highly integrates cyberspace and physical space.[3] In Society 5.0, it is foreseen that "innovation will create new value that bypasses regional, age, gender, and language gaps and provides products and services finely tailored to diverse individual needs, some not yet known. Society can thus promote economic development and solve social problems."[4]

UNIDO's Investment and Technology Promotion Network expert panel on "Exploring the Future of Manufacturing and Industries: Industry 4.0's Potential in Advancing the Attainment of the SDGs and Shaping Society 5.0" shed further light on this topic. The panel discussion was part of the GMIS Digital Series of online webinar discussions on the 4IR, foreshadowing the GMIS 2020 Virtual Summit held in September 2021.

As previously referenced, the United Nations Sustainable Development Goals (SDGs) sit at the center of the 2030 Agenda for Sustainable Development and guide global, regional and national development endeavours until 2030. The 17 SDGs and 169 targets serve as an opportunity to tackle many of today's most pressing world issues. They are universal, integrated and indivisible, and seek to balance the economic, social and environmental dimensions of sustainable development. Subsequently, as the 4IR continues to reshape the world, alignment with the SDGs is fundamental to ensure that benefits accrue for people, delivering them prosperity, and that the planet is protected.

[2] Terms found in the literature and used for digital technology include: new technology, 4IR technology, frontier technology, emerging technology, disruptive technology, future technology and transformational technology. This publication makes use of these terms inter-changeably.

[3] https://www8.cao.go.jp/cstp/english/society5_0/index.html

[4] Nature-like and Convergent Technologies Driving the Fourth Industrial Revolution, UNIDO, 2019

IMPLICATIONS FOR SUSTAINABLE DEVELOPMENT

The 4IR is in full swing and already has global implications for sustainable development. Enormous opportunities arise from the new and transformational technologies as they enable new modes of production, new businesses and societal models and new behaviours that can disrupt established and fundamental paradigms. **Strong global partnerships (Goal 17) between multiple stakeholders are needed to ensure sustainability is incorporated into digital technologies and the 4IR.**

The examples that follow provide a general context of the potential the 4IR has to contribute to the SDGs at different levels.

The implications of the 4IR for people are extensive and can contribute to ending poverty (Goal 1). Equitable access to and gender-responsive and gender-specific design of new technologies is needed to reduce inequality and promote gender equality (Goal 5). To foster peaceful, just and inclusive societies, the benefits of the 4IR need to be equitably distributed (Goal 16). However, unless actively addressed, the lack of digital connectivity and access to technologies promoting digital literacy will increase disparities between countries, societies and individuals, with the poorest and women and children suffering the most. Education and the health sector increasingly utilized digital technologies during the COVID-19 pandemic, which should be sustained. As evidenced by the least connected in society having suffered as access to education resources was restricted and health services having struggled due to reaching operational capacities, achieving accessible quality education (Goal 4) and promoting health and well-being for all (Goal 3) depends on developing an open and accessible digital technology infrastructure. New technologies deployed in agriculture can help increase productivity, improve resource efficiency and build resilient food supply chains, and therefore, have a role to play in delivering Goal 2, zero hunger.

The 4IR has positive implications for prosperity as digital technologies transform economic growth and can reduce inequalities within and between countries (Goal 10). Production transformation by advances in robotics, IoT, machine learning, AI and big data will change the workplace and alter jobs for people, potentially eliminating them or reducing their scope, challenging Goal 8. The integration of information and communications technologies (ICTs) within every part of the production process is the current and evolving interconnected realm of smart manufacturing. Agile, adaptive and intelligent manufacturing processes that combine the digital and physical in the complete value chain will produce products more rapidly, helping to advance enduring industrialization (Goal 9), and efficiently use fewer resources, stimulating responsible, sustainable production and consumption (Goal 12).

The advancement in economic growth delivered by new production methods should be aligned with full, productive and decent employment (Goal 8). Smart cities and infrastructure will become both more resilient and sustainable as digital technologies help deliver sustainable cities (Goal 11) and infrastructure (Goal 9), and reduce resource consumption. Goal 10, the reduction in inequality, depends on the equal distribution of benefits promised by the new technologies of the 4IR. However, the 4IR technologies are not without risks, for example, the potential to monitor and survey citizens, via AI face recognition technology, raises privacy and human rights issues.

The 4IR also presents environmental challenges and opportunities. Successive industrial revolutions and human activity use the earth for its resources and to deposit waste. Deployment of integrated new technologies can replace unsustainable behaviours, business models and industrial activities, contributing to sustainable energy (Goal 7), and help combat climate change (Goal 13). However, digital technologies are not without environmental impacts, for example, high energy consumption of ICT systems and the burgeoning waste disposal problem resulting from consumer electronic equipment. 4IR technologies can disrupt the traditional linear economic model (make, use and dispose) to a

DIAGRAM 1 – IMPLICATIONS OF THE 4IR FOR SUSTAINABLE DEVELOPMENT LINKED TO SPECIFIC SDGS

PLANET

New technologies can support a circular economy, increasing sustainable economic growth and the protection of marine and terrestrial ecosystems

Deployment of new technologies can promote sustainable practices, business models and industrial activities, thereby combating climate change

New technologies increase resource efficiency, stimulating responsible, sustainable production and consumption

PROSPERITY

The 4IR has positive implications for prosperity as digital technologies transform economic growth and can reduce inequalities within and between countries

Agile, adaptive and intelligent manufacturing processes that combine the digital and physical spheres across the entire value chain will increase productivity, helping to advance enduring industrialization

Advances in robotics, IoT, machine learning, AI and big data will transform production, altering the workplace and jobs for people

Smart cities and infrastructure will become more resilient and sustainable as digital technologies help deliver sustainable cities

Deployment of new technologies can alter unsustainable behaviors, business models and industrial activities, contributing to sustainable energy production

circular economy. An economy regenerative by intention and design seeks to replace the end-of-life concept with restoration and reuse aimed at sustainable economic growth and the protection of marine and terrestrial ecosystems (Goals 14 and 15).

The pace and the complexity of the 4IR can blur international borders and entangle boundaries between public and private, presenting national regulators with unique governance challenges. **Regulation can struggle to keep up with advances of the 4IR, hindering innovation and leaving society with outdated laws and regulations.** Regulators need to adopt a more agile, flexible approach to regulation to seize the potential of the 4IR to deliver benefits to society and manage its risks. In this vein, the G20 Digital Economy Task Force has been piloting an initiative on agile regulation for 4IR among several countries, serving as a useful tool to share experiences and common approaches to more agile governance and regulatory models for innovation.

To grasp the opportunities and mitigate the risks from 4IR technology, the 'regulate and forget' approach needs to give way to an 'adapt and learn' approach. The pandemic illustrated that regulation was outpaced by technology and reinforced the need for speed with fast-track regulation being developed to facilitate medical innovations, such as telemedicine. The transnational nature of many disruptive technologies calls for greater collaboration between national regulators and stronger international partnerships and consensus to build effective regulations and policies. Noting that good regulation is essential for economies to function efficiently, while meeting important social and environmental goals, the OECD Recommendation of the Council on Regulatory Policy and Governance is the fruit of careful assessments of best practice identified by the Regulatory Policy Committee through a decade of reviews of OECD countries. Representing a maturing of thinking and learning from experience in this complex policy area, the Recommendation develops a systemic governance framework that can deliver ongoing improvements to the quality of regulations. It provides governments with advice on the development of institutions and the application of regulatory management tools. It also provides practical measures or benchmarks against which countries can assess their capacity to develop and implement quality regulation.

As a voluntary complement to regulations, standards have a unique role to play in digital transformation governance. **Standards offer global, transnational, multidisciplinary and potentially rapid responses to the needs of the 4IR's technological developments.** Stakeholders, if fully engaged, are well placed to ensure standards for disruptive technologies that are reshaping businesses and societies worldwide are synchronized with the needs of people, serving everyone in society and sustainable development. Standards, therefore, must play a crucial role in harnessing digital transformation equitably.

DIGITALIZATION AND THE DIGITAL TRANSFORMATION

The Fourth Industrial Revolution (4IR) is a term coined in 2016 by Klaus Schwab, Founder and Executive Chairman of the World Economic Forum (WEF). It is characterized by the convergence and complementarity of emerging technology domains, including nanotechnology, biotechnology, new materials and advanced digital production (ADP) technologies. The latter includes 3D printing, human–machine interfaces and AI, and is already transforming the global industrial landscape. Incorporating ADP technologies into industrial production processes has given rise to the concept of Industry 4.0, also known as the Smart Factory—one that learns as it works, continuously adapting and optimizing its own processes accordingly.

The 4IR is also characterized by the widespread and ever-increasing phenomena of *digitization,* i.e. the conversion of analogue information into digital form. At the same time, the ever-greater *digitalization*—the development and application of digital and digitalized technologies that augment and dovetail with all other technologies and methods[5]—is serving to reinforce and expand the *digital economy* (Text Box 1).[6]

Text Box 1 – The Digital Economy

The OECD defines digital economy as incorporating all economic activity reliant on or significantly enhanced by digital inputs, including digital technologies, digital infrastructure, digital services and data. It refers to all producers and consumers, including the government, utilising these digital inputs in their economic activities.

In a larger context, digital transformation is a broader term than digitalization. It is the integration of digital technology into all organizational areas, fundamentally changing how the organization operates and delivers value to customers or stakeholders.[7] It is also about prioritizing organizational culture change, which requires organizations to continually challenge the status quo, experiment and get comfortable with failure. Digital transformation is a widely used term that, in practice, will look very different in each organization. In essence, it refers to the customer-driven strategic business transformation requiring organizational change and the implementation of digital technologies.

Three factors are driving the digital transformation. The first driver for digital transformation is necessity. Survival and adaptation to rapidly changing markets and circumstances challenge organizations to rethink how they execute their operations radically. The dramatic global impact of the COVID-19 pandemic advanced the adoption of digital technologies. It prompted more organizations, both commercial and governmental, to engage with digital transformation necessitated by stresses such as supply chain disruptions, time to market pressures and rapidly changing needs in the health sector.

The second reason why digital transformation is happening is the technology itself. According to the OECD, mobility, cloud computing, IoT, AI and big data analytics are among the most important technological drivers. The opportunities offered by digital technologies for innovation and efficiency drive change powered by rapid connectivity, exponential generation of data and affordability as time passes. Governments, for example, rolled out many large-scale digital innovations at speed during the pandemic, such as deploying AI and automation tools to deliver faster services and reduce workloads and the shift to the cloud, allowing employees to work remotely and helping governments reach citizens. Scaling digital infrastructure, creating a more digitally savvy workforce and investing in citizen connectivity are achievable goals for governments with digitalization.

Expectations have been raised by digitalization and this heightened set of expectations is the third factor driving digital transformation. Citizens count on the same kind of experience in a professional setting as they experience with technology in their personal lives. Delivery of services and products that meet or go beyond stakeholder expectations for seamless integrated and efficient customer experience that meet their demands require businesses, governments and all organizations to transform their delivery models, embracing digital technologies and innovative approaches.

[5] WBGU EU Policy paper on digitalisation
[6] OECD Roadmap Towards a Common Framework for Measuring the Digital Economy 2020
[7] The Enterprise Project 2021

DIGITAL TRANSFORMATION IMPACTS ON PEOPLE, PROSPERITY AND THE PLANET

The accelerated pace of change brought about by digital transformation to production, the economy, the environment and society will significantly impact the achievement of the 2030 Agenda for Sustainable Development and related SDGs. The digital transformation is in full swing and although little mention is made to it or digital technologies in the 2030 Agenda for Sustainable Development, it will have profound consequences for people, their prosperity and the planet. As it is a development driven by humans, it has the potential to be shaped to promote sustainability for the benefit of all parts of society.

Implications for planet

Unchecked digital transformation unaligned with the environmental constraints of the earth will negatively impact the **planet**, increasing resource and energy consumption, exacerbating damage to terrestrial and water ecosystems and accelerating climate change. Digital technologies offer the potential to contribute to the protection of the planet. Digitalization could transform energy and transport into low-carbon systems. Digital infrastructure technology could deliver smart cities, homes and roads that minimize resource consumption and waste whilst offering more sustainable communities. Digital technologies can address water scarcity, sanitation and water quality through sensors and IoT, as well as improve sustainability in fisheries. If businesses harness the innovative possibilities of digital transformation, they could achieve circular economy and dematerialization opportunities. However, any benefits to sustainability goals require sustainability concepts to be a fundamental part of the digital transformation.

DIAGRAM 2 – DIGITAL TRANSFORMATION **IMPACTS**

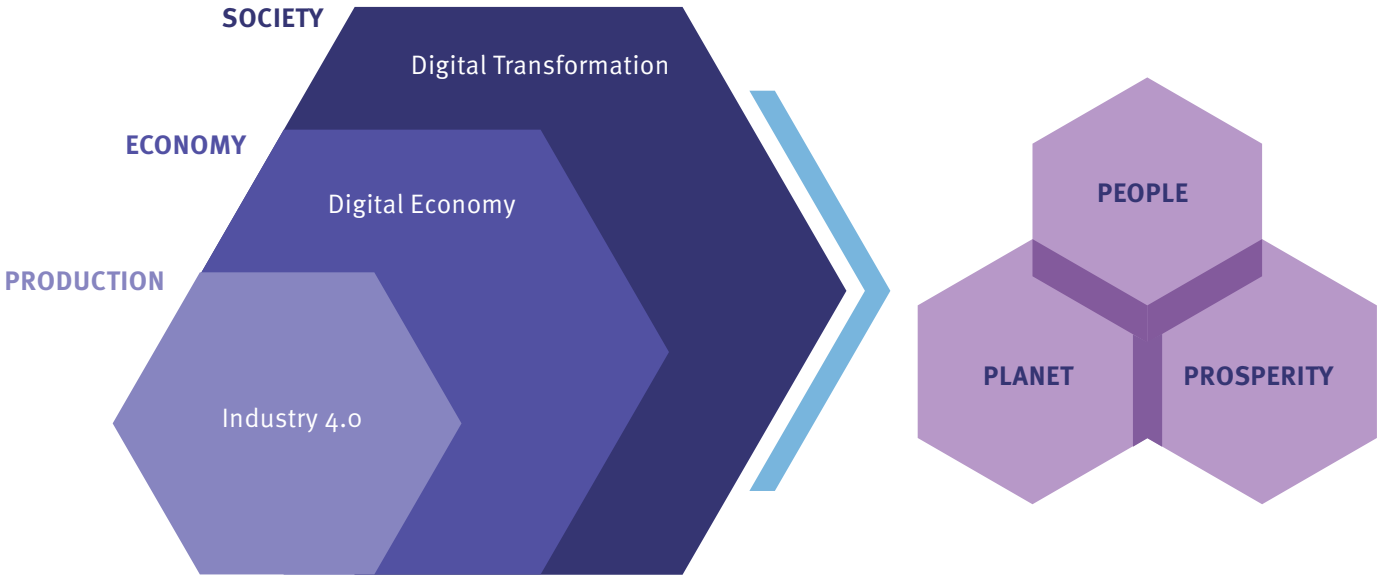
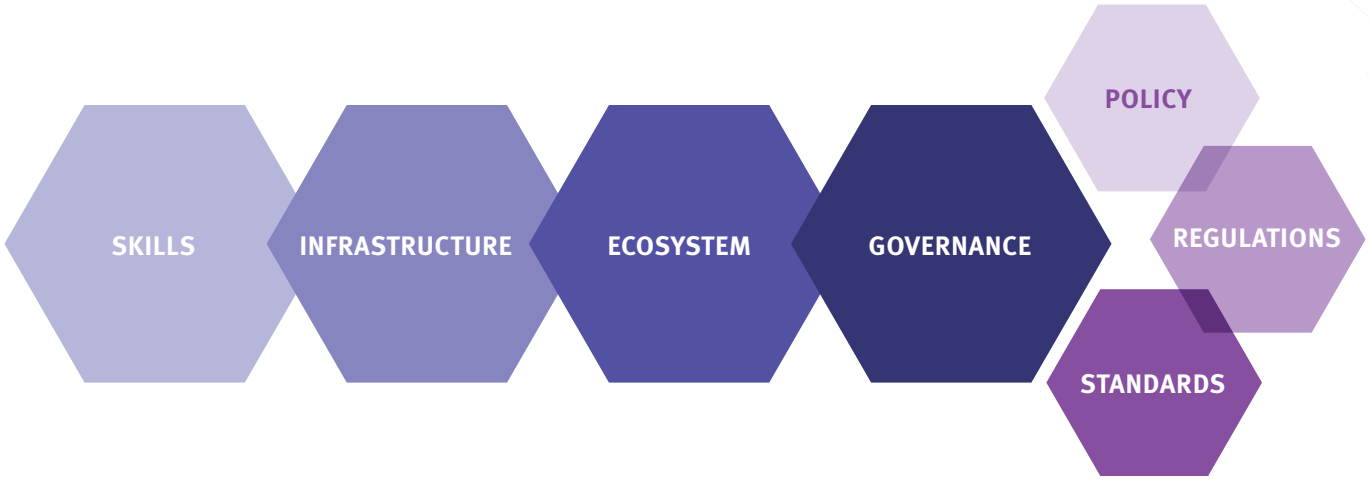


DIAGRAM 3 – DIGITAL TRANSFORMATION **ENABLERS**



Implications for people

Digitalization is unevenly distributed but offers the potential for overcoming spatial and social barriers to benefit people. Developing and emerging economies are poorly served by digital technologies, and their people, especially the poorest, are excluded from the opportunities and benefits. Poverty excludes participation in the digital economy and marginalizes vulnerable groups, especially women, children, migrants and rural dwellers who are further disadvantaged by lack of access to communication technologies. Around two billion people worldwide lack access to ICT, including access to the knowledge, education, and training needed for economic inclusion in the digital economy. The digital transformation is disrupting the employment landscape. New forms of employment are being created and global networks mean geographic location is less of a barrier to people working remotely in the digital economy. Science, technology, engineering and mathematics (STEM) skills are in demand, highly valued and rewarded, whereas other non-digital occupations such as child care remain undervalued. Limited education resources to increase STEM skills further weaken participation in the digital economy. Social and labour standards risk being undermined and jobs replaced by digital technologies deployed in smart manufacturing, agriculture and commerce. People are more interconnected and dependent on digital infrastructure that exposes them to cybersecurity threats such as privacy breaches, technical failures and unintended consequences of the new technology like gender and ethnic bias in AI.

Implications for prosperity

Digital transformation is fundamentally changing the commercial world, impacting competition whilst disrupting markets and affecting prosperity. Digital technologies are transforming production by enabling new production methods and business models. For example, smart manufacturing harnesses agile, adaptive and intelligent processes to combine the digital and physical spheres to produce more efficiently with greater returns, using fewer resources. The global market for digital transformation technologies and services was valued at USD 1.3 trillion in 2020.[8] However, the digital economy has created vast monopolies dominating sectors of society with little accountability or transparency. Digitalization has allowed data collection and monitoring systems, on a scale previously not seen, for use by a variety of actors that infringe on privacy and personal rights and freedoms. New and emerging technologies need to remain human-centered and serve society to ensure everyone has equitable access to benefit from the economic and social opportunities.

Ensuring digital transformation enablers are in place is integral to supporting the adoption and implementation of digital technologies and for people and the planet to prosper from technological change.

[8] IDC Market Report

PART 2: **STANDARDS**

The World Trade Organization's Agreement on Technical Barriers to Trade (WTO/TBT) defines a standard as a voluntary document to which compliance is not mandatory, as opposed to a technical regulation, to which compliance is mandatory. The WTO/TBT definition has introduced a clear-cut distinction between standards (voluntary) and technical regulations (mandatory), which is useful and has been broadly accepted in the field.

Standardization of digital technologies happen in the national, regional and international space in various organizations, including companies, professional bodies and trade associations, non-governmental organizations (NGOs), intergovernmental organizations and standards development organizations (SDOs).

At a regional level, SDOs are undertaking the analysis of the standards landscape in individual digital technologies, for example, the road map analysis from the European Committee for Standardisation and European Committee for Electrotechnical Standardisations (CEN-CENELEC) Focus Group on AI and European Union Observatory for ICT Standardisation (EUOS) global landscape analysis of AI standards. Coordination between international SDOs should be pursued to prevent duplication of work and harness the collective expertise and stakeholder engagement of these organizations.

THE ROLE OF STANDARDS IN ECONOMIC GOVERNANCE

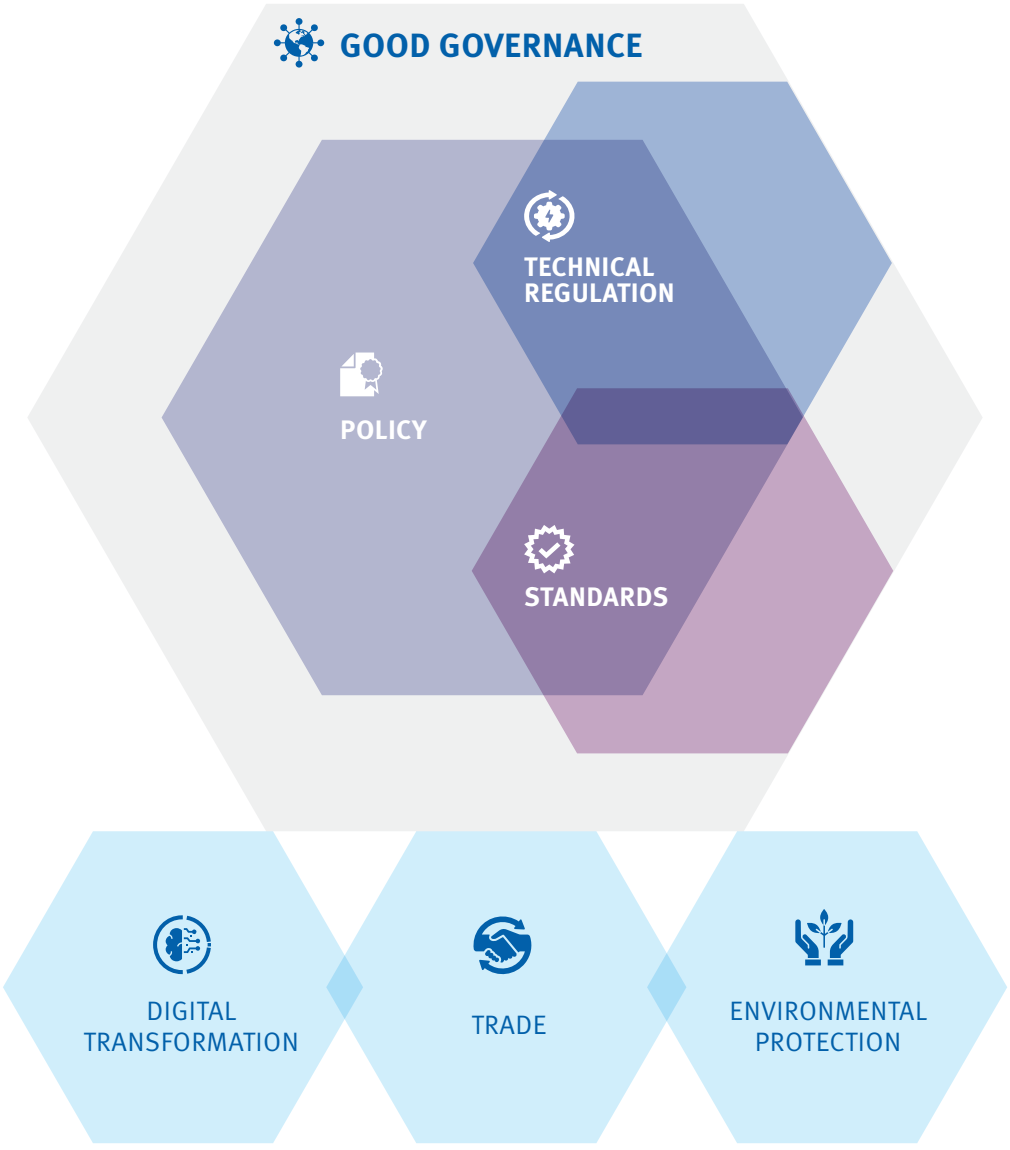
The role of standards in economic governance derives from the wide range of functions that they fulfil. Amongst others, standards define interoperability between products and processes, transfer information both between economic agents and between machines and systems, and guarantee minimum levels of quality and safety for consumers. These functions, in turn, affect the economy in a variety of ways, including through the improvement of competition and efficiency, the exploitation of network effects, the diffusion of innovation and the reduction of production costs. Besides interoperability of new and legacy technologies, in general there is also a horizontal dimension of interoperability of technologies, products, services and systems produced by different organizations at sectoral, national, regional and international levels. Interoperability enables the capability to communicate, execute programmes, or transfer data among these various functional components.

There is also a circular relationship between standards, regulations and policies, which feed into an overall concept/public good of good governance. Standards are a voluntary complement to regulation, which have the effect of enhancing efficiency and productivity. These standards inform effective regulations, which can create an enabling environment for innovation and minimize risk for disruptors and investors. The WTO/TBT acknowledges the role of technical regulations, standards, and conformity assessment procedures, e.g. testing, inspection and certification, for the efficient attainment of public goals, and sets rules to ensure that these measures are prepared, adopted and applied in ways that do not create unnecessary barriers to international

trade. Although the TBT Agreement is primarily about technical regulations, standards (which are voluntary by definition in the TBT Agreement) have an important role in the framework of the agreement. WTO's members are expected to use international standards (whenever they exist, or their completion is imminent) as a basis for technical regulations—and technical regulations in accordance with relevant international standards are not deemed to constitute an unnecessary obstacle to trade. The TBT Agreement requires that its members use relevant international standards, guides or recommendations for conformity assessment procedures as a basis for their own procedures for a positive assurance of compliance with technical regulations and standards. Standards developed by international organizations can, therefore, provide an effective response to market barriers.

In the context of digital transformation, the timely and harmonized adoption of standards is likely to play a key role to this end, both as a means of promoting interoperability, productivity and innovation, and of ensuring the successful scale-up of solutions to be implemented globally. Standardization can offer a number of benefits and opportunities for digital technologies, inter alia: unifying technologies and specifying common technical features; promoting interoperability and compatibility; helping to eliminate technological silos; enhancing innovation and growth; accelerating technology adoption; building trustworthiness and describing governance frameworks; aiding user understanding, acceptance and confidence in new technologies; helping to minimize risks, improving safety, avoiding technological lock-ins and validating quality; collating best practices and use cases; and supporting policy and legislation.

These outcomes may be especially beneficial in restoring international manufacturing and trade to their previous vitality, as both sectors slumped significantly due to the COVID-19 pandemic, the associated lockdowns and value chain breakdowns in many regions. The COVID-19 pandemic has become a catalyst to accelerate digital transformation for which a set of internationally recognized standards—urgently needed by policymakers, businesses, and the public—are indispensable as latent risks in all industries have been crucially revealed. Such risks include weak and untimely governance, the inefficiency of the global value chain, and the lack of knowledge, awareness and trust of the public. Commonly accepted standards will enhance the smooth operation of global value chains, enhancing confidence in quality, traceability and safety across borders, while also contributing to industrial recovery and resilience.



THE ROLE OF STANDARDS IN GOOD GOVERNANCE OF DIGITAL TRANSFORMATION

Digital technologies and the new business models of digital transformation (as previously outlined with respect to agile regulation) do not fit easily into the traditional regulatory framework regulators use to intervene in markets. It is clear that previous modes of governance, which are largely reactive in nature, cannot hope to be effective in the era of advanced digital transformation. Governance rules and regulatory approaches for new technology and processes of innovation need to be more agile, flexible and resilient through the development of experimental regulation such as regulatory sandboxes, anticipatory approaches, multi-stakeholder use of guidelines and standards, and the promotion of international initiatives. Furthermore, regulators, as stakeholders, need to be involved in the development of voluntary standards, e.g. participate in national standards body (NSB) technical committees, to ensure that the standards are suitable if they choose to refer to them in regulations.

The widespread recognition of a need for proactive regulation has led to some innovative developments in recent years concerning how we "square the circle" of developing timely standards and regulations for advanced technologies, without hindering innovation or leaving regulatory voids, in which little is done to mitigate the potential downside effects of unchecked digital transformation. This has begotten the concept of "agile regulation", which has appeared prominently in multilateral discourse on digital transformation in recent years. For instance, the concept of regulatory sandboxes first emerged in the United Kingdom in 2016, primarily in the fintech sector. This concept essentially allows for testing of innovative concepts in a controlled environment under the supervision of regulators, in order to facilitate innovation without encumbering innovators with overly-burdensome regulations in the initial stages of development.

Other forms of agile regulation include policy prototyping, in which new innovations are subjected to small-scale testing prior to scale-up; and technology foresight, which inputs for the formulation of technology policies and strategies that guide the development of the technological infrastructure. Such approaches have become very popular in recent years, with the World Bank reporting that 57 countries have implemented the concept of agile regulation to some extent.[9]

However, as innovative as the agile regulation concept is, it cannot meet all governance needs for digital transformation in a vastly heterogeneous international order, bearing very different capacities, needs and priorities. Least developed countries typically have very different capacities and needs than high-income countries with respect to digital transformation. The UNIDO Industrial Development Report 2020 found that just ten economies (mostly in the Global North) account for over 90% of advanced innovation patents and 70% of associated exports, while 88 developing countries play little meaningful role in the advanced digital production sector, either as consumers or producers. This indicates a vast digital divide which cannot be solved by piecemeal or ad hoc solutions. In light of this, developing countries are increasingly participating in the development of international standards, i.e. in the ISO and IEC systems. This is to such an extent that initiatives such as the Commonwealth Standards Network and the Belt and Road Initiative and other capacity building projects are seeking to mobilize developing countries in standards development.

Standards must, therefore, play a foundational role in any initiative to harness digital transformation equitably on a global basis. Standards are voluntary rules or guidelines that codify information. They provide specifications and technical information (intended for common use) on products, materials, services and processes. They are particularly relevant to technology-related products. Standards are not developed in isolation but are produced in a regulatory and policy framework, a framework evolving to encompass the challenges presented by digital transformation and the digital technologies, which also needs to account for challenges posed to sustainability.

Standards have an essential role in providing solutions to current and future technological and societal challenges derived from digital technologies because they set minimum requirements in terms of safety, security, reliability, efficiency, interoperability and trust. They also act as a precursor to regulations on a voluntary basis, granting expertise and buy-in from private sector innovators, and leading to regulations that minimize risk and create an enabling environment for innovators and investors. Consequently, several international organizations and professional bodies have developed considerable policy expertise regarding digital standards in recent years, not least the International Organization for Standardization (ISO), the International Electrotechnical Commission (IEC), the International Telecommunication Union (ITU), the United Nations Industrial Development Organization (UNIDO), the Institute of Electrical and Electronics Engineers (IEEE) and the G20.

Transnational blurring also serves as an opportunity for international organizations to fill the void of global leadership and contribute to the well-being of all humankind from a holistic perspective instead of a self-focused one at the national level. International organizations remain impartial in developing, implementing, and monitoring standards by engaging countries to be a standard-setter rather than simply a standard-taker to achieve a shared prosperous future. International organizations launch multiple voluntary initiatives, such as the United Nations Global Compact and the Global Manufacturing and Industrialisation Summit (GMIS) led by UNIDO, to involve all stakeholders, especially the private sector.

However, a preponderance of standards may also bring some challenges in terms of over-complexity and potential monopolies or abuse of a dominant market position by larger technology providers. It is thus vital to ensure collaborative processes/multi-stakeholder partnerships for the development of necessary standards and to strike the correct balance in this regard.

[9] https://blogs.worldbank.org/psd/four-years-and-counting-what-weve-learned-regulatory-sandboxes

ESSENTIAL CRITERIA FOR DEVELOPING STANDARDS FOR DIGITAL TRANSFORMATION

Standards can also be seen has having enabled digital transformation by codifying best practice and enabling technology transfer. Activities concerning the development of standards at the international level were comprehensively reviewed for the purpose of this publication to include the following categories: **foundational/general**, describing the technology's vocabulary, definitions, and taxonomies; **method and approaches/operation**, containing the characteristics of the technology in operation and special features of its operation and also including approaches, engineering aspects, interoperability, testing, health and safety, risk assessment, data, materials and quality and security; **trustworthiness**, covering such fields as governance, privacy, transparency, ethics, accountability, and cybersecurity; and **use cases/application,** referring to a selection of case studies and how these might inform best practice on applying seven of the most-trending digital technologies of the 4IR (such an approach has already been adopted by international fora in other contexts, e.g. the G20's Compendium on the Use of Digital Tools for Public Sector Continuity).

Not all categories apply neatly to each of the seven digital technologies. Each of the seven technologies has foundational or general standards, and the category of method and approach/operation is also relevant to all seven technologies.

As not all digital technologies have the same impacts on people and society, standardization efforts in trustworthiness are concentrated in AI and big data, DLT/blockchain and IoT. These technologies have the biggest potential impacts on people in terms of infringement on human rights and privacy and their societies than, for instance, 3D printing and unmanned aircraft systems (UAS). For example, standards on UAS cover the safety aspects of shared airspace and it is national civil aviation regulations and data protection laws that govern privacy aspects of civil drone operation in the EU.

These four criteria are essential to developing our understanding of what to consider when developing standards for digital transformation worldwide, and for seven of the most-trending technologies in particular, which will be further discussed in part three of this publication.

PART 3: **TECHNOLOGIES**

THE BIG 7 DIGITAL TECHNOLOGIES OF THE 4IR DESCRIBED

The digital transformation is powered by digital technologies of the 4IR. The rapid adoption of these disruptive technologies is accelerating and has been further boosted by the COVID-19 pandemic. Global spending on digital transformation technologies and services grew by 10.4% in 2020 to USD 1.3 trillion.[10]

Technological adoption is not a geographically even process; a greater quantity and rapidity of technology adoption is happening in developed countries. Least developed countries (LDCs) are hampered by, among other things, lack of ICT and access to proper architecture and basic assets such as computers and smart devices but most importantly, the capacity to ensure people have the right set of basic skills. Illustrating this unevenness: in 2019, 92% of Swiss households compared to 38% of Bangladeshi, 36% of Peruvian and 34% of Pakistani households had access to ICT.[11]

Seven digital technologies of the 4IR that will considerably impact people, their prosperity and the planet include: artificial intelligence (AI) and big data,[12] blockchain/ distributed ledger technology (DLT), Internet of Things (IoT), robotics, 3D printing and unmanned aircraft systems (UAS). **While the scope and impact of digital technologies vary, standardization has a role to play in each one to help deliver trust, privacy, protection, interoperability and sustainability.** A comprehensive review was undertaken for the purpose of this publication of the current developed digital-related standards and SDO committee activities in the digital space, with emphasis on the seven big digital technologies of the 4IR. These seven digital technologies and the role of standards for each will further be discussed below.

ARTIFICIAL INTELLIGENCE (AI) AND BIG DATA

About the technology

There are many and varying definitions of artificial intelligence (AI). Since it was first defined in the 1950s, defining AI has been driven by different categorizations mainly based on how the AI system thinks or acts, however, still today there is no straightforward definition. The UNIDO Industrial Development Report 2020 conceptualized it as, "...the branch of computer science seeking to simulate the human capacity to reason and make decisions. The term usually refers to such artificial intelligence techniques as machine learning, deep learning, neural networks, fuzzy logic, computer vision, natural language processing and self-organizing maps to provide machines and systems with human-like cognitive capabilities, such as learning, adapting, perceiving and solving problems. Artificial intelligence can be defined as making computers intelligent and capable of mimicking and predicting human behaviour and solving problems as well as or better than humans."

AI is a field that is growing exponentially, full of innovators and disruptors, and draws on the power of big data; consequently, these two technologies are considered together. Every two days more data is produced than in all of history before 2003 and the pace is increasing.[13] This surge in data generation has led to big data analytics and, along with the all-pervading ICT, has helped drive AI adoption. AI is making rapid inroads into domains previously the preserve of humans, potentially offering solutions to some of the biggest challenges facing the planet and its people. However, AI also presents risks that governments, society and businesses need to understand and tackle to ensure AI systems reach their intended functional goals, benefitting people and the planet, while avoiding unintended consequences.

Measuring the development of AI technologies is challenging as the boundaries between AI and other technologies blur and change over time; for example, AI is present in physical technology like driverless cars and care robots and software systems, like medical diagnostic tools and chatbots. The number of patent applications published by more than 100 patenting authorities in the AI field grew by an average of 28% a year between 2012 and 2017.[14] Japan, Republic of Korea and the United States accounted for over 60% of AI-related patent applications from 2014 to 2016.[15] The global value of the AI market size was USD 62.35 billion in 2020 with an anticipated compound annual growth rate of 40.2% from 2021 to 2028.[16]

Role of standards for AI and big data

Developing norms and standards is a big task in the AI and big data fields. SDOs have entered robustly into the field, and at the moment technical standardization work is being actively pursued by international SDOs including ISO, IEC, ETSI, ITU-T and IEEE. National standards bodies (NSBs) have also entered enthusiastically into the field, in particular in China, the United Kingdom and the United States. The comprehensive review of standards at the international level identified standard making in AI and big data occurs in the following categories:

- Foundational
  - Vocabulary AI and data
  - Taxonomies
- Methods and approaches:
  - Computational approaches
  - Architectures and engineering of AI systems and data
  - Characteristics of AI systems
  - Quality and data for AI

[10] IDC Market Report
[11] ITU Digital Development Dashboard
[12] For the purpose of this publication, AI and big data have been grouped together.
[13] David Stuart, Facilitating Access to the Web of Data
[14] *The IP behind the AI boom,* WIPO Magazine
[15] WIPO Technology Trends 2019 Artificial Intelligence
[16] Grand View Research Market Analysis Report

- Trustworthiness
  - Security, privacy, transparency, ethics, accountability, safety
- Use cases and applications
  - Repository of use cases and best practices for application domains

Standards activity is extensive in the AI field. As it is a transversal technology, affecting many other IT fields, it is being considered by many SDOs committees in addition to AI ones, such as robotics, vehicles, medical devices and financial services. A joint IEC and ISO technical committee (TC) on IT issues has been working on AI terminology for several years and has developed a suite of standards aimed at providing clear language and definitions on such areas as machine learning (ML), neural networks and natural language processing.

Standards can help increase the level of trust people have in AI. It is difficult to trust what cannot be defined, therefore, the lack of a common definition of a technology that is pervasive in peoples' lives and has the capacity to impact human rights and well-being can lead to distrust. By enabling a common definition to be reached, standards can ultimately help create trust in AI systems. Standards can also facilitate the understanding of AI systems which can also create trust in their outputs, decisions, recommendations and general ecosystem, thus enhancing the human–machine relationship. Furthermore, as humans are consumers of AI, in many cases unknowingly, standards can play a key role in providing protection to users, also ultimately leading to trust.

Despite the potential for standards to increase trust, standards-makers face challenges in the areas of governance, accountability, transparency and cybersecurity, and in how to standardize these aspects of AI. There is a need to foster a dialogue with various societal stakeholders not normally involved in standardization on AI and its trustworthiness. The IEEE Global Initiative on Ethics of Autonomous and Intelligent Systems brought together a diverse range of experts from technical as well as ethics backgrounds to discuss how to establish ethical and social implementations of AI that prioritize human well-being. This resulted in the Ethically Aligned Design documents and drove several standards development programmes under the IEEE 7000 series of standards addressing, amongst other issues, transparency and governance.[17]

UNIDO is also deeply engaged on this issue and is in the process of finalizing guidelines/principles for use of AI by small and medium enterprises in developing countries.

AI technologies such as ML and deep learning utilize big data. ML is the development of computer algorithms that learn autonomously based on data and information (see Case Study 1), while deep learning, which includes neural networks, uses reinforcement learning and has more autonomy to make decisions. One of the biggest concerns in AI systems is the capacity to cause perverse human-harming outcomes if bias is not properly managed and understood in the data sets and algorithms used. As this outcome results from the data and its respective weight, if there is a lack of understanding of the bias in the technologies and corrective action is not taken through modelling, misapplication of the AI systems could be perceived as human intention to manipulate outcomes, creating a distrust in the system. Acknowledging this, ITU-T has a Focus Group on ML for future networks including 5G, with one of its objectives being to identify aspects that enable safe and trusted use of ML frameworks. There is a crucial need for AI systems to be transparent (and to the extent possible, in the case of deep learning) about their intended purpose and decision-making processes and to be accountable to allow stakeholders to understand and challenge them. At the European level the EU established in 2018 the European AI Alliance, a multi-stakeholder forum engaged in a broad and open discussion of all aspects of AI development and its impact on society and the economy.

Case Study 1 – Promoting sustainable bush-processing value chains in Namibia[18]

Invasive bush species are a problem in Namibia. Converting it into animal feed and charcoal was deemed a viable solution to strengthen important sources of food and income. Based on a feasibility study, UNIDO proposed a strategy to deliver bush-based final products for agricultural, chemical and pharmaceutical purposes, as well as domestic use. NGGP, a special purpose production plant, is being operationalized for manufacture of high-value livestock feed, coal, chips, Arabic gum and other selected products utilizing invasive Acacia species.

Innovative digital technologies and know-how for sustainable bush thinning and harvesting were used specifically—the Machine Learning Model for Acacia species mapping based on remote sensing texture image analysis and satellite and drone supported image recognition for the agricultural sector. The ML algorithm was fine-tuned to provide yield predictions to enable the NGGP plant to produce high-quality bio charcoal and animal feed. This pilot plant is expected to have a multiplier effect and be reproduced in other locations in Namibia and the region. A branding and marketing strategy was designed to ensure the long-term resilience of the operation. Bush-based animal feed and charcoal acquired a brand name Bushtainable Harvesting - NutriPellets and Bushtainable Harvesting - BushBQ to emphasis the eco-branding philosophy.

The project contributes to SDG 15, i.e. removing invasive bush contributes to sustainable use of land and reduces land degradation, improves farming practices and productivity, as well as improves food supply for the local population (SDG 2). It also helps with water management and shortages (SDG 6) and the transfer of technological know-how and skills, developing job creation opportunities for local people in rural areas (SDG 8).

[17] https://ethicsinaction.ieee.org/

[18] Strategic Action Plan for Sustainable Bush Value Chains in Namibia, UNIDO, 2019

Standards can also create a solid basis to ensure inclusiveness through the management of bias that, if not well managed, has a greater possibility to cause harm. These challenges are common to all societies across the globe and will need to be dealt with at the international level. Standards are ideally placed to assist in this respect. A major joint standardization effort is the subcommittee ISO/IEC JTC 1/SC 42 on Artificial intelligence. It has established three sub groups: SG 1 covering computational approaches and characteristics of AI systems; SG 2 investigating approaches to establish trust in AI systems through transparency, verifiability, explainability and controllability; and SG 3 identifying use cases and applications in different AI application domains, e.g. social networks, and different use contexts, e.g. healthcare and smart home.

Considerations over gender equality play an important role in this respect. Further to considerations over the need to ensure data safety and responsible/ethical data processing, more practically, AI holds the potential to provide a multitude of benefits, such as the promise of better care and disease outcomes for women as a result of targeted analysis of women's healthcare data, avoiding data bias. AI also poses a risk of perpetuating (gender) stereotypes, fostering further discrimination on the grounds of sex and gender, and widening the digital gender divide. For example, using and benefitting from voice activated/voice recognition devices can pose a challenge for women (and other users, e.g. speakers of dialects), as AI is susceptible to data bias, identifying and better responding to default male users. Gendering of technologies is also problematic in this regard as digital assistants are oftentimes female by design and/or learning. Standardization activities for AI could be guided by inclusiveness and equity to avoid negative outcomes for gender equality.

AI has the capacity to exponentially change the way humanity lives, however, its accelerated pace is leaving behind vulnerable groups and communities. Standards can act as an enabler for AI to generate positive outcomes for people, planet and prosperity, thus contributing to achieve SDGs in a more efficient path.

While there are standardizations challenges in the technical aspects of AI such as coordinating efforts to ensure harmonized data models and semantics across different domains, the more fundamental challenge is how to develop standards that mitigate risks and negative impacts, including misuse, as AI evolve as socio-technical systems. In particular, we must elaborate upon how standards can assist in ensuring AI and big data are accountable, trustworthy, transparent and safe.

BLOCKCHAIN/DISTRIBUTED LEDGER TECHNOLOGY (DLT)

About the technology

Blockchain[19] and distributed ledger technology (DLT) is a rapidly evolving and expanding technology. The disruptive technology emerged in 2008, but the market has grown significantly since then. The global blockchain/DLT market value was estimated to be at USD 2.89 billion in 2019 and is projected to reach USD 137.29 billion by 2027, growing at a compound annual growth rate of 62.7% from 2020 to 2027.[20]

[19] N.B. Cryptocurrency is not covered by this publication.
[20] Allied Research Network - Blockchain Distributed Ledger Market

A *distributed ledger* is a type of database, shared, replicated, and synchronized among the decentralized network members with no central authority or third-party mediator like a bank. All records in the ledger are timestamped and given a unique cryptographic signature, thus providing a verifiable and auditable history that is highly resistant to unintended changes (i.e. tamper-resistant). Blockchain is a type of DLT that permanently records in a sequential chain of cryptographic hash-linked blocks. DLT and blockchain are useful wherever requirements for traceability, accountability, regulatory compliance, and authoritative data exist, such as finance, supply chain management, logistics and health (see Case Study 2). For example, in March 2020, the World Health Organization (WHO) unveiled its MiPasa-based blockchain programme to help convey information about the COVID-19 outbreak.

Case Study 2 – Feasibility assessment for blockchain in the Ghanaian cocoa value chain

UNIDO has developed a methodology to assess the readiness of a value chain to implement blockchain technology. With the support of the Global Quality and Standards Programme (GQSP), the methodology was applied in the Ghanaian cocoa value chain in 2020 and the Peruvian cocoa and coffee value chains in 2021. The assessment method allows governments and the private sector to make an informed and collective decision on adopting the right technology for their needs and to have a road map towards a blockchain solution adoption.

The methodology consists of three parts that are geared to answering the following questions:

1. SCOPING – Does this value chain need blockchain?

Identification of the issues or business problems in the value chain that could be addressed by implementing blockchain.

2. SCORING – Is this value chain ready for blockchain?

A more technical viewpoint on whether the value chain would be ready for implementing blockchain.

3. SOLUTION – What does it take to implement blockchain?

The assessment identifies benefits and makes final recommendations on requirements, next steps and stakeholders to be involved.

Central to the approach is a fact-finding mission to collect information on the potential benefits of and the possibilities for blockchain implementation in the value chain. On the ground information is gathered from questionnaires tailored to different value chain stakeholders.

The methodology only relates to an initial assessment of the readiness of a value chain for blockchain adoption not the actual implementation. The adoption of blockchain could contribute to SDGs by improving food safety and security (Goal 2), through improved transparency and traceability, and greater integration into global value chains for farmers, through increased competitiveness in international markets, potentially unlocking additional sources of income (Goal 8).

The DLT and blockchain landscape can be confusing because it is a unique combination of research in fields such as cryptography, consensus, game theory and distributed network technology, and is constantly changing. The majority of blockchain and DLT will operate in situations involving personal, private, company, government or otherwise sensitive data, therefore, security and privacy are challenges given the lack of best practices and standards. DLTs show much potential, but they require other technologies to be able to operate. This linkage and mutual dependency with other technologies necessitate a mutual reliance and interoperability between different DLTs and between DLTs and other technologies/systems.

BLOCKCHAIN/DLT OPPORTUNITIES	BLOCKCHAIN/DLT RISKS
» Traceable, transparent and secure and fully auditable information records e.g. financial systems and supply chain management; » Tamper-resistant and transparent systems facilitating record-keeping and promoting trust among participants; » Logistic and data efficiencies to convey information; » Empowers user control over information, e.g. identity management; » Can be deployed in smart contracts; » Decentralization and automation (assisted by smart contracts) of verification and approval processes to improve efficiency and productivity; and » Incentivizes (or discourages) certain human behaviours (e.g. saving energy, reducing CO_2 emissions) through programmable tokens.	» Potential infringements on human rights, freedoms and dignity; » Data privacy risks, e.g. in public blockchains; » Immutability of data if incorrect; » Uncertain legal framework, e.g. legal standing of smart contracts; » Cyber-security issues; » Criminal misuse, e.g. cryptocurrencies; » High cost of developing DLT; » High energy consumption, e.g. systems relying on proof-of-work; » Lack of accountability, e.g. permissionless systems; » Vulnerabilities in smart contracts if code is not properly audited; » Inappropriate handling of private keys, e.g. key custodianship; and » High demand of computing resources.

Role of standards for blockchain/DLT

The broad scope of application for blockchain and DLT and their range of impact means that there is a need for standards in the field, for example, in information security, privacy, compatibility and interoperability for any user or developer of the digital technology. Standard making is still relatively new for this digital technology and the standard landscape is uncluttered. A few SDOs have been predominately active in the field, including ANSI, DIN, IEEE, and ISO. IEEE was an early actor and has developed over 50 standards addressing the horizontal and vertical aspects of this frontier technology. ISO's Technical Committee (TC) 307 Blockchain and DLT is rapidly developing standards for the sector. The comprehensive review of standards at the international level identified standard making in blockchain/DLT broadly falls into the following four categories:

- Foundational
  - Terminology
  - Reference architecture
- Methods and approaches
  - Interoperability between different DLTs and between DLTs and other system components
  - Compatibility between technology and legal frameworks
  - Data format
  - Smart contracts
- Trustworthiness
  - Governance, security, privacy, and identity
- Use cases and applications
  - Repository of case studies

The benefits of standardization in the field are improved security, privacy, scalability and interoperability and enhanced governance. This could encourage the technology's widespread adoption, increase trust in the technology and stimulate greater innovation. However, the pool of experts with sufficient knowledge of DLT to participate in standardization is relatively limited, meaning inclusiveness in the standard-making process, whilst essential, is currently not being achieved. Women, people from developing countries and regions such as Africa and South America are underrepresented. Moreover, SDOs could consider taking into account structural limitations faced by low-income, developing countries in the standards they develop. SDOs can act as advocates of technology development that is responsive to different geographical, infrastructural and educational realities with the aim to eradicate barriers to participation and benefitting from new technologies. Use cases could include pertinent examples, such as that showcased by UN Women in which the IDbox "solar-powered device uses blockchain to create a unique digital identity and wallet in the absence of Internet or electricity using only a 2G mobile phone."[21] These types of low barriers to entry can be deployed in a variety of locations and settings, such as in humanitarian response. Furthermore, blockchain technology can have positive effects in promoting gender equality, for example, UN Women also reports that digital wallets have shown to provide displaced women with greater financial autonomy compared to physical money, which is oftentimes controlled by male family members.

Smart contracts are defined as a computer programme stored in a distributed ledger system wherein the outcome of any execution of the programme is recorded on the distributed ledger;[22] put simply, programmes stored on a blockchain that run when predetermined conditions are met. They are speedy and efficient because the contracts are digital and paperless, as well as being trustworthy and transparent as they involve no third party, are tamperproof and transactions are shared with participants. However, smart contracts have legal implications such as compatibility with existing legal frameworks, enforceability, language used, their legal standing, and use in automated and AI systems. ISO TC 307 on Blockchain and DLT is developing a suite of standards on smart contracts covering such topics as the technical aspects of smart contracts in blockchain and DLT systems, what smart contracts are and how they work, legally binding smart contracts and good practice in smart contract security. IEEE has also entered the standardization domain for smart contracts considering data formats for these legal contracts.

There are challenges for national lawmakers in developing legal frameworks applicable to DLT and blockchain, particularly in the financial services because the technology opens up cross-border activities and decentralized finance and the creation of new digital assets. Standards have a role in supporting national legal systems that seek to manage this new digital technology because international standards are transnational, being applicable in numerous jurisdictions. However, a balance is needed between a certain level of standards without hindering innovation. On the one hand, the lack of regulation limits the capacity of governments to cope with fraud, local regulatory compliance evasion, financing of illicit activities, scams and Ponzi schemes. On the other hand, it inhibits technology adoption and innovation, especially affecting entrepreneurs and start-ups which are often confronted with the uncertainty of incurring a legal problem.

Blockchain and DLT raises concerns, including criminal misuse, energy consumption, immutability as both a benefit and a risk, public safety, consumer protection, data protection and a lack of understanding by the general public. In addition, governance frameworks are needed for this digital technology as it impinges on privacy, identity, and data ownership and use (see Text Box 2). ISO TC 307 is developing guidelines for governance that set out a series of principles for good governance of blockchain and DLT systems. IEEE committees are looking into standards that are required for blockchain and DLT applications in energy, healthcare, agriculture, IoT and automotive sectors with a particular focus on building trustworthy end-to-end devices and systems.

Text Box 2 – Example international standard addressing privacy in DLT

Privacy and personally identifiable information (PII) protection issues are widely considered as a major barrier for the adoption of blockchain and DLT-based solutions. ISO/TR 23244:2020 Blockchain and distributed ledger technologies — Privacy and personally identifiable information protection considerations provides an overview of the issues and practical concerns related to privacy and PII protection identifying and assessing known privacy-related risks and the way to mitigate them, as well as the privacy-enhancing potential of blockchain and DLT.

Standardization efforts in blockchain and DLT are rapidly developing, helping to shape the digital technologies and encouraging innovation and user acceptance, however, the scale and diversity of the digital technologies means that standards-makers face the twin problems of the technology outpacing standards development and lack of adoption. Another risk related to standardization is the uneven progress reported across different industries. The "Distributed Ledger and Blockchain Technology Study Group" of the ANSI Accredited Standards Committee X9 notes that the needs of some economic sectors might not be adequately considered. Certainly, specialized standardization work would be needed according to the knowledge areas and legal requirements of different industries.

The many opportunities of blockchain are not without sustainability challenges. For example, blockchain has the capacity to change the way goods and services are transacted, however, its rapid growth fails to consider its carbon footprint. Standards can promote environmental balance and non-abuse of this technology for the planet and its inhabitants. Standards can also play a key role in

[21] https://blogs.worldbank.org/psd/can-blockchain-disrupt-gender-inequality

[22] ISO TC 307

defining proper energy consumption, particularly during the blockchain mining process, leading it to become a sustainable technology that ensures no harm to the planet. While the benefits will be seen by experience, the more blockchain advances, the more complex it will become for humans to fully understand its consequences. Standards can promote understanding of the effects of the technology, ultimately leading to sustainability for all.

INTERNET OF THINGS (IOT)

About the technology

The UNIDO Industrial Development Report 2020 defines the Internet of Things (IoT) as the next iteration of the Internet, where information and data are no longer predominantly generated and processed by humans (as most data created so far have been) but by interconnected smart objects, embedded in sensors and miniature computers that sense their environment, process data and engage in machine-to-machine (M2M) communication.

IoT relies on interconnections through the Internet's network of devices, machinery and objects, each uniquely addressable based on standard communication protocols. Today, there are more connected devices than people connected to the Internet. IoT is not a single technology but a complex ecosystem using various technologies applied in diverse settings. IoT applications span all major economic sectors including health, education, agriculture, transport, manufacturing and utilities.

IoT is becoming a common part of everyday life in G20 countries and beyond. The IoT global market value was USD 308.97 billion in 2020, a 23.1% increase on 2019 figures, and the Asia-Pacific region generated USD 120.85 billion because of the rapid adoption of IoT in developing countries, such as India.[23] Part of the underlying infrastructure of the IoT is M2M communication, i.e. SIM cards embedded in machines,[24] such as automobiles or sensors, which allow communication between devices.[25] In 2017, the United States had over 10 times the quantity of M2M SIM cards per 100 people compared to India, while China had 44% of M2M subscriptions, the largest share worldwide.[26]

In terms of achieving inclusive and sustainable industrial development, IoT offers numerous possibilities. For instance, UNIDO's Sustainable Technology Promotion Platform (STePP) has harnessed IoT to increase geothermal energy production capacities in Kenya, thus reducing dependence on fossil fuels.

Role of standards for IoT

Standardization activity is high in the IoT field. It is a significant prerequisite to achieving interoperability between products and between different solutions, applications and domains. Giving rise to interconnected devices is the intention of IoT. The standards scene is complicated. There is a bewildering list of standards and standard-making organizations engaged in standards in the IoT landscape. The comprehensive review of standards at the international level identified standard making in IoT broadly falls into three categories:

- Foundational
  - Vocabulary
  - Architecture
- Method & approaches
  - Interoperability
  - Characteristics of IoT systems
  - Sensors, applications and domains
- Trustworthiness
  - Trust, identity, privacy, protection, safety, and security

Standardization of vocabulary, terms and definitions in the realm of IoT can reduce the level of ambiguity and promote understanding. International standards have an important role to play in establishing a single, homogenous body of terminology in a field, as shown in Text Box 3.

[23] Fortune Business Insights - Market Insights IoT 2021
[24] Excluding consumer electronics
[25] OECD Toolkit for Measuring the Digital Economy, 2018
[26] Groupe Spéciale Mobile Association (GSMA) tracks the number of M2M subscriptions worldwide.

Text Box 3 – Internet of Things vocabulary standard[27]

The international standard IEC 60050-741 provides a definition of Internet of Things, along with related terms and definitions, as an infrastructure of interconnected entities, people, systems and information resources together with services which processes and reacts to information from the physical world and virtual world. This definition is to be used by all IEC Technical Committees.

Standardization for architectures for common service frameworks can help eliminate IoT silos. Interoperability in IoT has to be considered at different layers from component, to communication, information, function and business layers, i.e. architectural frameworks. Many IoT applications are deployed in silos, e.g. one application using one communication network to interact with devices or sensors. IoT silos impede operational scaling or resource reuse. Standards can play a key role in encouraging a common language among machines' systems, ultimately leading to interoperability as a common language among machines leads to proper optimizations. As the IoT market matures, IoT applications will employ distributed architectures. All require new and standardized enablers. One attempt to address the lack of interoperability in industrial IoT (IIoT) is the collaboration between Industrial Internet Consortium (IIC) and oneM2M (see Text Box 4). IoT in different sectors are being rapidly developed by big tech companies, therefore, standards can act as a fair trader to avoid monopolies and provide opportunities for all. IoT is advancing through niches, creating silos, closed ecosystems and avoiding proper integration. Standards can promote interoperability, leading to cost reduction and ultimately providing opportunities for emerging developers.

Text Box 4 – Collaboration on IoT architecture for interoperability[28]

IIC is a membership organization that seeks to accelerate the adoption of IIoT by enabling trustworthy industrial Internet systems and has a testbed programme for industrial innovation for new technologies, applications, products, processes and services. oneM2M brings together several major regional ICT SDOs, such as ARIB (Japan), ATIS (North America) and TSDSI (India) to collaborate and develop and manage technical standards to enable IoT solutions. IIC and oneM2M have different origins and approaches in addressing IoT and IIoT architectural challenges, but they share common objectives in helping industries achieve interoperability and reusability and are committed to develop common standards for a common service layer applicable to different industrial segments.

In 2017, IIC and oneM2M announced their agreement to work together to contribute to the creation and development of the Industrial Internet. Under this agreement, the organizations will promote the digital economy by preventing fragmentation and by harmonizing various aspects in the IIoT. Joint activities between the IIC and the oneM2M will include:

- Collaboration, review and two-way feedback pertaining to IoT use cases, requirements and reference architectures;
- Feedback to oneM2M standards from IIC testbeds and interoperability events;
- Feedback from oneM2M to IIC Industrial Internet Reference Architecture; and
- Joint workshops, showcases and interoperability events.

[27] https://webstore.iec.ch/publication/66698

[28] https://www.iiconsortium.org/press-room/09-27-17.htm

A crucial factor driving the IoT market growth is the increasing adoption of smart sensors. Smart sensors measure the external environment and physical inputs, e.g. temperature, light and pressure, and convert them into raw data stored digitally for analyzing the processes. With the rapid technological development of sensors, wireless sensor networks (WSNs) will become the key technology for IoT. IEC notes[29] that IoT standard making for WSNs is characterized by disunity with a lack of coordination between SDOs, incompatible as different SDOs develop different unique standards and divergent since standards are developed behind the curve of application development. A major prerequisite in achieving the interoperability of smart sensors such as WSNs, not only between products of different vendors, but also between different solutions, applications and domains, is standardization. For example, IEEE 802.5.14 is the most relevant communication standard for the WSN and ISO/IEC JTC 1 subcommittee (SC 31) is one of the major standardization drivers with its ISO/IEC 18000 series of standards. The development of overarching international standards would allow for greater cross-border trade and production, as well as an improved common technical understanding.

Standards are leveraging IoT technologies to create more efficient, responsive, make-to-order systems. An important feature of IoT is data management. Vast amounts of data and information are collected by all Internet-connected devices raising cybersecurity and privacy issues as the technology is vulnerable to attacks. Standards can optimize the response to threats and play a key role to provide protection to data, ultimately leading to a safer and more secure ecosystem. Cyber-risks have more than quadrupled since 2002.[30] SDOs such as the National Institute of Standards and Technology (NIST) cybersecurity programme for IoT supports the development and application of standards, guidelines and related tools to improve the cybersecurity of connected devices. Furthermore, the more interconnected devices become, the more in demand and overextended IoT cybersecurity experts will also become. By promoting an understanding of the field, standards can aid in attracting more experts and facilitate its expansion.

As IoT systems get more integrated and complex, issues related to trustworthiness, i.e. privacy, identity, trust, security, protection and safety (TIPPSS), become more important to users. Standards can address privacy issues on personal data and accountability in data usage and lack of transparency that could negatively impact personal freedoms and infringe upon human rights. IEEE is focusing on critical aspects of TIPPSS in IoT, for example, the project IEEE P2933 on standards for Clinical Internet of Things (IoT) Data and Device Interoperability with TIPPSS.

IoT has numerous applications. IoT makes factories more intelligent, safer and more environmentally sustainable. IoT connects industry to a new range of smart manufacturing solutions to run the production, streamline product development and manufacturing processes (see Case Study 3). Homes have smart appliances to become smart homes and integrated, smart, sustainable cities are being invested in, particularly in the EU, and smart infrastructure becomes achievable with IoT. For example, smart city and digital technology standards developed by ITU-T Study Group 20 Internet of Things and Smart Cities and Communities help cities ensure their investments in digital technologies deliver maximum positive results for their citizens and businesses and also assist cities in harnessing these new technologies to implement SDGs. Another example application of IoT is the UNIDO project, in partnership with the Government of Japan, to improve the efficiency of geothermal electricity production in the Great Rift Valley Region in East Africa. The project aims to install sensors in power generators and turbines to detect temperature and vibrations, and the data extracted from the process then will be computer-analyzed to increase the efficiency of the geothermal power plants in the region. The technology allows companies to remotely monitor and manage the production and distribution of energy in real time. The technology will also improve the plants' operational safety, as geothermal power plants are usually built in earthquake-prone areas. The possibility of managing the plants remotely also has clear advantages for avoiding employees' exposure to chemicals often released by geothermal power plants.

In spite of the promises of IoT systems, earlier in 2021, the European Parliament's Policy Department for Citizens' Rights and Constitutional Affairs published a briefing outlining the dangers of IoT-related abuses, which stipulates that women face an increased risk of being affected by gender-based violence and "tech abuse" enabled or facilitated by IoT. Ethical considerations are already being addressed by standards, especially over data protection, but there is room for SDOs to mainstream further approaches aimed at counteracting and preventing possibilities for misuse and, arguably more importantly, abuse. Provisions pertaining to the usability and also the sale of IoT products need to be gender-responsive. For example, the marketing of digital or digitally enhanced products is oftentimes geared towards men, and it has been noted that it is mostly men who make related purchasing decisions and control the installation/setup and maintenance of the new technology.[31] As pointed out in a European Parliament briefing, IoT devices often require one designated administrator as well as password protection; this type of control increases dependency and the vulnerability of women and girls in the home. Smart door locks, for instance, are at risk of being abused by controlling, and effectively granting or denying, entry and exit to the home.

Digital twins help transform the physical assets of industries into a virtual representation and aids in controlling, examining and viewing the operations based on the digital platform. For example, ISO/IEC JTC 1/SC 41 Internet of things and digital twin has published 32 standards in the IoT landscape on IoT architecture, interoperability and applications, and has working groups specifically dedicated to digital twins and their applications.

[29] IEC White Paper IoT – Wireless Sensor Network 2019

[30] The Economist June 19th 2021

[31] https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/690358/IPOL_BRI(2021)690358_EN.pdf

Case Study 3 – Smart manufacturing in the automotive industry – Colombia

From 2019 to 2020, Solocauchos S.A.S., a Tier 2 automotive sector supplier in Colombia, participated in the World Class Competitor project supplier upgrading activity. This provided tools and methodologies to increase productivity and quality of participating companies and contributed to SDG 9—delivering innovation in industry and promoting prosperity. Over 2 years, the company received coaching and training on Lean Manufacturing tools, Six Sigma, Theory of Constraints and quality management approaches.

Solocauchos developed its own real-time flow and production control software called SWRF-DRO3 (basic unit). The unit receives real-time data from the production line to determine the process status and monitor the production cycle. The software was developed to provide real-time information in order to increase productivity, profitability and innovation by the integration of knowledge on Overall Equipment Effectiveness (OEE), IoT, and E-finance, i.e. link between production systems measurement technology and enterprise financial information.

Solocauchos' participation in UNIDO activities resulted in the enterprise increasing its productivity and making estimated production costs savings in the first year of USD 35,300. Further analysis in 2020 revealed an additional USD 10,000 savings in new processes improvements. The company's software facilitates automation, digitalization and better control of process and resources, and has been successfully sold to and adopted by 2 other automotive enterprises.

IoT developments are outpacing standardization and the lack of adoption of standards by IoT applications are issues for the sector. Numerous standards have been developed for IoT by a range of international SDOs and international bodies. The lack of harmonization is an impediment to IoT growth affecting the reusability and interconnectedness of things in the IoT ecosystem, and increased coordination is needed between SDOs to rectify this problem. Increased coordination is required between standard-making organizations to achieve harmonization and reduce divergence amongst standards, and increase the pace of standardization for the IOT domain.

ROBOTICS

About the technology

Eurostat has defined the robot as "a machine, programmed by a computer, capable of carrying out a series of more or less complex actions automatically." Robots can be industrial robots or service robots. An industrial robot is an automatically controlled, reprogrammable and multipurpose manipulator in three or more axes, either fixed in place or mobile, used in industrial applications such as manufacturing processes (welding, painting and cutting) or handling processes (depositing, assembling, sorting and packing). A service robot is a machine that has a degree of autonomy and operates complex and dynamic interactions and coordination with persons, objects and other devices (when used, for example, for cleaning, surveillance or transportation).

The field of robotics is complex, diverse and rapidly evolving; for example, a recent development is soft robotics which takes inspirations from living organisms to make flexible robots with highly compliant materials. Robots operate in many different settings and have distinct functions such as industrial robots; service robots, including medical ones; robots in logistics; field robots, e.g. agriculture; and personal and domestic robots, e.g. care robots and vacuum cleaners.

In 2019, 2.7 million industrial robots operated in factories worldwide—an increase of 12% from 2018—equivalent to a worldwide robot density in manufacturing of 113 robots/10,000 employees.[32] Sixty-seven per cent of industrial robots operate in three sectors: automotive, electrical and electronics and metal industry. The sales value of the professional service robot sector increased by 32% to USD 11.2 billion worldwide (2018–2019) and medical robotics accounted for 47% of this sector's turnover in 2019. The COVID-19 pandemic created high demand for robotic solutions for tasks such as disinfection, logistics in factories and warehouses and home delivery.

Collaborative robotics is when automatically operated robot systems share the same workspace with humans and refers to a system or application rather than a particular type or brand of robot. The adoption of human–robot collaboration is on the rise and installations grew by 11% in 2019, however, the market is still in its infancy at only 4.8% of the total industrial robot market.[33] Asia remains the strongest market for industrial robots with China being the region's largest adopter, and India has doubled the number of industrial robots operating in the country's factories in five years to 26,300 units.[34]

Role of standards for robotics

International standardization in robotics became more concentrated as robots began to increasingly possess a degree of autonomy. ISO set up its first committee in 1983 on "robots for manufacturing environment" and

[32] World Robotics Report 2020
[33] International Federation of Robotics World Robotics Report 2020
[34] https://ifr.org/ifr-press-releases/news/record-2.7-million-robots-work-in-factories-around-the-globe

upgraded the committee in 2016 to cover the broader field of robotics.[35] The ISO committee TC 299 on Robotics has published 26 standards with a further 11 under development.[36] The comprehensive review of standards at the international level identified standard making in robotics occurs in the following categories:

- Foundational
  - Vocabulary
- Method and approaches
  - Performance and testing
  - Health and safety
  - Security
  - Management
- Trustworthiness
- Ethics

The expansion of traditional caged robots capable of handling all payloads quickly and precisely to new collaborative robots that work safely alongside humans, fully integrated into workbenches, raises issues of protecting people from injury and their employment being economically devalued. Standardization around the parameters under which humans and robots can work together is increasingly important as more collaborative robotics are developed. Standards can also facilitate the common understanding of AI systems among all affected actors, leading to trust of the technology and extending to their outputs, decisions and recommendations and general ecosystem, thereby enhancing the human–machine relationship. While the focus is mainly on robots understanding humans, there is room for humans to understand robots as robots can be better utilized when they are designed to work in partnership with humans, and partnership works when there is mutual understanding. Standards can play a critical role in facilitating human–machine understanding, thus contributing to trust, increased efficiency and productivity in organizations. Closer interaction between human systems and robotic systems will drive the demand for standards on safety management, privacy, identity and independence as more complex and intuitive AI is integrated into robotics. For example, the international standard ISO/TS 15066 gives specific, data-driven safety guidance needed to evaluate and control risks when robots work alongside humans in collaborative working spaces.

As the field of robotics evolves, standardization efforts will need to be broadened to support the sector's development. Standards can ensure stakeholder concerns about service robots, e.g. care robots, or robots in medical settings, are taken into account. For example, IEC has published standards on the basic safety and performance of medical robots, however, medical robots are diverse in their form and function, such as robotic exoskeletons that provide external support and muscle training for rehabilitation, and appropriate standards are needed. Autonomous Internet-connected robots of all types will challenge current rules on data protection and privacy, particularly where users are unaware of how much and for what purpose data are being collected. Ensuring the safety of data always remains a major concern when using robotic solutions. There is currently no clarity on the ownership of the data the robot has, and disputes arise from whether the owner of the data is the end-user, the robot manufacturer, or its software provider. Standards can facilitate a path to implement proper data management, ultimately leading to trust. The IEEE Standards Association global initiative on the ethics of autonomous and intelligent systems considers some of these data protection issues. Another issue related to data is that data collectors often do not foresee the uses of the data before or while collecting it, only realizing its potential uses once is has already been collected at scale. It is important for standards to be developed regarding clear intimation of the data's purposes, and for those stated purposes to not later be expanded upon without the data provider's knowledge or consent.

[35] https://committee.iso.org/home/tc299
[36] https://www.iso.org/committee/5915511.html

Standards can also ensure ethical and cultural aspects are considered to make robots acceptable to society, particularly when automation eliminates jobs. The OECD Policy Brief on the Future of Work – Going Digital: The Future of Work for Women notes that some large industries with high shares of women are at a high average risk of automation, though summing across all industries, the average risk of automation is similar for men and women.[37] It is important for SDOs to be aware of any gender-specific constraints (e.g. in historically women-dominated occupations that can be more easily automated) and ensure concerns of adequate representation of women generally, and vulnerable workers specifically, are reflected in standards to minimize detrimental effects of the technology on certain members of society, thus encouraging inclusiveness.

Although standardization is only just beginning to address trustworthiness, IEEE has a project developing an ontological standard for ethically driven robotics and automation systems. Standards and guides are being developed on subjects such as:

- Safety issues in the increasingly diverse range of human/robotic interface situations;
- Integration of robot's autonomous features to other digital technologies particularly AI and associated risk management, and cyber security and privacy issues;
- Application of robots in diverse settings such as medical and care services;
- Environmental impact of robots, such as material selection to allow recycling, energy use in operation and disposal; and
- Trustworthiness issues linked to the cultural, ethical and social aspects of deploying robots and human rights issues as robots pervade peoples' lives.

The benefits of standards in the sector are to increase safety and protect humans, to specify technological aspects such as performance and recyclability and to contribute to cost reduction and innovation as well as to engage with diverse stakeholders to take account of their views as robots extend into different domains in society. However, advancement in robotics with AI and ML mean standardization is being outpaced by the technological developments' resulting inefficiencies from a lack of compatibility and divergence with basic parameters such as safety.

As the main technology for operability of robotics is AI, standards can play a key role in the development of reliable AI that will define proper management on bias reduction in AI systems, ultimately leading to inclusiveness. Development of robots has the capacity to offer a better life for those that are in need, the challenge lies in leaving no one behind. Standards can act as an enabler for robotics to benefit people, planet and prosperity, thereby also contributing to inclusiveness.

[37]https://www.oecd.org/employment/Going-Digital-the-Future-of-Work-for-Women.pdf

3D PRINTING

About the technology

Eurostat defines 3D printing/additive manufacturing as "…the use of special printers to create three dimensional physical objects from 3D model data by adding layer upon layer through material extrusion, directed energy deposition, material jetting, binder jetting, sheet lamination, vat polymerization and powder bed fusion. Additive manufacturing is contrasted with subtractive manufacturing methods, which use moulds or rotating milling cutters to remove material from a solid block of material."

3D printing is a popular term that refers to a broad range of additive manufacturing (AM)[38] techniques. AM is the process whereby a material is usually layered to create solid objects from computer-aided design (CAD) models or 3D scans under computer control. The AM sector is relatively young, and will develop and mature over time as knowledge of the technology grows. Additive manufacturing technology (AMT) is primarily used in the industrial and business sector, followed by electronic goods, motor vehicles and medical devices. Wohlers Report 2021 found the AM industry expanded by 7.5% to nearly USD 12.8 billion in 2020. Due to the pandemic, growth was down considerably compared to the average growth of 27.4% per annum over the previous ten years.[39]

AM has a smaller environmental footprint than traditional manufacturing and contributes to circular economy aims, reducing material usage and waste. Instead of milling a workpiece from a solid block of material, an AM machine can read CAD files to determine the time and material needed to build up 3D structures from fine powders or liquids, reducing wastage and saving time. AM allows for more fluid product development and design because it permits the manufacture of prototypes and parts on-demand, allowing the freedom to redesign and innovate without significant penalties of time and material costs.

AM is an enabling technology. It produces parts that may not have been feasible with existing technology, creating endless possibilities for innovation. For example, regular and customized hearing aid shells, dental implants and prosthetic limbs have all been successfully produced by AMT. AM also enables decentralized manufacturing of consumer goods eliminating unnecessary transportation and multiply assembly processes. This could potentially impact the locations of manufacturing facilities, rebuilding lost manufacturing bases—such as those lost in Europe—or decentralizing and localizing manufacturing close to population centers, reducing transportation costs and climate change impacts.

3D printing may be especially useful in providing cheap and durable construction materials for the housing sector, as well as reducing industrial waste, thus addressing Goal 9 of the 2030 Agenda to "build resilient infrastructure, promote inclusive and sustainable industrialization and foster innovation." It also has great potential to meet needs in the medical manufacturing sector amidst the COVID-19 pandemic, especially for production of personal protective equipment.

[38] 3D printing and AM are used interchangeably.
[39] Wohlers Report 2021

Role of standards for 3D printing

One of the stumbling blocks to the technology's wider application is the lack of supporting standards. International standardization has been slow to develop for AMT because interest in standards has been limited, which has led to a proliferation in national standards. American Society for Testing and Materials (ASTM) International created a committee (F42) to create standards for AMT in 2009 and ISO entered the field in 2011 establishing TC 261 on AM. The EU project for Support Action for Standardisation in Additive Manufacturing (SASAM) delivered a roadmap for standardization activities for AM in 2013 that included standards for process stability, product quality, materials used and productivity.[40] As in most standardization activities, women are largely underrepresented in AM-standardization activities as well as in the industry in general (similarly as in robotics and other tech sectors). While professional women's associations have been established over the last few years, the gender gap in 3D printing can in part be attributed to a lack of girls and women in STEM fields, with a lack of female role models, and limited industry awareness of underrepresentation being problematic. It is important for SDOs to consider underrepresentation of women in the industry when developing standards for AM and to ensure standards developed account for women, thus encouraging inclusiveness.

The plethora of standards means there is a need for international standards for quality, materials, testing, safety and performance to guarantee a level of reproducibility in AMT and to contribute to innovation in the field. To avoid work duplication, or worse, the development of conflicting/competing standards resulting in market confusion, ISO and ASTM established a working framework as part of the Partner Standards Development Organization (PSDO) cooperation agreement to develop standards for AM in a variety of industry-specific applications, settings and conditions. The collaboration in ISO TC 261 agreed a common structure in AM standards and has resulted in 19 international standards being published with a further 37 under development including standards for AM for aerospace and construction and environmental, and health and safety requirements for specific AM machines. The comprehensive review of standards at the international level identified standard making in the 3D printing field occurs in the following categories:

- Foundational
  - General concepts
  - Fundamentals and vocabularies
- Method and approaches
  - Common requirements or generally applicable (e.g data format, design guidelines, hardware and software, applications) to most types of AM materials, processes, and applications
  - Testing
  - Quality and safety
- Category standards
  - Specific to a feedstock material e.g. metal powders, process/equipment (e.g. powder bed fusion) or finished part (e.g. mechanical test methods)
- Specialized standards
  - Specific to a material (e.g. titanium alloy powder), process (e.g. powder bed fusion with nylon), or application

Notably, unlike other digital technologies such as AI, big data, blockchain and IoT, standards in AM are not being developed in the trustworthiness category. This is because AM technology does not as yet have the potential to infringe on human rights, freedoms or dignity. However, the increase in available design files that can be easily and often freely downloaded and 3D printed poses a risk to intellectual property (IP). In addition, there is a lack

[40] European Commission Digital Transformation Monitor: The disruptive nature of 3D printing, 2017

of clarity in many legal areas in AM, including patents, copyrights and trademarks and printing of items used illegally.

AM biomedical systems are capable of printing cells, proteins and organs and research is underway in bio-printing of skins, organs, bone and cartilage. Standards-makers have entered the AM biomedical field, for example, IEEE has projects on standards for In Vivo Evaluation of 3D Printed Polymeric Scaffolds in Bone Defects and Artificial Joint Implant Design Modelling for Medical 3D Printing. This new field for AMT raises many issues such as safety and reliability, acceptance and ethical issues for medicine.

Further safety concerns relate to certain types of materials used in AM that can release particulates and other harmful chemicals into the air, while others are flammable or combustible. Standards will help to shape the industry and ensure that AM processes, materials and technologies are safe and reliable as well as ensure compatibility of AMTs, impacting the well-being of people and the planet. AM can shorten development cycles of weapons, decrease production costs, and simplify witting and unwitting transfer of military hardware and know-how. This applies to every conceivable weapon category, from small arms to weapons of mass destruction. Standards will play a critical role to frame the scope of these developments for the proper use of AM technology and to avoid harming people and the planet, ultimately increasing safety. An AM security concern relates to the fact that 3D printers include computers and run software that could be vulnerable to security issues that bad actors could exploit. To mitigate this issue, standards can play an important role for 3D printing vendors to make secure coding and design a core part of their development process.

From a sustainable development standpoint, 3D printing can also be deployed for the construction of affordable housing in developing countries as well as for the easy provision of personal protective equipment to combat COVID-19. The adoption of AM is leading to shorter and more localized and collaborative value chains. Standards have the potential to offer sustainable benefits by improving resource efficiency in production and use phases as manufacturing processes and products can be redesigned for AM. Further contributing to sustainability, the capacity of AM to create extended product life can benefit from standardization through sustainable socio-economic patterns such as stronger person–product affinities and closer relationships between producers and consumers. AM also has the capacity to be processed in a way that is energy saving and optimizes the use of materials. In this regard, standards can play a key role in defining proper by-products during the printing process, leading AM to become a sustainable technology that ensures no harm to the environment and the planet.

Standards can also help guarantee a level of reproducibility, and give business and manufacturers the much-needed quality assurance in AM processes, materials and technologies. The quality and durability of surface finish and mechanical properties are of concern, particularly for the usage in final or functional parts manufacturing, and standardization has an important role to play in providing users with the necessary standards for a variety of industry-specific application. For example, F3122 Guide for Evaluating Mechanical Properties of Metal Materials Made via AM Processes.

AM industry is growing rapidly, helped in part by a big fall in the price of AMT increasing the accessibility of the digital technology to enterprises, and the innovation in uses for the technology. Standardization efforts have been dispersed and uncoordinated and late to the market, however, standards-makers have an opportunity to help AM producers and consumers by providing a common set of standards that benefits the market by specifying requirements for such areas as quality, performance, test and inspection methods, environment, health and safety, and design and data format. Better coordination between SDOs will prevent duplication of efforts and the development of standards to provide the technical rigor for AM and delivery consistency, and therefore, confidence in the technology for the market.

UNMANNED AIRCRAFT SYSTEMS

About the technology

Unmanned aircraft systems (UAS)[41] are guided remotely or autonomously and vary greatly in size, capabilities and cost. UAS are composed of an unmanned autonomous vehicle (UAV), commonly referred to as a *drone*, a ground-based controller of the UAV and the system that connects the two. The global commercial drone market size was valued at USD 13.4 billion in 2020, with an estimated 7 million flying in American skies in 2020. The most extensive use is in China and Japan.[42]

The application of UAS has expanded into a wide range of uses, such as detecting forest fires, monitoring traffic, disinfecting areas, delivering parcels and surveying agricultural land. They can be integrated with AI and ML to understand their surroundings better and give analytical feedback and real-time, data-driven decision-making ability to their users. AI-powered vehicles also enable users to collaborate and access information from other drones; coupling this with predictive learning software means faster data analysis, which enables a variety of actions to be taken. The advent of 5G and the integration of cloud computing technology with drone technology is expected to increase growth in the commercial drone market with the global drone market size forecasted to grow to USD 42.8 billion by 2025, according to Drone Market Report 2020–2025.

Role of standards for UAS

The use of UAS is more frequently and widely distributed, causing growing concerns about their uncontrolled use in urban areas and near airports. This poses safety issues therefore, these new airspace users—civil, commercial and leisure—need to be integrated into the airspace not only to ensure the safe operation and prevention of harm to people, but also to realize this growing industry's potential. There is a need to develop a traffic management system for UAS and define how it will work technically and

[41] In this publication, the terms UAS and drones are used interchangeably.
[42] Global Drone Market Report 2020-2025

institutionally, however, regulations are inconsistent or lacking. Standards can facilitate the structure of such traffic management system, thereby contributing to safety and security. Some countries, such as France and the United Kingdom, have clearly defined laws that stipulate such things as line-of-sight operation, non-urban use, drone weight limits and often a flight altitude ceiling. Other countries, in the absence of regulations, have banned drone use. Standardization could play an important role where there is a lack of regulation and also in support of existing regulations developed by national Civil Aviation Authorities (CAA).

The comprehensive review of standards at the international level identified standard making for UAS occurs in the following categories:

- Foundational
  - Terminology
- Method and approaches
  - Health and safety
  - Air space sharing and coordination
  - Quality
  - Testing
  - Training
  - Remote identification

The low level of existing standardization and the complexities of sophisticated, varied and incompatible UAS present a significant challenge in standards development. Most of the standardization activity has concentrated on the technical aspects of UAS with some attention to specific operational situations and the training of drone operators. ISO TC 20 SC 16 on Unmanned aircraft systems has published 5 standards with a further 25 under development on topics such as UAS classification, design, manufacture, operation, including traffic management and training of drone users, maintenance and safety management (see Text Box 5). IEEE standardization efforts have focused on drone application framework in standards that specify Interface Requirements and Performance Characteristics of Payload Devices in Drones (IEEE P1936.1 and IEEE P1937.1).

Text Box 5 – Safe operation of unmanned aircraft systems standard

The ISO21384-3, *Unmanned aircraft systems – Part 3: Operational procedures* - standard specifies internationally agreed and accepted requirements for safe commercial UAS operations and applies to all commercial UAS regardless of size, categorization, application or location and represents the international best practice.

The ever-increasing range of applications for UAS means that standards are required to bring about a globally harmonized airspace for routine UAS access that will increase the commercial market while maintaining safety and increasing airspace efficiency. There is a lack of standardization activity concerning the use of UAS and their impacts on privacy issues and potential infringements of people's rights through the misuse of drones to monitor and collect data. Standardization can mitigate this risk, resulting in a more secure environment. Moreover, despite the increase in production at different scales, still today there are no international supply chain regulations. Security and privacy remain issues as a result of certain countries monopolizing the production of UAS. Standards can help to ensure fair and trustful systems used in UAS. The increase in autonomous vehicle production and its accessibility raises the risk of potential targeted attacks if leaks in their security are not well managed. This technology integrated with AI can better understand their surroundings, map areas accurately, track and monitor the movement of specific objects, including people, as well as offer precise analytical feedback. Therefore, there is a need to develop standards in trustworthiness for UAS, particularly to protect human rights and privacy.

While the market for consumer drones is expanding, it has been observed that women are once more starkly underrepresented and underserved when it comes to skills building and other training as well as engaging with the community of drone professionals. UAS are largely marketed towards men, and aspiring girl and women drone pilots would benefit from more female role models. It is vital for SDOs and educators to ensure that girls and women are represented and encouraged as well as adequately capacitated to pursue careers in this field.

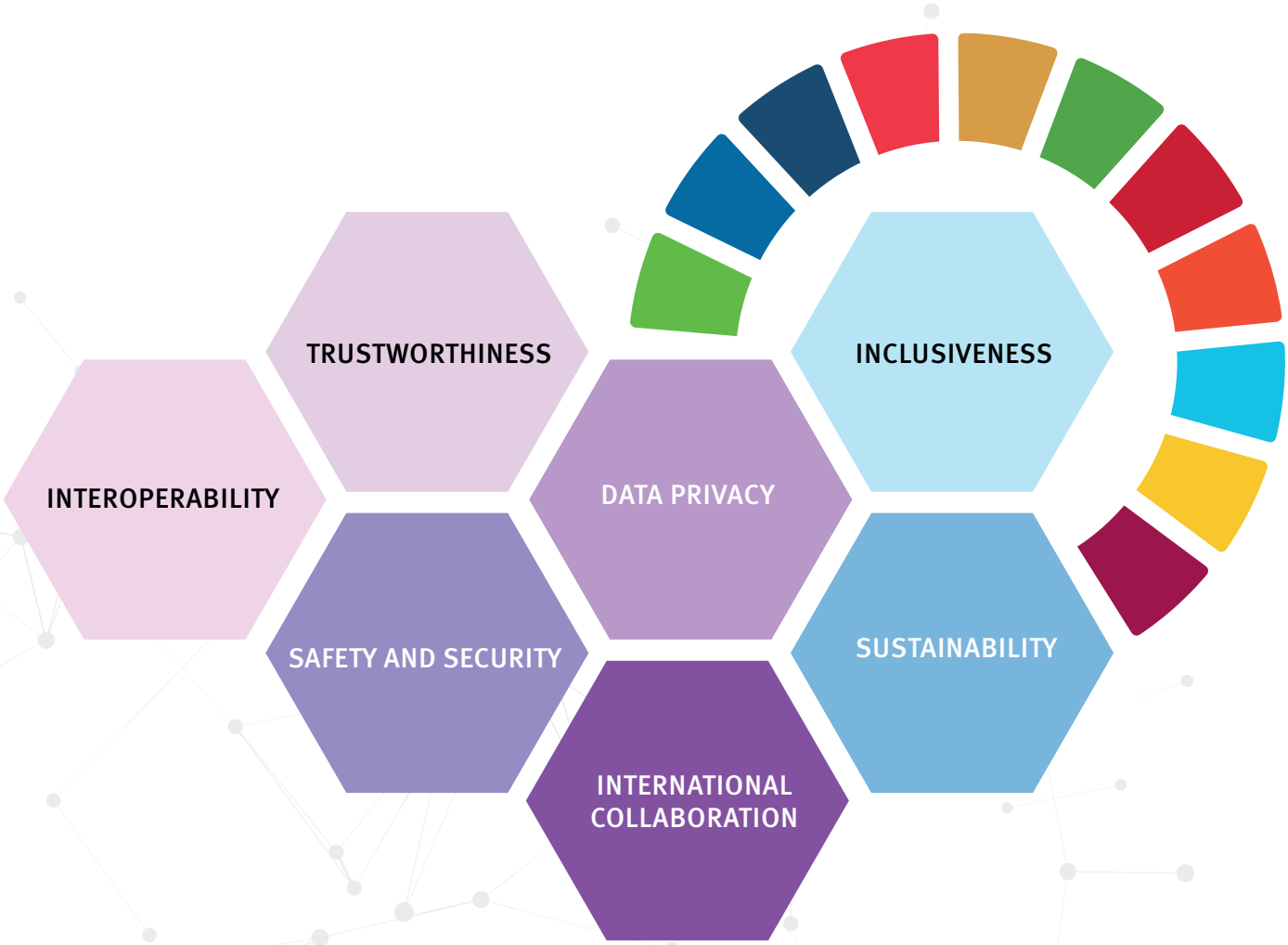
PART 4: **PRINCIPLES**

PRINCIPLES FOR STANDARDS IN DIGITAL TRANSFORMATION

The rapid and extensive adoption of digital technologies and their far-reaching pervasive impact on people, their prosperity and the planet suggest a core set of distinct principles is needed to guide standards developed for digital transformation governance. Standards that account for these principles contribute to the integral process of risk management, helping to avoid undesired outcomes associated with digital technologies while ensuring the technologies achieve their functional goals, benefitting people and the planet.

The comprehensive review undertaken of the current developed digital-related standards and SDO committee activities in the digital space, particularly for the seven big digital technologies of the 4IR, identified the following seven principles for standards to be placed in the center of standard making:

- Trustworthiness,
- Inclusiveness,
- Sustainability,
- Interoperability,
- Safety and security,
- Data privacy, and
- International collaboration.



The principles relate to the impacts of new technologies in the digital era and are based on the nature and internal mechanism of standardization. They cover notable concerns about the complex impacts of new technologies on people and the planet, in terms of well-being and ethics, as well as the key factors emerging from the evolving discussions about what should be considered in standard making in the context of digital transformation.

It can be observed that many standards related to new technologies address issues of productivity, *interoperability*, and *safety and security*. While issues like *sustainability, inclusiveness,* and *trustworthiness* are also sometimes addressed, the cases are the exception rather than the rule. There is potential to upscale these efforts in view of achieving sustainable development. Standardization can play a key role in digital transformation governance and should, therefore, include considerations in line with the suggested principles.

Data privacy is an emerging topic of global interest where standards can play a key role.

All these efforts cannot be made in isolation. *International collaboration* is key to strengthening the role of standards in digital transformation governance and has a truly global impact on sustainable development.

TRUSTWORTHINESS

Trustworthiness encompasses the full range of topics at the cutting edge between 4IR technology and humans, their rights and society. It encompasses human rights and the characteristics of accountability, transparency, robustness, equity, privacy, and ethical and lawful use of technology. A key component of trustworthiness is how ethical concerns raised by digital technologies are handled.

Trustworthiness addresses digital technology and its impacts in the widest societal context rather than a narrow technical one. It is particularly relevant to AI and big data (see Text Box 6), blockchain/DLT and IoT. It captures the interface between humans and new technology in its broadest way. Not all digital technologies have the same impact on humans. For example, drones for remote physical surveillance and monitoring utilizing facial recognition CCTV cameras raise civil rights issues. The scope of impact depends on the technology type and its application, therefore, the application of the trustworthiness principle will vary.

As a result of their impacts on humans, trustworthiness issues are increasingly being considered in standardization. Trustworthiness-oriented standards set out guidance on best practices for managing, controlling and using technology to provide a trustworthiness framework. However, the voluntary nature of standards means that regulators have an essential role in setting the legal framework and appropriate laws to protect fundamental human rights and make the technology human-centered.

Achieving trustworthy digital technologies requires technology-related ethical issues to be addressed. Ethics is set in a cultural context and framed by society and the laws that govern that society. Concerns vary depending on the stakeholder group, the risks and impacts of the technology and who has responsibility for the technology in operation. For example, if technology fails, questions arise regarding who or what monitors, adapts or interrupts its process, and whether it is another system or a human being. Standards can help describe the ethical features associated with a piece of technology and the risk assessment needed. Moreover, they can act as a guarantor of equity related to gender and marginalized groups in 4IR technology design and application, avoiding unintended biases.

Text Box 6 – AI and big data bias and protection

AI and big data are interconnected and have significant societal impacts and risks as AI allows for collecting vast quantities of data, and citizens unknowingly, unwittingly or mandatorily have their data collected. This harvested data is available for many uses, including tracking payment habits, a person's location, personal circumstances, relationships and health. AI systems can have failings that introduce data bias or poisoning and model extraction and evasion, therefore, the systems require more complex privacy-preserving techniques. The development of standards that deal with the entire life cycle of AI systems—from the inception of the idea, during development, monitoring and disposal—can help achieve accountability and transparency and build trust in the technology. Such standards can support legislation like the EU's General Data Protection Regulation (GDPR) that provides measures to remedy the misuse of personal data.

INCLUSIVENESS

The inclusiveness principle seeks to address two interlinked problems in the digital transformation, namely unequal representation in the standards development process and groups of people being excluded and/or negatively impacted by new technologies.

Technological experts and users (e.g. businesses and governments) are the majority participants in standards development. The inclusion of a broader range of societal stakeholders (e.g. consumer groups, labour, NGOs, civil society and faith groups) can highlight the socio-ethical impacts of digital technology, which are increasingly essential considerations in standard making to mitigate the societal exclusion impacts of the digital transformation. Standardization has a role in

helping manage and mitigate these impacts to ensure inclusivity and equity and to challenge bias by applying the inclusiveness principle.

No particular person, organization or interest group should dominate standards-making activities. However, participation in standardization is not geographically even, or gender or culturally-balanced, often excluding minorities and indigenous people. There is a predominance of experts from developed countries, with LDCs most underrepresented and unable to participate, for example, because of a lack of financial and technical resources, technical experts and English language skills. Women are also significantly underrepresented in SDOs. Their unwitting exclusion is counterproductive as gender diversity brings a fuller range of experiences and the possibility of developing gender-responsive standards. Breaking it down further, since women are not a homogeneous group, representation and inclusion has been observed to also differ due to intersectional disadvantages.

This de facto exclusion of certain stakeholders' contributions is a significant concern, as ethnic and gender biases can creep into digital technology, particularly those utilizing AI and big data, and varied perspectives add greater relevance and credibility to standardization.

Furthermore, as a means to inform policymaking and national development strategies, standards should explicitly advocate for technology design and development processes that are informed by representative data sets, including sex-disaggregated data as well as qualitative data informing about the needs and experiences of different user groups, such as differently abled users. ISO/IEC Guide 71:2014 – Guide for addressing accessibility in standards suggests ways of determining user accessibility needs without providing specific solutions, noting that optimal solutions vary greatly depending on the specific users and contexts of use and that additional sector-related guides might need to be developed for specific product or service sectors. Equitable, high-quality access to new technologies and creating an enabling environment, which allows excluded or underserved persons to benefit from new technologies, while being a complex goal, should be supported through standardization. In addition to acknowledging and raising awareness on the necessary and unequally distributed infrastructural aspects, guidance on skills and capacity building aimed at addressing challenges associated with limited access and barriers to usage, affordability, digital literacy as well as digital skills should form an integral part of any standardization activity in the realm of digital transformation.

SUSTAINABILITY

Sustainability is not embedded in the digital transformation. Standardization is one area where the link needs to be more explicit between digital technology and its sustainability impacts. Standardization has a role to play in articulating the opportunities and threats from new technology for sustainability. For example, smart manufacturing crafted around circular economy ideas and smart agriculture potentially increases yields and reduces inputs protecting biodiversity and the environment. The absence of consideration of sustainability issues in the digital technology standardization space makes this principle important.

Noting the importance of sustainability in standard making, the London Declaration is a push from ISO to transform the approach to climate action and advance international work to attain net-zero goals. It emphasizes international standards' important role in assisting communities, organizations and industries in the transition to cleaner, renewable energy sources, and in helping to preserve biodiversity at the same time as opening up markets for innovations that address global environmental challenges. The London Declaration promises to embed key climate considerations into every new standard that is created. It will also retrospectively add these requirements to all existing standards as they are revised, a change on an unparalleled scale.

Emphasizing sustainability specifically in digital-related standard setting will encourage the usage of digital technologies to promote transformation towards an efficient, intensive and environmentally friendly development model, and enhance interoperability and cyclic utilization of digital hardware.

However, the incorporation of sustainability in standard making in the digital space is unsystematic and cursory. This principle is not systematically considered in the standard-making process despite the fact that digital technologies significantly influence the achievement of SDGs and standards have an important role in shaping achievement.

Given the far-reaching and long-term impact the digital transformation will have on people, their prosperity and the planet, digital technologies have a crucial role in delivering sustainability, therefore, aligning the digital transformation with the change needed for sustainability is essential.

SDOs and other standard-making organizations need to ensure that standards incorporate sustainability as a principle utilizing the SDGs and the 2030 Agenda to record impact and shape standards and digital technology outcomes. For example, ISO has published the standard ISO Guide 82:2019 giving guidance on how standards-makers can address sustainability in standards. The guide strongly encourages standards developers "to consider sustainability issues in their work at all stages in the standards development process. If sustainability issues have not been considered, this can be a valid reason to start the revision of a standard." ISO Guide 84:2020 – Guidelines for addressing climate change also references sustainability, noting that standards that take into consideration climate change can also directly or indirectly contribute to the achievement of sustainability. ISO also maps its standards impacts to specific SDGs.

INTEROPERABILITY

Interoperability is necessary for creating added value through the integration of compatible digital technologies. It is being given much attention in the standardization activities for the seven digital technologies addressed in this publication. Standards have a pivotal role in ensuring technology interoperability. In the context of digital transformation, standards development following the principle of interoperability should encourage the convergence of technical terms, criteria and methodologies not only in individual industry, but also on a broader cross-sector scale. They also should promote multi-stakeholder dialogue and coordination in digital-related standard setting to enhance standard harmonization and eliminate technological standard silos which create market access barriers and hinder competition.

Interoperability will enable digital transformation in organizations to be quicker, more affordable and effective. For example, harmonized standards in IoT allow technology to work together to enhance user experience. Compatibility between digitally transformed infrastructures will help instil long-term agility and economic efficiency in smart systems such as smart cities, infrastructure and manufacturing. Compatibility between digital technology and other frameworks such as the legal framework and DLT will help leverage the technology and ensure outcomes that benefit users and mitigate risk.

The successful implementation of pro-interoperability standards ensures compatibility and connectivity so that new technologies can be seamlessly adopted. By promoting interoperability in digital technologies, standards ensure market efficiencies, lubricate trade and increase efficiency and progress.

SAFETY AND SECURITY

Safety and security issues need to be a principal tenet on which standards are developed in the digital technology landscape because digital technology presents many challenges and risks. As more digital technologies interact with the physical world in the workplace and at home and play, people are exposed to physical and psychological safety and security risks.

4IR technologies also pose gender-differentiated safety and security concerns, particularly in terms of exposure to hazardous substances on reproductive health or the ergonomic design of physical technological devices. The legal framework has a raft of health and safety and product safety legislation applicable to new technologies. However, this legislation may not have the relevant elements to ensure emerging technologies integrate safety and security-by-design. For example, AI used in a self-driving vehicle must satisfy higher safety requirements than when AI optimizes a fully automated industrial process.

Standards and guidelines can specify how to prevent misuses, modifications and failures, and have procedures to enable humans to stay in control of security. The robustness of cybersecurity systems of digital technology that collect and utilize vast qualities of data is also a concern. Greater connectivity equates to more data that can be misused or attacked. For example, in 2015, hackers demonstrated that they could control a vehicle's braking and acceleration systems. Effective cybersecurity, therefore, is essential not just for cars but also for all connected digital technologies exposed to the threat of attack. Standardization has taken up the safety and security issue, supporting legislation by clearly focusing on the safety and cyber security risk in standards for digital technologies.

DATA PRIVACY

The digital transformation is driven by data. As people are increasingly interconnected and dependent on digital services, data privacy has become a horizontal and cross-sectoral issue that involves AI and big data, blockchain/DLT, IoT and UAS.

Data privacy governs how data is collected, shared and used. It is an area of data protection that concerns the proper handling of sensitive data, including, most notably, personal data, but also other confidential data, such as certain financial data and intellectual property data. Data privacy is not data security. Improper handling of privacy data may not lead to security concerns but can be classified as privacy intrusion.

Future standards directly or indirectly related to the collection, storage, exchange and usage of privacy data need to be developed by:

1) Highlighting the protection of privacy data as a priority;

2) Avoiding using technical terms, indicators, criteria and guidelines that may create loopholes for intrusion and abuse of privacy data; and

3) Providing guidelines to normalize the behaviour of data collectors, holders and users, and to empower original data owners by enhancing their awareness and visibility.

INTERNATIONAL COLLABORATION

As digital transformation creates both opportunities and challenges that transcend borders, international cooperation is a key dimension to make the most out of the digital transformation at local, national and international levels (see Text Box 7).

Text Box 7 – Cooperation and participation in Africa and South America

The African Organisation for Standardisation (ARSO) signed a memorandum of understanding (MoU) with ISO in 2021, aiming to strengthen the cooperation between the two organizations with a critical feature to improve the ability of ARSO members to participate in international standardization activities effectively.

The Pan American Standards Commission (COPANT) highlighted finding experts who were also fluent in English a particular issue for South American members of their organization. The organization has enhanced investment in ICT and IT tools during the pandemic, however, the lack of these resources persists and can inhibit active participation in standardization.

Highlighting international collaboration in standards development will facilitate coordination and harmonization of regional and global digital markets and promote more effective regulatory response. More specifically, it can help to:

1. Lower technical barriers for international flow of digital goods and services and build a more integrated regional and global digital market which can help countries fully tap into their digital potential;
2. Mitigate the risk of transnational cybercrime, privacy intrusion and intellectual property violation; and
3. Address national security concerns on data security, communication technology reliability and key infrastructure resilience.

To promote international collaboration, it is essential for international organizations to strengthen their roles in trust building and partnership mobilizing, actively engaging with their members and effectively leveraging collective efforts in international standards development and capacity building. National standards bodies need to consider applying international standards before developing their own set or referring to them as recognized equivalents.

PART 5: **FUTURE**

REFLECTIONS ON THE FUTURE OF STANDARDS IN DIGITAL TRANSFORMATION GOVERNANCE

Digital technologies will forever transform systems changing how societies live, work and play. They possess transformative potential for developing countries and for the achievement of the SDGs, on the condition that dedicated access mechanisms are created and implemented internationally and that developing countries are not excluded from the standard-setting process. While these emerging technologies have the potential to drive enormous social breakthroughs and economic value, they also have the potential for unintended consequences and adverse effects for people, their prosperity and the planet.

This is a call to action as society must understand the risks and rewards of the digital transformation. Standards-makers need to leverage the role of standards to ensure that digital technologies remain human-centered and aligned to the goals of sustainability, providing everyone in society with equitable access and unbiased participation.

Progress in the innovation and development of digital technologies and digital transformation is creating a fast-moving environment and is unstoppable. The regulatory and policy frameworks develop appropriate governance rules for technology, however, this evolving framework has limitations such as being primarily nation bound and time-consuming. Standards have an important role in this framework, being transnational, multi-stakeholder driven, speedy to develop and responsive to user needs.

Standards have the potential to contribute to digital transformation governance. In order to unlock this potential, the following aspects should be considered:

» The scope of impacts of the digital technologies shaping the 4IR vary. A robust strategy is required to understand the implications of current and future technologies and to shape the digital transformation towards people, their needs and the planet.

» Standards developers worldwide need to work as a community to provide objectivity, credibility, and transparency in their standards work and to ensure their output is understandable and usable.

» There is a need for collaboration and technical cooperation between standards developers of all types to ensure the most comprehensive, high-quality, and up-to-date selection of standards for digital technologies and a high level of convergence is produced. This includes creating an inclusive environment and allowing equal and appropriate representation of all relevant stakeholders, which is paramount in standardization.

» Sustainability is an area where the link must be made more evident in standards developed for digital technology. In doing so, the impacts of digital technologies can be taken into account and their transformative capabilities can be better leveraged to strengthen all SDG pillars—people, planet, prosperity, partnership and peace.

» Standardization, guided by the seven principles of trustworthiness, interoperability, safety and security, data privacy, inclusiveness, sustainability and international collaboration, can support people, prosperity and the well-being of the planet. Building on strong partnerships, the standards community can ultimately contribute to good governance.

As this decade is critical for the planet and its people, this publication is a call to action to all stakeholders in the development of regulations and standards to consider the outlined principles in their work in order to leverage the opportunities offered by digital technologies and thereby accelerate prosperity for all.

Department of Digitalization, Technology and Innovation (DTI)
Vienna International Centre
Wagramerstr. 5, P.O. Box 300,
A-1400 Vienna, Austria

+43 1 26026-0

www.unido.org

dti@unido.org

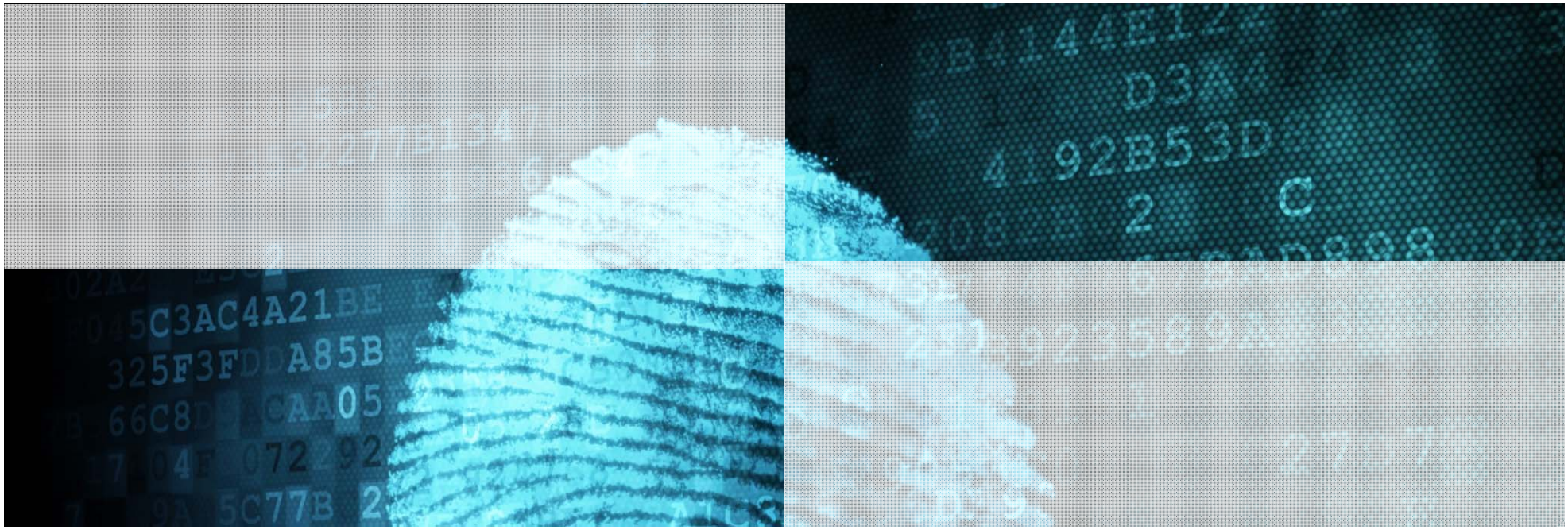
UNITED NATIONS
INDUSTRIAL DEVELOPMENT ORGANIZATION

WORLD ECONOMIC FORUM

COMMITTED TO IMPROVING THE STATE OF THE WORLD

A Blueprint for Digital Identity

The Role of Financial Institutions in Building Digital Identity



An Industry Project of the Financial Services Community | Prepared in collaboration with Deloitte

Part of the Future of Financial Services Series • August 2016

Foreword

Consistent with the World Economic Forum's mission of applying a multi-stakeholder approach to address issues of global impact, the creation of this report involved extensive outreach and dialogue with the financial services community, innovation community, technology community, academia and the public sector. The dialogue included numerous interviews and interactive sessions to discuss the insights and opportunities for collaborative action.

We extend sincere thanks to the industry and subject matter experts who contributed their unique insights to this report. In particular, the members of the Project's Steering Committee and Working Group, who are introduced in the following pages, played an invaluable role as experts and patient mentors.

We are also very grateful for the generous commitment and support to Deloitte Consulting LLP in the U.S., an entity within the Deloitte[1] network, in its capacity as the official professional services advisor to the World Economic Forum for this project.

Contact

For feedback or questions, please contact:

R. Jesse McWaters, Lead Author
jesse.mcwaters@weforum.org
+1 (212) 703-6633

[1] Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee ("DTTL"), its network of member firms, and their related entities. DTTL and each of its member firms are legally separate and independent entities. DTTL (also referred to as "Deloitte Global") does not provide services to clients. Please see www.deloitte.com/about for a detailed description of DTTL and its member firms. Please see www.deloitte.com/us/about for a detailed description of the legal structure of Deloitte LLP and its subsidiaries. Certain services may not be available to attest clients under the rules and regulations of public accounting.

Acknowledgements

Acknowledgements

Members of the Steering Committee

The following senior leaders of global financial institutions have provided guidance, oversight and thought leadership to the “Disruptive Innovation in Financial Services” project as its Steering Committee:

Bob Contri

Vice Chairman,
Deloitte & Touche LLP

David Craig

President, Risk and Financial,
Thomson Reuters

John Flint

Chief Executive Officer, Retail Banking and Wealth Management, *HSBC*

Kim Hammond

Chief Operating Officer,
Deutsche Bank

Jason Harris

Chief Executive Officer, International Property and Casualty, *XL Group*

Michael Harte

Chief Technology Officer and Chief Operations Officer, *Barclays*

Axel Lehmann

Chief Operating Officer,
UBS

Jason Patwardhan

Chief Innovation Officer,
Standard Chartered Bank

David Puth

Chief Executive Officer,
CLS Group

William Sheedy

Global Executive, Corporate Strategy, M&A, Government Relations, *Visa*

Dietter Wemmer

Chief Financial Officer,
Allianz

Acknowledgements

Members of the Working Group

The project team would also like to acknowledge the following executives of global financial institutions who helped define the project framework and shape strategic analyses as its Working Group:

Tom Brown

Partner,
Paul Hastings

Lena Mass-Cresnik, PhD

Head of Innovation, Strategic Product Management, *BlackRock*

Christof Edel

Global Head of Trading Strategy & Business Development, *Thomson Reuters*

Rob Galaski *(Project Advisor)*

Head of Financial Services,
Deloitte

Dorothy Hillenius

Director of Corporate Strategy,
ING

Marc Lien

Director of Innovation and Digital Development, *Lloyds Banking Group*

Matthew Levin

EVP and Head of Global Strategy,
Aon

Victor Matarranz

Director of Strategy & Chief of Staff to the CEO,
Santander

Neil Mumm

VP Corporate Strategy,
Visa

Max Neukirchen

Group Head of Strategy,
JP Morgan Chase

Christine O'Connell

Global Head of Strategy & Business Development, *Thomson Reuters*

Robert Palatnick

Managing Director and Chief Technology Architect, *DTCC*

Kosta Peric

Deputy Director Financial Services for the Poor, *Bill and Melinda Gates Foundation*

Justin Pinkham

SVP and Group Head, Payments Innovation,
MasterCard

Bob Reany

SVP and Group Head, Identity Solutions,
MasterCard

Peter Rutland

Senior Managing Director,
CVC Capital Partners

Nicolas de Skowronski

Chief of Staff,
Bank Julius Baer

Huw Van Steenis

Managing Director and Head of Financial Services Research, *Morgan Stanley*

Colin Teichholtz

Partner & Co-Head of Fixed Income Trading,
Pine River Capital

Fabien Vandenreydt

Head of Markets Management, Innotribe & the SWIFT Institute, *SWIFT*

Acknowledgements

List of subject matter experts (1 / 2)

In addition, the project team expresses its gratitude to the following subject matter experts who contributed their valuable perspectives through interviews and workshops (in alphabetical order):

Mukul Ahuja	Deloitte Canada
Christoph Albers	SWIFT
Alex Batlin	UBS
Eric Benz	Credits
Peter Berg	Visa
Vikram Bhat	Deloitte & Touche LLP
David Birch	Consult Hyperion
Francis Bouchard	Hamilton Place Strategies
Andre Boysen	SecureKey
David Brewer	Digital Catapult
Ben Brophy	ENTIQ
Tom Brown	Paul Hastings
Preston Byrne	Eris Industries
Claire Calmejane	Lloyds Banking Group
Alicia Carmona	Identity 2020
Nicolas Cary	Blockchain
Shawn Chance	Nymi
Emily Clayton	Bank of England
John Clippinger	MIT Media Lab
Jeff Coleman	Ledger Labs
Wayne Crombie	Citigroup
Malcolm Crompton	Information Integrity Solutions
Stephen Cross	Aon
Mark Davies	Avox Ltd.
Howard Davis	RBS
Nicolas de Skowronski	Julius Baer
Rachel Dixon	Digital Transformation Office of Australia
Ivan Djordjevic	Deloitte UK
Justin Dombrowski	Historiocity Tech
Jon Duffy	TradeMe
Carlo Duprel	Deloitte Tax & Consulting, Luxembourg
Andre Durand	Ping Identity
John Edge	Digital Stored Value Association
Anna Ewing	Nasdaq
Daniel Feichtinger	Digital Asset Holdings
Chris Ferguson	UK Cabinet Office
Jerry Fishenden	VoeTek
Marissa Flowerday	TradeMe
Conan French	IIF
Emilio Garcia	Santander
Joe Guastella	Deloitte Consulting LLP
Alka Gupta	Global ID
Aran Hamilton	DIACC
Jonathan Hardinges	Thomson Reuters
Adrienne Harris	National Economic Council, The White House
Jonathan Hayes	Julius Baer
Dorothy Hillenius	ING
Bill Hodash	DTCC
Rainer Hoerbe	The Kantara Initiative
Chuck Hounsell	TD Canada
Arne Vidar Huag	Signicat
Afsar Hussain	GSMA
Marta Ienco	GSMA
Raj Iyer	BNY Mellon
Natasha Jackson	GSMA
Charlotte Jacoby	Agency for Digitization, Ministry of Finance, Denmark
Hyder Jaffrey	UBS
Andrew Johnston	TELUS
Tanis Jorge	Trulioo
Sean Kevelighan	Zurich Insurance Group
Alim Khalique	Bank of America Merrill Lynch
Hwan Kim	Deloitte Canada
Dan Kimerling	Standard Treasury
Philipp Kroemer	Commerzbank AG
Jaap Kuipers	Kantara Initiative
Jo Lambert	Paypal
Ian Lee	Citi
Chris Locke	Caribou Digital
Joseph Lubin	Consensys
Adam Ludwin	Chain
Christian Lundkvist	Consensys

Acknowledgements

List of subject matter experts (2 / 2)

In addition, the project team expresses its gratitude to the following subject matter experts who contributed their valuable perspectives through interviews and workshops (in alphabetical order):

Joanna Marathakis	Deloitte Transactions and Business Analytics LLP
Stephen Marshall	Deloitte UK
Simon Martin	LeapFrog Investments
Todd McDonald	R3CEV
Morgan McKenney	Citigroup
Adel Melek	Deloitte Canada
Pat Meredith	Canadian Payments Taskforce
Paul Morgenthaler	Commerzbank
Renny Narvaez	BNY Mellon
Eddie Neistat	AlixPartners
Nina Nieuwoudt	Mastercard
Pascal Nizri	Chekk
Robert Palatnick	DTCC
Cheryl Parker Rose	CFPB
Justin Pinkham	MasterCard
Rick Porter	Deloitte & Touche LLP
Reinhard Posch	Austrian Federal Government
Dan Quan	CFPB
Rhomaios Ram	Deutsche Bank
Kai Rannenberg	Goethe University
Bob Reany	Mastercard
David Richards	DIACC
Pierre Roberge	Digital and Payment Innovation Consultant
Andre Romanovskiy	Deloitte Canada
Andrew Rudd	AssureUK
Peter Rutland	CVC Capital Partners
Wiebe Ruttenberg	European Central Bank
Joel Sacmar	Daon
Jean-Louis Schiltz	Schiltz & Schiltz
Charles Schwarz	Barclays
Rocky Scopelliti	Telstra
Amy Scott	Identity2020
John Scott	2Keys Security Solutions
Anton Semenov	Commerzbank
Beth Shah	Digital Asset Holdings
Rajesh Shenoy	Citi
Nick Smaling	Deloitte Netherlands
Stan Stalnaker	HubID
Matthew Stauffer	Clarient Entity Hub
Gavin Steele	Lloyd's of London
Ashley Stevenson	ForgeRock
Matt Stroud	Digital Catapult
Paul Szurek	Blockchain
Pavlo Tanasyuk	BlockVerify
Marc Taverner	BitFury
Simon Taylor	Barclays
Adizah Tejani	Level39
Kenneth Tessem	Finansiell ID-Teknik BID AB
Don Thibeau	Open Identity Exchange (OIX)
Michael Turner	PERC
Keith Uber	GlobalSign
Eric Van der Kleij	Level39
Huw van Steenis	Morgan Stanley
Aneesh Varma	Aire.io
Ivan Vatchkov	Algebris Investments
Roy Vella	Vella Ventures Ltd.
Helene Vigue	GSMA
Franziska von Arnim	Deutsche Bank
Patrick Walker	PERC
Colin Wallis	Kantara Initiative
Peter Watkins	Government of British Columbia
Derek White	Barclays
Conor White	Daon
Greg Williamson	MasterCard
Gregory Williamson	MasterCard
Stephan Wolf	GLEIF
Kevin Young	Deloitte Canada
Fei Zhang	Allianz
Tom Zschach	CLS Bank

Acknowledgements

Project Team and Additional Thanks

Project Team

The “Disruptive Innovation in Financial Services” project team includes the following individuals:

WORLD ECONOMIC FORUM PROJECT TEAM

Jesse McWaters
Project Lead, Disruptive Innovation in Financial Services

Giancarlo Bruno
Senior Director, Head of Financial Services Industries

Michael Drexler
Senior Director, Head of Investors Industries

PROFESSIONAL SERVICES SUPPORT FROM DELOITTE

Rob Galaski
Project Advisor, Deloitte

Christine Robson
Lead Author, Deloitte

Additional Thanks

The project team expresses its gratitude to the following individuals for their contribution and support throughout the project (in alphabetical order):

Faiza Harji

Alex Rinaldi

Sabrina Sdao

And to:

The Deloitte Greenhouse (Event Facilitation & Location Services)

Level 39 (Location Services)

The Value Web (Event Facilitation)

Executive Summary

The Blueprint for Digital Identity project is the most recent phase of the Forum's ongoing Disruptive Innovation in Financial Services work

WORLD ECONOMIC FORUM
COMMITTED TO IMPROVING THE STATE OF THE WORLD

2015

THE FUTURE OF FINANCIAL SERVICES

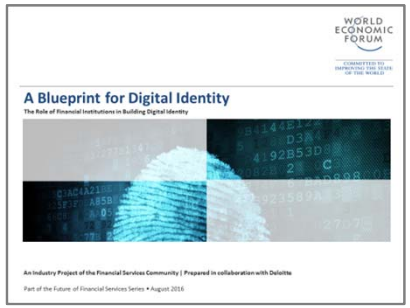
The Future of Financial Services project explored the landscape of disruptive innovations in financial services, provided the first consolidated taxonomy for these disruptions, and explored their potential impacts on the structure of the industry

2016

BEYOND THE FUTURE OF FINANCIAL SERVICES

This phase of the disruptive innovation work explores two topics with key potential as foundational enablers of future disruption

A Blueprint for Digital Identity: The role of Financial Institutions in building Digital Identity



This project explores the potential for digital identity in financial services and beyond and lays out a blueprint for the implementation of effective digital identity systems

The future of financial infrastructure: An ambitious look at how blockchain can reshape financial services

This project explores the potential for distributed ledger technology to transform the infrastructure of the financial services industry

The mandate of this project was to explore digital identity and understand the role that Financial Institutions should play in building a global standard for digital identity

WORLD ECONOMIC FORUM
COMMITTED TO IMPROVING THE STATE OF THE WORLD

PROJECT CONTEXT

Identity is a critical topic in Financial Services today. Current identity systems are limiting Fintech innovation and well as secure and efficient service delivery in Financial Services and society more broadly. Digital identity is widely recognized as the next step in identity systems. However, while many efforts are underway to solve parts of the identity challenge and create true digital identity, there is a need for a concerted and coordinated effort to build a truly transformational digital identity system.

This document is intended as a guide for Chief Strategy Officers of Financial Institutions as well as policy makers who are interested in the topic of identity and want to understand the digital identity and their own potential role in the creation of robust digital identity systems.

PROJECT SCOPE

The mandate of this project was to explore identity and its importance in Fintech, Financial Services and in developed societies broadly, the topic of digital identity, and provide a landscape scan of current efforts to build digital identity solutions.

This report will discuss different structures for identity systems and discuss which configurations are best suited to solve different problems, and provide a perspective on the role of Financial Institutions in building digital identity systems.

This report will not focus on the creation of standards around identity; much valuable work has already been done in this space and current developments such as the publication of the European Union eIDAS Regulation are moving the conversation on this front. Nor will it discuss technology solutions. Rather, it will attempt to provide clarity and direction around the structure of identity and provide a call to action for Financial Institutions to move against the identity challenge.

Over 12 months of research we engaged with subject matter experts through interviews and multi-stakeholder workshops

WORLD ECONOMIC FORUM
COMMITTED TO IMPROVING THE STATE OF THE WORLD

Industry Leaders

Guidance and thought leadership from **12 C-suite executives and 24 strategy officers** of global financial institutions

Subject Matter Experts

In-person and phone interviews with **100+ subject matter and industry experts**

Global Workshops

Four multi-stakeholder workshops at global financial hubs with 200+ total participants including industry leaders, innovators, subject matter experts, and regulators

Singapore	New York, USA	London, UK	Davos, Switzerland
Oct. 2015	Nov. 2015	Dec. 2016	Jan. 2016

This report synthesizes our findings and presents a Point of View on the role that we see for Financial Institutions in digital identity

PROJECT OUTCOMES

Our Perspective: The Role of Financial Institutions in Digital Identity

How should Financial Institutions engage with digital identity? What role can they play in the development of digital identity solutions?

1	**Introduction** What is the global identity challenge, and what problems does it pose for Financial Institutions?
2	**Digital Identity Primer** What is the purpose of identity systems, and why is digital identity the solution to the global identity challenge?
3	**The Landscape of Digital Identity** What do efforts to build digital identity systems look like globally?
4	**The Right Solution to the Right Problem** How should digital identity systems be constructed to serve different needs?
5	**Benefits of Digital Identity** Who stands to benefit from the introduction of digital identity systems?
6	**Implementation** How do you reach a global digital identity solution?

The Role of Financial Institutions in Digital Identity

Current identity systems place major limitations on Fintech innovation

Lack of digital identity limits the development and delivery of efficient, secure, digital-based Fintech offerings

Identity is currently a critical pain point for Fintech innovators. Many of these innovators are trying to deliver pure digital offerings, but the process of identifying users consistently forces them to use physical channels. These Fintech innovators now see the development of a new generation of digital identity systems as being crucial to continuing innovation and delivering efficient, secure, digital-based Fintech offerings.

Examples

Payments

Payments require validation of ACH information, meaning that digital payments innovators must either require users to provide identity information through pseudo-digital channels (such as by photographing their driver's license) or act as platforms on top of established Financial Institutions and rely on their KYC processes

Loans

Evaluating customer risk and issuing loans requires validation of basic customer information, requiring innovators to gather information from users, again through pseudo-digital channels such as photographing existing ID or gathering trusted information from an existing source, and therefore decentralizing a central piece of the product offering

Digital identity is a critical enabler of activity inside Financial Services broadly

Digital identity would allow FIs to perform critical activities with increased accuracy over that afforded by physical identity, and to streamline and partially or fully automate many processes

Identity is also central to the broader financial services industry, enabling delivery of basic financial products ands services. Reliance on physical identity protocols introduces inefficiency and error to these processes. Digital identity has great potential to improve core financial services processes and open up new opportunities.

Examples

Operational decisions

Traditional FS offerings such as insurance and credit and well as customer experience such as contact centers and collections rely on accurate and detailed knowledge of the customer

Regulatory compliance

FIs are required to comply with strict regulation on identifying their customers and are liable for mistakes and inaccuracies

Customer experience and product delivery

Improved knowledge of customer preferences and habits can help FIs deliver radically better customer experience (e.g., tailor authentication requirements based on behaviour)

The relevance of digital identity stretches beyond Financial Services to society as a whole

Identity enables many societal transactions, making strong identity systems critical to the function of society as a whole

Physical identity systems currently put users at risk due to overexposure of information and the high risk of information loss or theft; they also put society at risk due to the potential for identity theft, allowing illicit actors to access public and private services. Digital identity would streamline and re-risk completion of these public and private transactions.

PUBLIC TRANSACTIONS

Entities are required to prove their identities or certain attributes to demonstrate their eligibility for public services

Examples

- *Access to social assistance (e.g., old age security, unemployment insurance)*
- *Access to education*
- *Access to healthcare*
- *Access to civic structures (e.g., voting)*

PRIVATE TRANSACTIONS

Entities are often required to prove their identities or certain attributes to participate in private transactions

Examples

- *Many basic merchant transactions (e.g., buying alcohol)*
- *Large private provider transactions (e.g., renting an apartment, buying a car)*

The need for digital identity is becoming increasingly pressing

Five key trends are increasingly the need for efficient and effective identity systems:

1 

Increasing transaction volumes
The number of identity-dependent transactions is growing through increased use of the digital channel and increasing connectivity between entities

2 

Increasing transaction complexity
Transactions increasingly involve very disparate entities without previously established relationships (e.g., customers and businesses transacting cross-border)

3 

Rising customer expectations
Customers expect seamless, omni-channel service delivery and will migrate to services that offer the best customer experience

4 

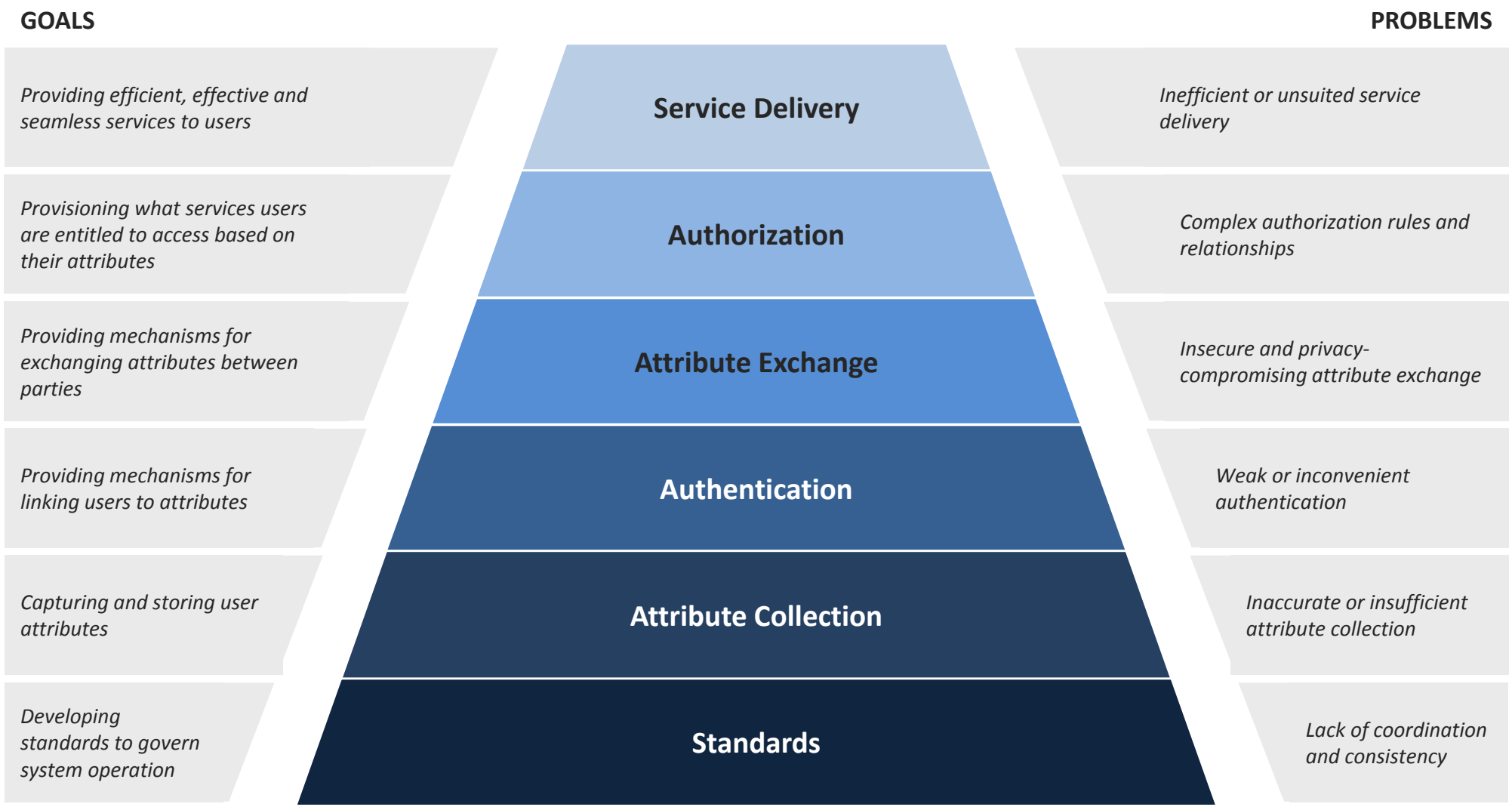
More stringent regulatory requirements
Regulators are demanding increased transparency around transactions, meaning that FIs require greater granularity and accuracy in the identity information that they capture and are increasingly being held liable for inaccurate or missing identity information

5 

Increasing speed of financial / reputational damage
Bad actors in financial systems are increasing sophisticated in the technology and tools that they use to conduct illicit activity, increasing their ability to quickly cause financial and reputational damage by exploiting weak identity systems

However, identity is a multi-layered problem making the creation of digital identity systems complex

Each layer of identity of serves a different purpose, and suffers from a distinct set of problems in today's identity landscape

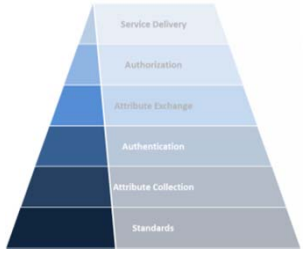


There are currently many distinct gaps in the digital identity landscape

1. Confusing authentication with identity

Many efforts today focus on authentication as a solution to the identity challenge without addressing the strength of the underlying attribute collection and authorization processes

- *Authentication technology solutions, while valuable, rely on preexisting onboarding and attribute collection processes*
- *Authentication solutions provided by global technology platforms are convenient for users but do not provide security or verification of the identity behind an account or username*



2. Enabling transaction completion rather than user activity

Many solutions are driven by the goals and perspectives of a single organization and therefore are designed to serve the needs of particular transactions rather the broader needs of users

- *eGovernment solutions are intended to make government service delivery to users more efficient, and do not enable further transactions in which users might want to participate*
- *Transaction-focussed solutions result in the repeated collection of 'tombstone' data rather than effective collection of user-centric and risk-relevant data such as transaction habits*

3. Building consensus rather than driving action

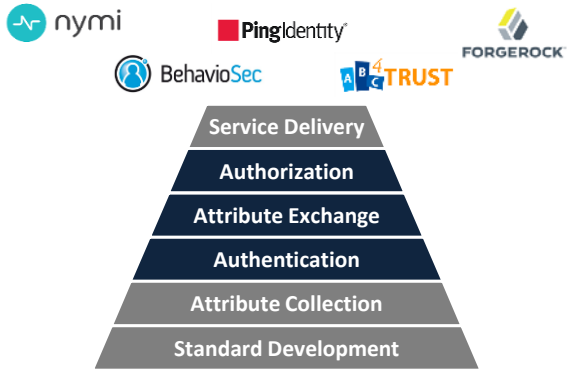
Many efforts focus on building agreement around standards and processes rather than creating a full identity solution and therefore do not result in private sector-implementable solutions

- *Utilities and standards organizations are focussed on creating consensus and a standardized view of data, rather than providing a full identity solution*
- *Multi-governmental efforts have considerable scale but are mainly focussed at the regulatory level, and do not offer a commercially viable solutions*

These gaps are a result of the crowded digital identity landscape, with many different entities building solutions

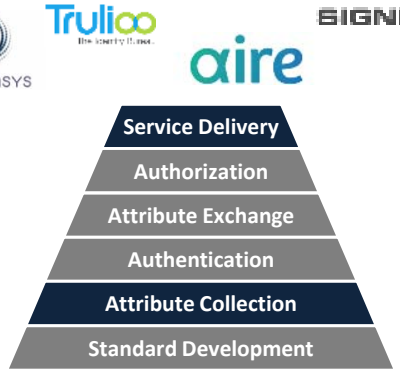
Technology solution providers

Technology solution providers focus on point solutions for authentication, attribute exchange or identity management for enterprises



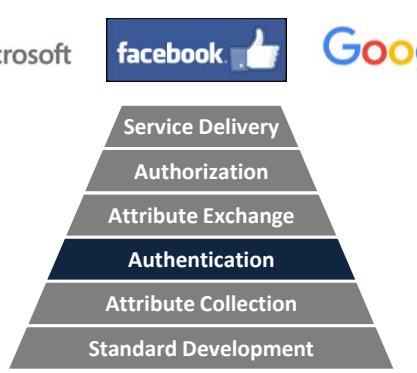
Private Service Providers

Private service providers focus on collecting the attributes they themselves need to provide specific services to users



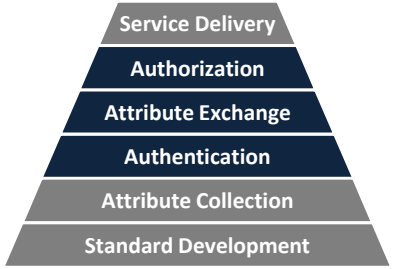
Global technology companies

Global technology companies act as platforms to authenticate users to a wide variety of other service providers



Industry Bodies

Industry bodies focus on standardizing and centralizing the collection of attributes within that specific industry



Governments

Governments focus on the provision of identity to their citizens, and providing citizens with services based on these attributes

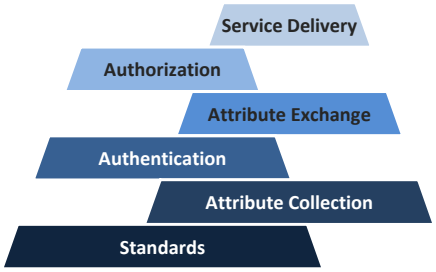
Standards Organizations

Standards organizations focus on frameworks and guidance for developing identity systems

There is an opening for new digital identity systems that can deliver scope and scale

While many ongoing efforts, such as new authentication solutions, are critical to building digital identity, there is a core need for a strong system will enable effective action against each layer of the stack

The entire stack does not need to be provided by a single entity – some components may be modular – but the entire stack must be effective and integrated to provide digital identity systems that have certain critical features



Critical characteristics of a strong identity system

1. **Operationally effective**
   The system allows digital transactions to be completed conveniently and effectively

2. **Scope & scale**
   The system enables large volumes of transactions through provision of transaction-critical attributes and connecting large numbers of users with important and frequently used service providers

3. **Security**
   The system prevents user information from being overexposed, lost or stolen

4. **User control & privacy**
   The system allows users to determine where their information is held and when it is shared or exposed

5. **Viability**
   The system delivers value to all stakeholders, creating broad support and uptake and making it a commercially viable system

Financial Institutions are well positioned to drive the creation of digital identity systems

Financial institutions are exceptionally well positioned to drive identity systems that fill the gaps left by current efforts

	STRUCTURAL
1	FIs already act as **stores of customer attributes** for their own commercial purposes, and therefore are positioned to act as identity providers without extensive incremental effort
2	FIs are one of very few types of institutions that can **verify user information**; they already perform this function for commercial and regulatory purposes
3	FIs are **incentivized to collect accurate user information** for their own commercial purposes
4	FIs have **proven executional ability** to develop new systems and standards (e.g., Interac) that have been widely adopted and effectively used within the private sector
5	The FS industry has near-complete **coverage of users** (people, legal entities, and assets) in developed economies
6	Global FIs have interconnected **operations across multiple jurisdictions**, giving them a structural advantage in enabling cross-jurisdictional identity transactions and systems

	POSITIONING
1	FI operations and use of customer data are **rigorously regulated**
2	FIs act as **established intermediaries** in many transactions and are therefore well positioned to act as identity intermediaries
3	FIs are typically **trusted by consumers** beyond other institutions to be safe repositories of information and assets

There is a strong business case for Financial Institutions to lead the development of digital identity systems

FIs could derive substantial benefit from investing in the development of digital identity solutions. We have categorized these benefits into three categories: efficiency / cost avoidance, new revenue opportunities & brand enhancement, and transformational future state opportunities

Efficiency / Cost Avoidance

Opportunities to streamline current processes, increase automation, and reduce error and human intervention

New Revenue Opportunities

Opportunities to create new revenue streams from new products and services, and to increase the positive recognition of the brand

Transformational Future State Opportunities

Opportunities to stretch outside of core business and capabilities to create transformational new business models and reach new customers

Financial Institutions could benefit from basic efficiency improvements and cost avoidance…

Efficiency / Cost Avoidance

Process streamlining & automation
Streamline and improve onboarding and compliance processes through access to a reliable and consolidated digital view of user attributes, minimizing RFIs and information remediation due to inaccuracy and human error

Improved service delivery
Provide increasingly tailored products and services to customers by leveraging non-traditional attributes
Improve process efficiency and increase STP by automating processes through use of standardized, reliable digital data

Improved customer experience
Improve customer experience by leveraging a variety of user attributes to better understanding the customer's needs and preferences

Improved risk assessment & scoring
Improve risk assessment and reduce fraud by creating more holistic and accurate customer risk profiles to inform suspicious transaction monitoring, insurance payouts, and provision of credit- and risk-based products

Develop new revenue streams…

New Revenue Opportunities

New financial products & services
Offer new products and services based on increased knowledge of customers (e.g., extended financial advisory, new insurance products such as insurance on fractionally owned assets and behaviour-based insurance)

Identity-as-a-service
Offer identity as a service to relying parties who cannot or do not wish to store customer information

Identity-only customers
Offer identity as a separate, fee-based service for individuals who do not otherwise transact with that FI

… and stretch beyond current business and markets to fundamentally transform their businesses

Transformational Future State Opportunities

Allocation of liability
Shift the liability for incorrect information, and the outcomes of holding this information, from Financial Institutions to other entities in the network (e.g., users through approval and consent requirements)

Trust brokerage
Act as a 'broker of trust' in previously trustless interactions between disparate parties in multiple industries, expanding the reach of FIs beyond the FS industry and reaching new profit pools

Disruption of the credit bureau model
Evaluate customer creditworthiness based on accurate identity data including preferences and financial history rather than relying on third parties and the mining of multiple different data sources

Refocussing around the customer
Refocus business around customer service, assisting with day-to-day decisioning and blurring the lines between financial and non-financial advisory

Public sector partnerships
Become the trusted identity provider of the public sector, assisting with social services and civic requirements such as tax filing

WORLD ECONOMIC FORUM
COMMITTED TO IMPROVING THE STATE OF THE WORLD

We are calling on FIs to champion the development of digital identity systems

FIs should champion efforts to build digital identity systems, driving the building and implementation of identity platforms through the creation of minimum viable digital identity systems

Requirements of a minimum viable identity system

1	**Identity provision** Identity provider(s) that hold trusted information and have coverage over a critical mass of users within their target area, and can therefore serve a large number of users and transactions
2	**High-transaction volume attributes** Secure storage of verified attributes that are required for common transactions (inherent attributes such as name, date of birth, nationality, national identifier number, and some assigned attributes such as address)
3	**Relying party adoption** Involvement of relying parties that offer important and frequently used user-facing services
4	**Technology platform** A technology platform that enables secure attribute exchange between identity providers and relying parties with a convenient user consent mechanism (e.g., operates on mobile and desktop)
5	**System standards** Supervisory & liability standards that guide operation and use of user information in the system and provide liability and user recourse
6	**Legal & regulatory acceptance** Legal & regulatory acceptance for using third-party verified information, attribute exchange and external use of user information

FIs could take several different approaches to creating identity systems

There are different configuration options for the development of digital identity systems, each with advantages and drawbacks

Single-Institution

Global institutions could create internal systems that stretch across the jurisdictions in which they operate

This would enable quick implementation but a single institution would likely have difficulty in gaining a critical mass of users, limiting its ability to drive system adoption and integration of relying parties

Consortium

Consortiums of financial institutions could form networks that cover large, contained oligopoly economies (such as Canada or Australia)

A consortium requires a high degree of collaboration among parties but is an effective method of getting complete coverage over a user group

Consortiums are well suited to provide identity for individuals as data storage is not centralized, increasing privacy and system resilience

Utility

Financial Institutions could create industry utilities to deliver identity services across the industry

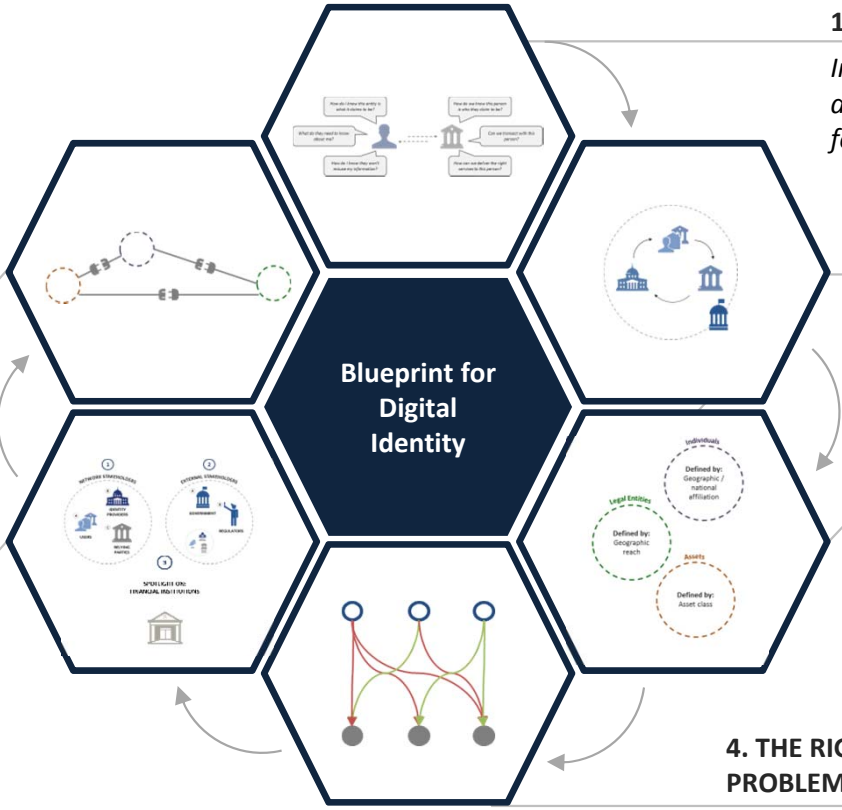
This model is effective in creating standardization and broad coverage, but implementation may be difficult due to the involvement of many different stakeholders

Utilities are a good model for legal entity and asset identity because they provide a standardized view and golden record of information

This report will provide guidance on constructing effective and robust digital identity systems while avoiding implementation pitfalls

Implementation of identity systems is extremely sensitive and therefore easy to get wrong; situational, operational and cultural factors all have important implications for identity systems, and implementation or operational failure has extremely negative consequences for both the drivers of identity system (e.g., wasted resources) and for users (e.g., data breaches).

We have studied the landscape of identity providers to understand what efforts are ongoing and which system models are best suited to different situations and to provide recommendations on system configuration and implementation.



1. INTRODUCTION

Introduces the global identity challenge and how problems with identity manifest for Financial Institutions

2. DIGITAL IDENTITY PRIMER

Summarizes key digital identity concepts

3. THE LANDSCAPE OF DIGITAL IDENTITY SYSTEMS

Describes the landscape of digital identity solutions and introduces a set of archetypes that represent the existing set of solutions

4. THE RIGHT SOLUTION TO THE RIGHT PROBLEM

Discusses how identity solutions should be configured for success

5. BENEFITS OF DIGITAL IDENTITY

Introduces the stakeholders that are involved in a digital identity network, and the types of benefits each stakeholder may derive

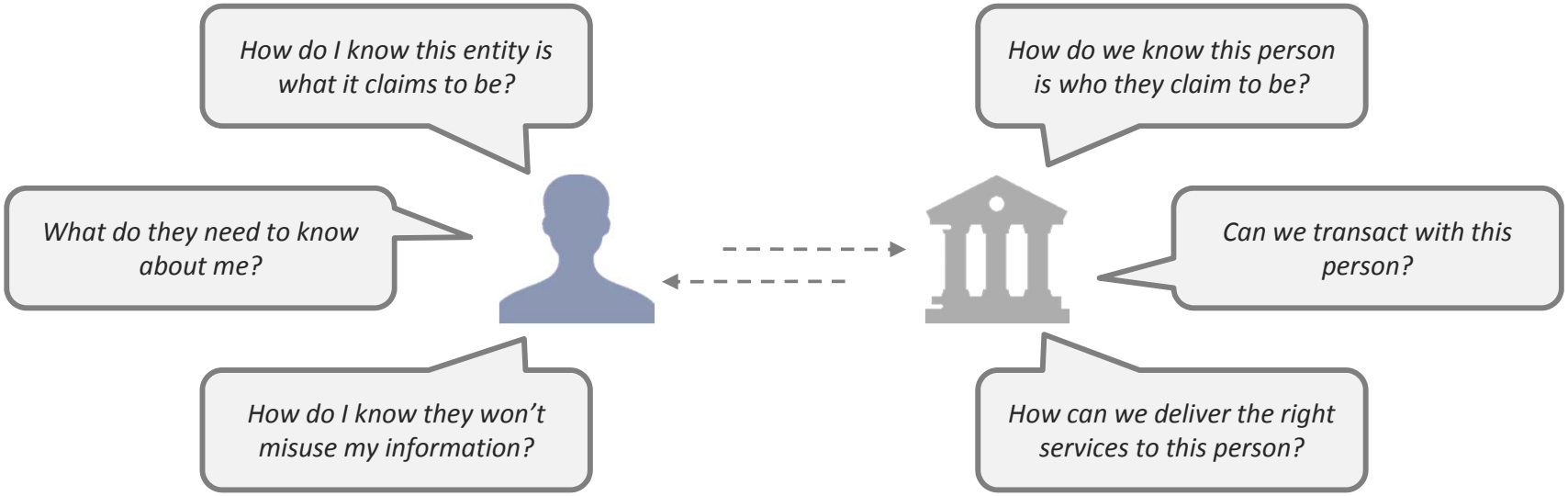
6. IMPLEMENTATION, INTERCONNECTION & CALL TO ACTION

Highlights the next steps and key stakeholders that must be involved to successfully implement a digital identity network

The Global Identity Challenge

Identity is critical to today's society

Identity is foundational to many of the transactions that occur in today's society. In any exchange with requirements about the transacting parties – they must be a certain age or reside in a certain jurisdiction – structures must be in place that allow entities to determine certain information about their counterparty, and to have confidence that the information is true.



THE ROLE OF IDENTITY IN TRANSACTIONS

Many transactions do not require identity. Some, such a crime reporting, may in fact require anonymity. However, many transactions do require identity: to determine if the necessary conditions for the transaction to occur exist, to establish a relationship for repeated transactions, or to tailor delivery of products and services.

Society requires identity systems to enable identity-requiring transactions at scale, putting methods in place that enable the formal asking and answering of identity queries at scale, to allow many day-to-day transactions to occur.

Ineffective identity systems create global challenges for people, for businesses and for society as a whole

Reliance on legacy identity systems that do not effectively enable the transactions that people and entities wish to engage in create challenges for a wide set of stakeholders.

FOR PEOPLE

Service exclusion
Individuals are excluded from key services due to their inability to demonstrate identity

Poor user experience
Services provided to users do not match their needs or are delivered inconveniently

Information overexposure
User information is overexposed, putting users at risk of identity theft and privacy breach

Process inefficiency
Proving identity involves many steps and documents

FOR BUSINESSES

Inefficient service delivery
User-facing processes are cumbersome, resulting in poor customer experience

Obscure risk
Lack of reliable information prevents businesses from accurately calculating the risk of doing business

Fraud
Businesses suffer fraud resulting from stolen or incorrect customer information, or poor authentication

Process inefficiency
Processes provide out-of-date data or require checking multiple sources

FOR SOCIETY

Service exclusion
Entities may be unable to prove attributes and therefore be excluded from key social structures

Service mismatch
Services are delivered incorrectly due to the lack of information

Fraud
Entities can use false information or misrepresent information to gain illicit access to services

Process inefficiency
Processes are highly manual and paper-based, requiring human intervention and remediation

These global identity challenges manifest as specific business problems for FIs

Identity is critical to FIs; their businesses are entirely transaction-based, involving transactions with a high degree of risk and require a high degree of certainty in completion. Global problems with identity therefore manifest as specific business problems for FIs.

ILLUSTRATIVE: BUSINESS PROBLEMS IN FINANCIAL SERVICES

Business problem	Retail / small- to medium-sized enterprise banking	Corporate and investment banking
Inefficient and costly onboarding processes	✓	✓
Inefficient, costly and ineffective know-your-customer (KYC) and due diligence processes	✓	✓
Highly manual and time-consuming compliance processes	✓	✓
Difficulty aggregating information on legal entities and determining total risk exposure	✓	✓
Difficulty attaching individual identity (e.g. corporate directors) to corporate identities	✓	✓
Difficulty identifying all transaction counterparties (e.g. third parties in trading relationships)	✓	✓
Difficulty complying with regulatory standards around data handling and privacy	✓	✓
Multiple views of the customer	✓	✓
Difficulty providing effective/suitable products and services	✓	
Lack of visibility into financial history for new customers	✓	
High fraud rates	✓	
Difficulty tracking asset origination and ownership		✓
Difficulty monitoring and tracking asset rehypothecation		✓

Many of these challenges are driven by the use of physical identity protocols to serve digital transactions

Today's standard identity systems are based on physical documents and processes, which creates many limitations.

CHARACTERISTICS OF PHYSICAL IDENTITY SYSTEMS

Document-based: Identity is based on physical records – the ability to prove identity depends on access and authentication to physical documents (e.g. passports, ID cards and records)

Siloed: Identity information is held in discrete places that are not interconnected and do not enable aggregation, which may be desired by the entity itself or required for some applications

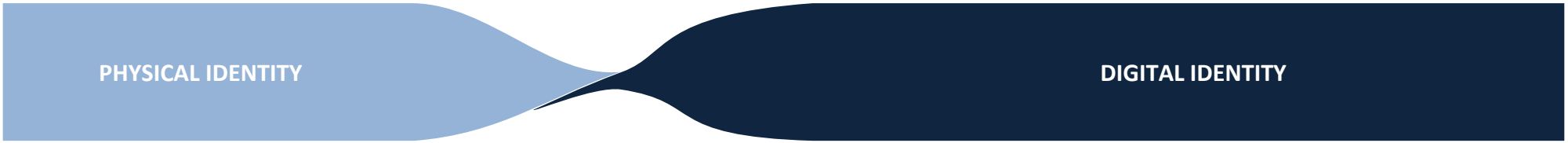
Inflexible: Identity is codified in documents as a limited and standardized set of information about an entity that cannot be easily adapted to transaction requirements

THE PROBLEMS WITH PHYSICAL IDENTITY

- *Proof of identity that is based on possession of physical documents may not require demonstration of a link between an individual and the documents (i.e., authentication), enabling use of an entity's credentials by a different user*
- *Physical identity documents can be falsified, altered or tampered with, as well as lost or stolen*
- *Physical attribute presentation and transfer create the potential for human error in transactions*

THE IDENTITY SHIFT

Identity is now at an inflection point; physical identity systems are breaking down and digital systems are emerging in response.



Physical identity *was designed to enable face-to-face transactions among entities*

The digital economy *is changing the way that identity transactions occur*

Digital identity *enables transactions in the digital world and offers improved functionality for its users*

Digital identity systems support the needs of today's world

Digital identity systems emerged as a direct response to the requirements of transactions in the digital world.

CHARACTERISTICS OF DIGITAL IDENTITY SYSTEMS

Digital-based: Identity exists as a set of digital records that the user can control and use to complete transactions

Interconnected: Proof of identity can be communicated between entities in a standardized, digital format

Flexible: Identity systems adapt to the nature of the transaction, and continuously adapt to requirements by integrating additional information to create a rich view of the user

THE PROMISE OF DIGITAL IDENTITY

- *Digital information can be protected from damage, tampering, loss and theft, with cutting-edge authentication and security protocols*
- *Digital information can be shared in streamlined, tailored and secure ways, predicated on user consent*
- *Institutions can better know and serve their customers, improving existing products and offering new products and services to the underserved*

BENEFITS

Digital identity would deliver a range of benefits to people, businesses and society.

Privacy and control
People would be able to control access to their information

Revenue growth
Financial Institutions would have opportunities to offer Identity-as-a-service

Improved compliance
Regulators would have increased access to trusted, up-to-date information

Improved service delivery
Governments could more easily and effectively deliver public services

New and maturing technologies have important implications for the creation of robust digital identity systems

These technologies may hold considerable promise for identity, and are being explored by many different players.

Data storage

New technologies may offer improved methods of storing user information and increasing user control, privacy and security

- Distributed Ledger Technology combined with encryption and cloud storage allows information to be held and transferred point-to-point in a dispersed, immutable network
- Federated identity standards, such as SAML 2.0, create interoperability between identity management networks and external applications, allowing federated identity systems to scale to large numbers of identity providers and relying parties

Data transfer

Improved attribute exchange protocols allow information to be securely shared between endpoints without risk of interception or decryption, and with more controls that create privacy for users

- Improved encryption protocols, such as Keyless Signature Infrastructure on the blockchain and hashing, provide strong protection for sensitive information and increase the reliability of digital activities
- Data transfer protocols, such as Attributed Based Credentials 4 Trust and zero-knowledge proofs, prevent the creation of metadata by concealing transaction endpoints, increasing user privacy

Authentication

Many new techniques for authenticating users are being explored for their potential to increase information security and user control in certain circumstances by linking users to their digital activities in more robust and persistent ways

- Behavioural and contextual authentication incorporate human and environmental factors to authenticate a user or device
- Biometrics, including fingerprint, retina scanning, heartbeat waveform and facial recognition based on mobile devices have potential to provide greater convenience and security and are being integrated into many anti-fraud controls

Digital identity systems have great potential but also many pitfalls in implementation

Many new identity systems are under development around the world in response to the need for digital identity and new technology capabilities. However, not all have been successful, illustrating some of the pitfalls inherent in the construction of identity systems.

PITFALLS IN IDENTITY SYSTEMS

Stakeholder rejection

- Users may not adopt the system due to poor design or distrust of the system's purpose or structure
- Stakeholders may perceive systems with limited scope and scale as valueless, and therefore not adopt them

Ineffective technology

- A poor technology platform can reduce system functionality, preventing user integration or transaction completion
- Insufficient data protection results in breaches, system compromise and data leakage

Limited support

- Systems that have support from a narrow set of interests may fail due to inconsistent efforts behind their construction and operation
- Systems that lack support from all key stakeholders may not experience sustainable and continuous uptake

Unsustainable operation

- Systems with unsustainable operating or business models will fail

Policy Changes

- Large, complex and emotive programmes such as ID cards can be susceptible to political and / or ideological shifts

Examples of identity system challenges are common…

Hack Brief: Turkey Breach Spills Info on More Than Half Its Citizens
-WIRED, April 2016

Philippine electoral records breached in 'largest ever' government hack
-The Guardian, April 2016

Aadhaar Bill passed in Lok Sabha, Opposition fears 'surveillance'
-Indian Express, March 2016

South Korea at a crossroads with ID card, data theft losses
-CBC News, October 2014

The National [UK] Identity Card scheme will be abolished within 100 days with all cards becoming invalid
-BBC News, May 2010

Identity Primer

Identity is the frontier of privacy and security in the digital world

In an increasingly borderless and digital world, privacy and security cannot be ensured through the construction of walls around sensitive information

Identity is the new frontier of privacy and security, where the very nature of entities is what allows them to complete some transactions but be denied from completing others

To understand the importance of identity and the criticality of strong identity protocols that protect against cyber-risk and suit the needs of transacting parties, it is essential to understand what identity is, and its role in enabling transactions

9-Figure Deals Lift Cybersecurity Investments To An All-Time High
-Forbes, February 2016

Cybersecurity top on government agenda
-Times of India, February 2016

In Today's Era of Data Breaches, Are You Sure Your Data Is Protected?
-Security Intelligence, January 2016

1 in 3 Americans Victim of Healthcare Data Breach in 2015
-Information Management, February 2016

U.S. presses retail banks to help millions of 'unbanked' Americans
-Reuters, February 2016

How to Fight Tax Identity Theft
-Huffington Post, February 2016

FCA fines Barclays £72 Million for poor handling of financial crime risks
-Automated Trader, November 2015

Identity is a collection of pieces of information that describe an entity

Identity is not a monolith; it is a collection of individual attributes that describe an entity and determine the transactions in which that entity can participate. While the total existing set of attributes is endless, they can be broadly categorized into three groups: inherent, inherited and assigned attributes. These attributes differ for members of three main user groups: individuals, legal entities and assets.

	For individuals:	For legal entities:	For assets:
INHERENT ATTRIBUTES Attributes that are intrinsic to an entity and are not defined by relationships to external entities.	• *Age* • *Height* • *Date of birth* • *Fingerprints*	• *Industry* • *Business status*	• *Nature of the asset* • *Asset issuer*
ACCUMULATED ATTRIBUTES Attributes that are gathered or developed over time. These attributes may change multiple times or evolve throughout an entity's lifespan.	• *Health records* • *Preferences and behaviours (e.g. telephone metadata)*	• *Business record* • *Legal record*	• *Ownership history* • *Transaction history*
ASSIGNED ATTRIBUTES Attributes that are attached to the entity, but are not related to its intrinsic nature. These attributes can change and generally are reflective of relationships that the entity holds with other bodies.	• *National identifier number* • *Telephone number* • *Email address*	• *Identifying numbers* • *Legal jurisdiction* • *Directors*	• *Identifying numbers* • *Custodianship*

Specific attributes enable entities to complete certain transactions

Identity is the total set of an entity's attributes. These attributes enable entities to participate in transactions, by proving to their counterparty that they have the specific attributes required for that transaction.

EXAMPLE: Users and transactions

Individuals	Legal entities	Assets
To purchase alcohol, users must prove that they are over the legal drinking age in that jurisdiction	*To onboard with a FI, the entity must have proof that it is a legal and non-sanctioned entity*	*Asset trading, such as trading of equities on a stock exchange, requires proof of ownership and origination*
To vote, users must prove that they are over the legal voting age, have citizenship and reside in that jurisdiction	*To transact in capital markets, the entity must have proof that it is a legal and non-sanctioned entity with an acceptable risk profile*	*Transfer of title of an asset requires proof of ownership from the entity that is transferring the asset*
To open a bank account, users must prove that they are a non-sanctioned person who is legally allowed to engage in financial transactions		

Note: Assets have identity, but are unable to act or transact on their own. Assets require custodians who are entitled to act or transact on the asset's behalf.

Identity transactions have three main aspects

Authorization	*Attributes*	*Authentication*
What must be true about the users to complete the desired transaction?	*Can users prove that they are eligible to complete this transaction?*	*Do the attributes being presented genuinely belong to the entity that is presenting them?*
Authorization is a function of the transaction and the transaction counterparty; they will determine the requirements for transaction eligibility, and make a query about certain user attributes (e.g. age, address).	Users must present their proof of attributes in response to the query. Once users present the required attributes, the counterparty must determine if they are reliable.	The counterparty will determine whether the attributes match the presenting users. If the users are able to authenticate the attributes, the transaction can proceed.

Repeated identity transactions

This model of identity transaction applies to onboarding transactions, that is, transactions where the counterparties do not have an established relationship or where the counterparty is required to gather identity information with every transaction.

Some identity relationships may have a single onboarding transaction; after initially onboarding the users and verifying them through a full identity transaction, the counterparty may use an authentication method (e.g. username and password, chip-and-PIN card) for each subsequent transaction. This allows them to verify that the same entity is transacting each time without going through the full identity transaction process.

*Note: Not all transactions require **exact knowledge** of attributes. Many transactions simply require attribute data to fall inside certain parameters (e.g. instead of knowing an individual's birthdate, a transaction may only require that the user be over a certain age); this is critical in constructing privacy-enhancing identity systems.*

Different identity transactions require different levels of assurance

The level of assurance (LoA) in an identity transaction is the degree of certainty that the transacting parties have in the veracity of the identity being presented.

ASSURANCE IN TRANSACTIONS

A high LoA in identity transactions is not always desirable, as a high LoA requires intensive onboarding and strong authentication processes that may be cumbersome for the user. The LoA required in an identity transaction should therefore generally be dependent on risk – the risk level of the transaction and the consequences of error.

DETERMING ASSURANCE LEVELS

The level of assurance of a given transaction is determined by two main factors:

1. Registration protocols: How stringently the identity provider verifies attributes when onboarding users
2. Authentication method: The strength of the authentication method used to complete transactions between the identity provider and the relying party

Low assurance transactions

Transactions that do not involve a release of information and only involve an information flow from the user to the relying party are low-assurance transactions

Examples include online registrations (e.g. signing up for a news site) and some payments (e.g. paying a parking ticket online)

High assurance transactions

Transactions that involve the release of sensitive and private information, or the transfer of money or assets, are high-assurance transactions

Examples include banking and other financial transactions, such as using an online brokerage account, and many government services

Identity systems tend to evolve inside natural boundaries…

Identity exists within networks that enable transactions between the entities inside that network. These networks tend to evolve around user groups with similar needs and characteristics. These boundaries form what are called “natural identity networks”. Every natural identity network has different needs and therefore will require different system configurations.

NATURAL IDENTITY NETWORKS

The networks that form inside the natural boundaries of identity systems for individuals are based on **geographic location** or **affiliations with a supervisory entity**

Examples include national identity systems, state or provincial identity systems, and employee management systems

The networks that form inside the natural boundaries of identity systems for legal entities are based on **national affiliation, industry** or **geographic reach**

Examples include national or global business registries and industry identifier systems

The networks that form inside the natural boundaries of identity systems for assets are based on their **asset class, origination** or **ownership**

Examples include registries of assets of a single class, or registries of assets that are all owned by a single entity

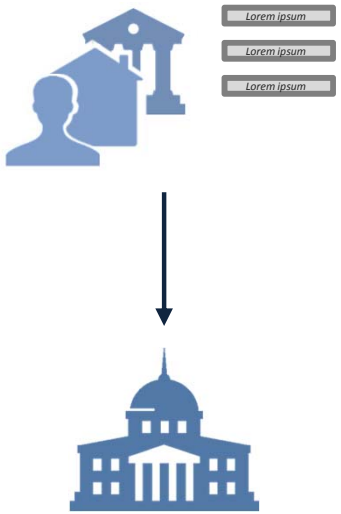
… and operate on a basic shared structure

The purpose of a formal identity system is to allow counterparties without a previously established relationship to engage in trusted transactions.

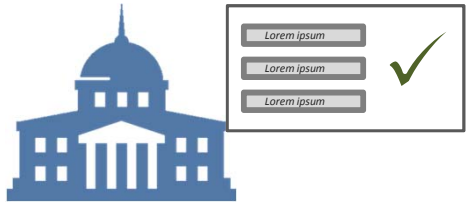
- In a formal identity system, the users' attributes are attested to by trusted third parties; these third parties issue credentials that tie their attestation to the specific attributes, with some method of authenticating the credential to the entity that is presenting it
- Users can use their wallet of credentials to engage in transactions with other entities that require some proof or knowledge of their attributes

THE STRUCTURE OF IDENTITY SYSTEMS

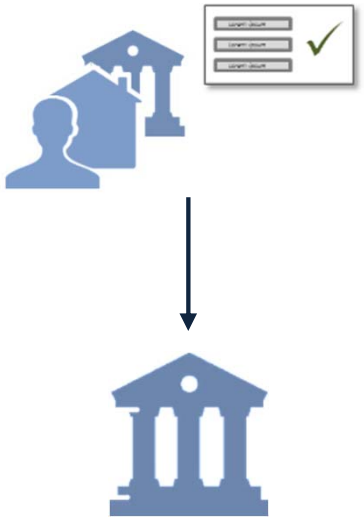
1. *The user presents a set of attributes to a third party*



2. *The third party verifies the attributes and attaches its attestation to the attributes, becoming an identity provider for the user*



3. *The user then uses the credential from the identity provider in transactions with relying parties*



Certain roles and functions must exist in every identity system

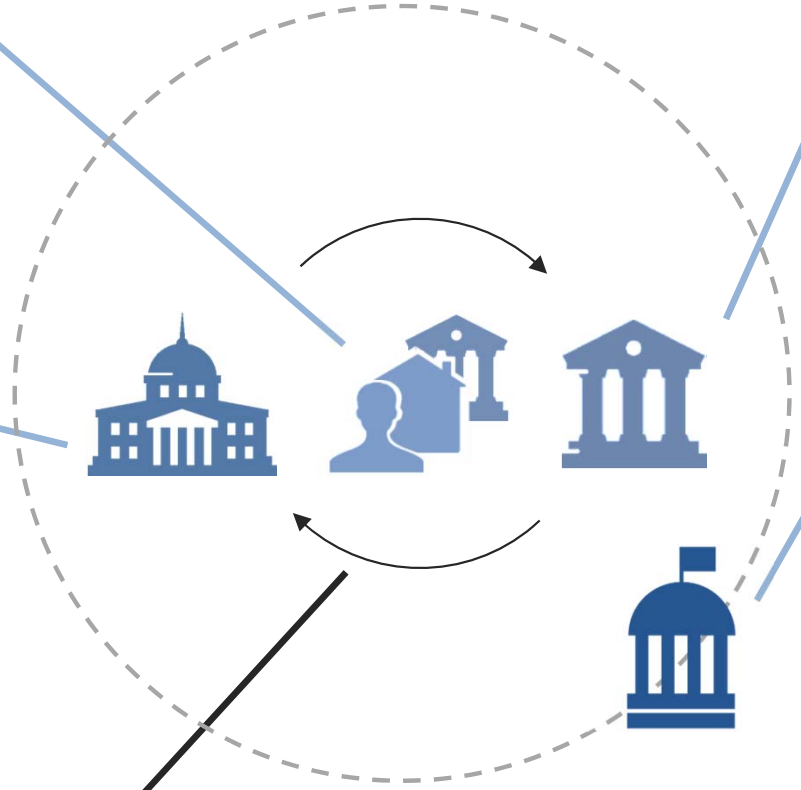
Every identity system must have four roles and one function to operate.

Users

Users are entities for which the system provides identity, for the purpose of allowing them to engage in transactions

Identity providers

Identity providers (IdPs) are entities that hold user attributes, attest to their veracity and complete identity transactions on behalf of users



Relying parties

Relying parties (RPs) are entities that accept attestations from identity providers about user identity to allow users to access their services

Governance body

The governance body provides oversight for the system and owns the operating standards and requirements

Attribute exchange platform

The attribute exchange platform completes transactions by matching identity queries from RPs with attributes from IdPs and exchanging attributes or proof of identity

Role
Function

Methods have evolved, but the concept of identity proofing has not changed over time

The fundamental concept, purpose and structure of identity systems have not changed over time, while methods and technology have made huge strides forward.

Past → **Present**

A letter of introduction is one of the oldest forms of identity documentation.

- **User:** Individuals would use a letter of introduction as an attestation of identity and character to someone they did not know
- **IdP:** The letter writers would provide attestations for various attributes of the users (e.g. that the user was a person of good character)
- **RP:** The recipients of the letter would choose whether or not to accept the attestations based on their knowledge of the IdP and their evaluation of the letter's veracity

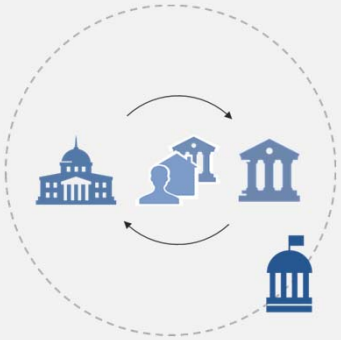
Today a passport issued by an individual's country of residence or origin is one of the most common, trusted identity documents.

- **User:** Individuals are often asked to present their passport to complete transactions that require proof of identity (e.g. entering new countries, opening a bank account, etc.)
- **IdP:** The government of that country acts as an IdP, making certain attestations about the user
- **RP:** The attestations made by the IdP are accepted by a RP based on its trust in the document, its issuer and its evaluation of whether the bearer is the true owner of the passport

Digital identity allows identity transactions to be completed through digital channels

A digital identity system has the same basic structure as a physical identity system, but attribute storage and exchange are entirely digital, removing reliance on physical documents and manual processes.

FEATURES OF DIGITAL IDENTITY SYSTEMS



Digital information storage and transfer

- User identity information is captured and stored in digital form
- User identity information is transferred between IdPs and RPs in digital form
- Form factors, such as computer or mobile devices rather than physical documents, can be used to complete transactions

Direct connectivity

- Information transfer occurs directly between IdPs and RPs, without an intermediary (although user consent can be built in) and without manual intervention (e.g. physical information entry)

THE CURRENT LANDSCAPE OF DIGITAL IDENTITY

Digital identity is not a new concept; many identity systems exist in the world today that either incorporate some digital elements or are entirely digital-based systems. The landscape of digital identity solutions is explored further in the next section of this report. These systems exist along a spectrum of maturity and degree of sophistication; however, all are designed to capture some of the benefits that digital identity brings over traditional physical-based identity systems.

Digital identity offers significant benefits over physical identity systems

Beyond offering new functionality, digital identity has significant functional benefits over physical-based identity systems.

Security

- ✗ Physical identity documents can easily be lost, stolen or replicated by illicit actors, as well as read by entities with no legitimate reason to have the user information
- ✓ Digital identity information could be stored, transferred and exposed using cutting-edge digital security protocols that would prevent against data breach, modification, loss and theft

Privacy and control

- ✗ Physical identity does not allow the release of information to be tailored to the identity transaction; identity documents display a fixed set of information that can be read by almost any entity
- ✓ Digital identity allows individuals to control the sharing of their information, to expose the minimum amount of information required for a given transaction, and shield their information from illicit access

User experience

- ✗ Physical identity requires users to manually show documents or enter identity information in transactions, resulting in a cumbersome user experience and creating potential for human error in transactions
- ✓ Digital information transfer would streamline the transaction process for users and RPs across all channels, increasing the ease of transacting for both parties and removing the potential for human error

Flexibility

- ✗ Physical identity results in the crystallization of user identity in physical documents, and a fixed view of identity that cannot be expanded to cover additional user attributes
- ✓ Digital identity would provide a flexible and scalable system that could incorporate a greater richness of identity information than is currently possible

The Landscape of Digital Identity Systems

WORLD ECONOMIC FORUM

COMMITTED TO IMPROVING THE STATE OF THE WORLD

Many digital identity systems exist in the world today, serving various natural networks

The digital identity systems that exist today fall across broad ranges of purpose, scope and sophistication. Some systems have a digital element bolted onto what is still fundamentally a physical identity system, while others are fully digital and are built to scale and expand as user needs evolve.

Disparate identity systems were studied, including systems for all user groups, to understand the landscape of digital identity solutions, categorize these systems and draw high-level conclusions on which systems best suit different needs.

TYPES OF DIGITAL IDENTITY SYSTEMS

Systems for individuals

The majority of identity systems are designed for individuals, and are often government-driven systems

Purpose:

Designed to increase financial or social inclusion and streamline the delivery of services, or to control access to internal systems for a single organization

Systems for legal entities

Identity systems for legal entities often take the form of centralized registries of information that are owned by a single government or utility

Purpose:

Intended to standardize data across entities, streamline processes and enable data aggregation at a macro level

Systems for assets

Identity systems for assets often take the form of a centralized registry or an internal system for a single organization

Purpose:

Intended to clarify ownership, standardize data or enable the operation of networked systems

The most significant differences in identity systems fall across three primary dimensions

Primary dimensions of choice are the set of choices that must be made in the design of a digital identity system that have the greatest impact on the system's function and structure.

These are not always conscious choices; they are often a natural outcome of the setting in which the system is being implemented, and the problem that the system is intended to solve or the needs that it is intended to serve. The three primary dimensions of choice are:

Nature of identity provision

Is there a single source of identity information? Are there a limited set of parties who provide attributes? Is identity provision distributed across many different entities?

Centralized: One entity stores and provides the identity information

Federated: A limited number of entities store and provide identity information

Distributed: Many different entities store and provide identity information

Number of relying parties

Is there a single RP that can access user attributes, or are there many RPs that can access user information?

One: The system has a single RP that is able to access identity information

Many: The system incorporates many RPs that are able to access identity information

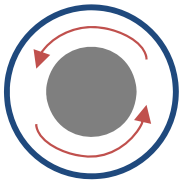
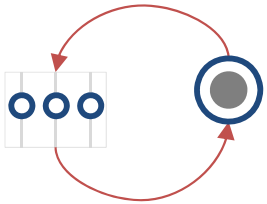
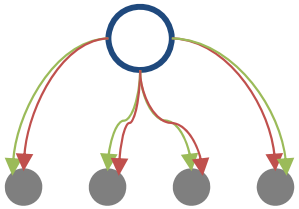
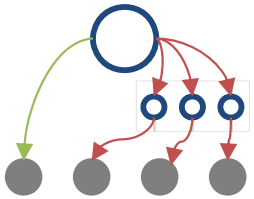
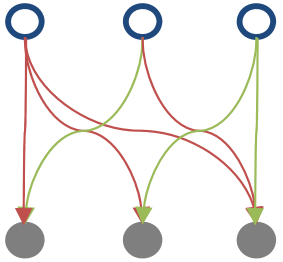
Nature of information transfer

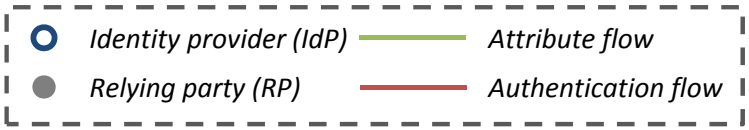
Is information transferred from the IdP to the RP for the purpose of authenticating a user, or is there a transfer of user attributes that the RP requires to execute a given transaction?

Authentication: The IdP authenticates the user for the RP, allowing the RP to complete transactions using information or records that the RP holds

Transaction: The RP requires information from the IdP for the purposes of completing a transaction for the user

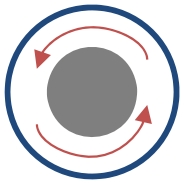
We have defined five distinct archetypes that exhibit significant differences in structure and purpose

	Internal identity management	External authentication	Centralized identity	Federated authentication	Distributed identity
Structure	 One entity acts as both the IdP and RP	 Many IdPs authenticate users to a single RP	 One IdP serves many RPs	 A set number of IdPs authenticate users to many RPs	 Many IdPs serve many different RPs
Flow of information	• The system provides users within a single network access to services that they are permissioned to access based on their attributes • All user attributes are held inside the single entity and are used to permission users to either grant or deny access to a given service or pathway	• The system authenticates users to the RP based on their authentication to one of a set of IdPs • No attributes are transferred between the IdPs and the RP; the authentication transaction is used to simply grant or deny the user access to the services offered by the RP	• The system has a single IdP that authenticates users and transfers or exposes attributes to many different RPs	• The system has a single IdP that stores user information, while a separate set of IdPs authenticate users who are attempting to transact with RPs • After authentication, the requested attributes are transferred from the IdP that holds attributes to the RP with which the user is transacting	• The system involves multiple IdPs that authenticate users and transfer attributes to many different RPs



Internal identity management solutions are designed for use by one entity

INTERNAL IDENTITY MANAGEMENT



In internal identity management systems, the same entity acts as an IdP and a RP. The entity uses information that it holds on users to permission them to access various internal services.

A good example of an internal identity management system would be a company or a government that permissions its employees or citizens to access different services based on their attributes.

KEY ARCHETYPE FEATURES

- The IdP/RP owns the required attributes needed to determine user permissions within the organization
- The system is used to control which users within a single organization or entity have permission to access certain services
- These types of solutions are generally developed by private organizations and sold as a product or service to various entities and institutions

CASE STUDIES

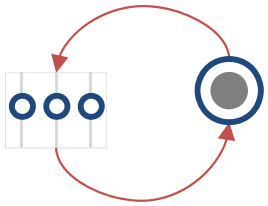
Closed Internal Management Systems

Private solutions, global

Leading software as a solution (SaaS) providers such as Salesforce, Oracle, SAP and Microsoft provide solutions that help their customers better understand, manage and interact with a set of users. SaaS has become a common delivery model for many business, as these solutions help keep users, data and applications within a closed system secure. These solutions serve a variety of industries and user groups (e.g. customers, employees, citizens, etc.).

External authentication systems facilitate access to high-traffic services

EXTERNAL AUTHENTICATION



In external authentication systems, one entity acts as both the IdP and the RP but uses an additional external set of IdPs to authenticate its users. The purpose of this system is to improve user experience for individuals or businesses when accessing online services; these users can use existing logins rather than maintaining multiple usernames and passwords for each service.

KEY ARCHETYPE FEATURES

- The system has one RP, often a government, that holds user information and leverages a set of established institutions as IdPs (e.g. FIs, telecom providers)
- The IdPs are usually trusted entities that perform strong authentication in user onboarding and are therefore trusted to provide a high level of assurance in identity transactions
- Users can use their existing authentication methods through this group of IdPs to gain access to the RP's services
- Both the RP and IdPs store user attributes – the authentication system is used to verify that the entity authenticating through the IdP should be permitted to transact with the RP
- No attributes are transferred from IdPs to the RP

CASE STUDIES

GOV.UK Verify

Public-private programme, United Kingdom

The GOV.UK Verify programme is an external authentication system that allows UK citizens to access government services online. Users verify their identity online with one of nine IdPs. Once the users are authenticated through one of these providers, they are granted access to the government service they are trying to access.

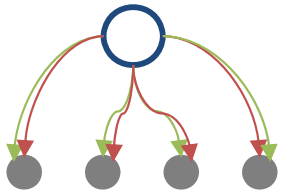
SecureKey Concierge

Public-private solution, Canada

SecureKey Concierge is a digital authentication system that allows individuals to choose a trusted credential they already have with one of a set of FIs to access government services online. The users log in with their online banking username and password and are authenticated by their bank. Once authenticated, the users are granted access to the service. No attributes are transferred in the system.

Centralized identity systems use one IdP as a single source of truth

CENTRALIZED IDENTITY



In centralized identity systems, a single entity acts as an IdP that authenticates users to RPs and transfers their attributes. These systems are often designed to streamline service delivery, enable data aggregation and provide a single view of users across multiple RPs.

KEY ARCHETYPE FEATURES

- A single IdP holds all user attributes and owns the identity system; this is often the government or another central governing body
- The IdP authenticates the user to the RP and transfers either a fixed or a tailored set of attributes to the RP to enable it to complete a transaction on behalf of the user
- Some systems require RPs to pay a fee to use the system and to gain access to user attributes
- Identity information can be transferred directly through a physical form factor (e.g. a smart card) or through a digital brokerage system

CASE STUDIES

DigID

Government programme, Netherlands

DigID is a digital authentication system for Dutch residents who are accessing government services online. Individual attributes are held in a national citizen registry; these attributes are used to authenticate users when they apply for a DigID. Individuals can then use their DigID username and password to authenticate themselves to government agencies. Their national identifier number is transferred from the national citizen registry to the RP.

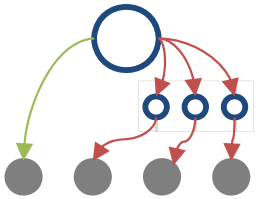
Population Registry

Government programme, Finland

The Population Registry is a national database that is owned and maintained by the Finnish government. The government acts as the IdP, transferring attributes to public and private RPs. The purpose of the system is to collect data that can be used for elections, tax filing, judicial administration, etc. Private RPs may also access this data if they pay a fee and have received user consent.

Federated authentication systems rely on third parties to grant user access to services

FEDERATED AUTHENTICATION



In federated authentication systems, one IdP uses a set of third parties to authenticate users to a range of RPs. The primary IdP is the entity that stores and transfers user attributes. These systems are designed to improve the login and transaction processes for users who are accessing online services by allowing them to use a single set of credentials to authenticate, and transferring attributes to RPs on their behalf.

KEY ARCHETYPE FEATURES

- Identity information is stored centrally by one IdP
- A set of third-party IdPs act as brokers that authenticate users to the RPs with which they are attempting to transact
- RPs are able to access user attributes from the primary IdP, often for a fee; many systems also require explicit user consent for attributes to be transferred
- In systems that allow for the discretionary transfer of attributes rather than a fixed set of attributes, the user must explicitly consent to the transfer of specified attributes from the primary IdP to the RP
- These systems are often government-driven, and the government acts as the central IdP that holds citizen or entity data

CASE STUDIES

NemID

Private sector solution, Denmark

NemID is an electronic ID, digital signature and secure email solution that provides individuals access to public and private services. The government tendered the system to the private sector. Users use a common NemID login and password, as well as unique one-time passwords to authenticate themselves to online services. User attributes are stored in a central registry.

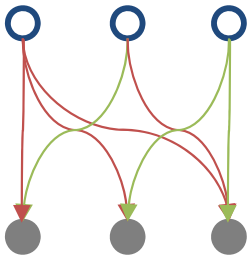
Sweden BankID

Public-private service, Sweden

Sweden has established an eID system that provides citizens and businesses access to over 300 public and private services. Digital identities are issued by a set of private entities, including large banks and a major telecommunications provider. The public sector buys identity validation services from the private sector. Private sector service providers can join the BankID system by signing contracts with eID providers for authentication. The solution has been very successful; over 9 million citizens currently use the service.

Distributed identity systems connect many IdPs and RPs

DISTRIBUTED IDENTITY



In distributed identity systems, many IdPs collect, store and transfer user attributes to many RPs. These systems are notable in that they do not rely on attributes from a single IdP. The purpose of these systems is to allow users to interact easily with many different entities in an online environment by giving them a digital "wallet" of credentials.

KEY ARCHETYPE FEATURES

- Identity information may be stored by multiple IdPs, on a distributed protocol (e.g. blockchain), or may be collected from a variety of sources and aggregated by a single entity that operates the system
- Attributes can be transferred from IdPs to RPs through a variety of methods, including smart cards or digital/mobile protocols
- These systems are often privately owned and funded; governments or other public sector bodies may not play an active role within the network
- Users own their own identities and often control which transactions occur and what attributes are transferred from one or more IdPs to the RP
- These systems may not have a governance body and instead rely on common operating standards for interoperability

CASE STUDIES

TUPAS

Private sector solution, Finland

TUPAS is an identity system in which over 10 banks act as IdPs. Individuals can log into a wide range of services with credentials from their bank. The users' full names and National ID numbers are transferred from the IdP to the RP.

Global Legal Entity Identifier Foundation (GLEIF)

Non-profit organization, global

GLEIF supports the implementation of the Legal Entity Identifier (LEI) standard. This system assigns LEIs to every entity that engages with FIs; entities can use their counterparty's LEI to access their identity information from the GLEIF's partner network.

Mobile Connect

GSMA, global

Mobile Connect is a digital identity system that authenticates the users through their device, allowing users to access a variety of services. This eliminates the need for users to have many usernames and passwords to access online services.

The potential of blockchain technology in identity

Blockchain, or distributed ledger technology (DLT), is a technology protocol that allows data to be shared directly between entities in a network, without intermediaries. DLT has certain key features that hold potential for identity systems:

FEATURES OF DISTRIBUTED LEDGER TECHNOLOGY

Low transaction cost

Distributed ledgers eliminate the need for intermediaries and therefore lower the cost of completing transactions

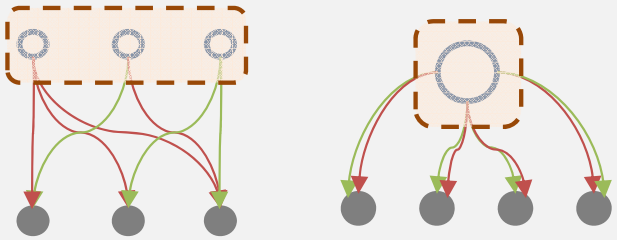
Immutability

Transaction history is maintained and verified through the network, preventing the falsification of information

Convenience

Record-keeping and transactions can be executed from any device, on- or offline

Illustrative: Applications of DLT in digital identity



DLT has potential in identity applications as an information storage and transfer mechanism within different archetypes. DLT could be applied as a distributed protocol, giving users the ability to store their identity attestations on a ledger and expose them to different RPs, or in a centralized system where the ledger would be owned by a single entity that would provide a consolidated view of the users' attestations for use in transactions, but would not reveal the nature of the credentials.

Many initiatives are currently underway that explore the true potential for DLT in identity systems; this report will not explore this topic in detail.

The Right Solution for the Right Problem

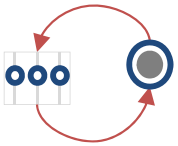
The archetypes of digital identity are built to serve very different needs

Internal identity management

Best suited to: manage user permissions inside a single entity based on internal information, to ensure the right individuals have access to the right resources and endpoints

Example: Large organizations that need an identity access and management solution to control access to their internal services with a select user group (e.g., employees, customers, etc.)

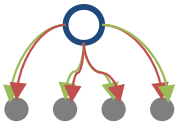
External authentication



Best suited to: streamline user access to a suite of services that are offered by a single entity and eliminate proprietary logins

Example: A government offering its citizens online services that are critical but infrequently used

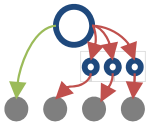
Centralized identity



Best suited to: provide a single version of the truth and a complete, accurate and standardized view of non-confidential data across different users

Example: An industry utility offering a comprehensive view of the entities in that industry to manage risk and exposure

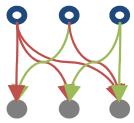
Federated authentication



Best suited to: provide a single version of the truth and a complete, accurate and standardized view of data while allowing users to authenticate to a set of third parties, thereby eliminating proprietary logins

Example: A government enabling identity transactions for its citizens through collaboration with third parties

Distributed identity



Best suited to: incorporate large numbers of IdPs and RPs, providing user convenience, control and privacy in an online environment

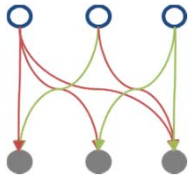
Example: A full digital economy requiring multiple independent connections between IdPs and RPs to enable user transactions

Two of these archetypes are well suited to solve broad identity problems

Centralized and distributed identity systems are best suited to provide digital identity at scale; however, these two archetypes are not equally well suited to provide identity for different user groups.

FOR INDIVIDUALS

Distributed identity

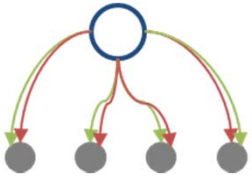


Distributed identity systems are the best fit to provide identity for **individuals** at large scale

- Distributed identity systems are built to scale to large numbers of IdPs and RPs, enabling a full set of convenient and efficient transactions for users
- These systems protect user privacy and increase control by allowing users to choose which entities hold their information, and by removing a single point of failure from the system

FOR LEGAL ENTITIES AND ASSETS

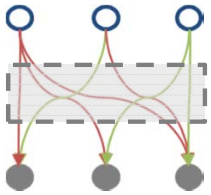
Centralized identity



Centralized identity systems are suitable to provide identity for **legal entities** and **assets** on a large scale

- Centralized identity systems offer a consolidated and standardized view of identity information, and offer the single source of truth that is required for transactions involving legal entities and assets to deliver key value to external stakeholders such as regulators

Distributed identity



Distributed identity systems are also suited to provide identity for **legal entities** and **assets** on a large scale; however, these identity systems should have a “wallet” or aggregation layer that can provide a consolidated view of the user

- Distributed identity solutions offer identity at scale, and an aggregation layer provides the single view of the user required for legal entities and assets

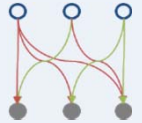
The centralized and distributed identity archetypes would also solve many of the business challenges that FIs are currently experiencing

IN RETAIL / SMALL- TO MEDIUM-SIZED ENTERPRISE BANKING

The need:

- Trusted, up-to-date individual identity information
- Ability to access additional user attributes with consent
- Ability to internally link identity information to provide a single view of the customer
- Secure repositories for user information to prevent identity theft due to stolen data

Distributed identity



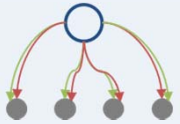
Distributed identity for individuals would allow FIs to access trusted user information and link it back to a single user identity; it would also ensure that user information would be securely stored with redundancy in the case of breach.

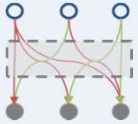
IN CORPORATE AND INVESTMENT BANKING

The need:

- Trusted, up-to-date user identity information
- Visibility into asset and user identity information
- Ability to link asset, entity identity and individual information
- Ability to aggregate identity information across entities

Centralized identity | **Distributed identity**



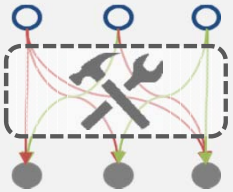


Centralized identity and **distributed identity with an aggregation layer** for legal entities and assets would allow FIs to have a consolidated, trusted source of digital attributes for these users.

Configuring and implementing an identity system require many additional choices beyond archetype selection

Configuring an identity system requires choices to be made against a secondary set of dimensions that do not have the key functional and structural importance of the primary dimensions, but have strong impact on how the system will operate. The choices made against the secondary dimensions should therefore be tailored to suit the specific needs and requirements of the natural identity network.

ILLUSTRATIVE: SECONDARY DIMENSIONS OF CHOICE



Types of IdPs and RPs: What types of entities are allowed to act as IdPs and RPs in the identity system?

Broker mechanism: How are RP queries connected with IdP attestations? Can the system support attribute exposure and attribute inquiry transactions? Does the system support transaction blinding?

Data management: Where are data stored - in a central database, on a smart card, on a distributed protocol (e.g. blockchain)? Are user attributes aggregated by a third party?

Scaling: Is the system designed to scale beyond its initial set of applications?

Business model: What is the business model that supports the system? Who funds the system?

Governance: Who is responsible for system governance and oversight? Who is responsible for system operation?

User rights: What level of control do users have over the information that is held on the system, who holds it, and when and how it is shared?

Note: This is not an exhaustive list of choices; many further choices must be made

It is impossible to provide an exhaustive list of the secondary dimensions of choice in the configuration and implementation of an identity system, or to give recommendations against each. A set of guiding principles has therefore been developed to steer secondary decision-making and to assist in delivering a robust identity system that suits the needs of its stakeholders.

Guiding Principles

The guiding principles shape the choices that need to be made against the secondary set of dimensions

A successful natural identity network is a product of the choices made against the secondary dimensions. Five principles inform decision-making around these choices and guide the development of robust, value-accretive systems.

GUIDING PRINCIPLES FOR DIGITAL IDENTITY

Social good

The system is designed as a social good that is available to all users and will deliver maximum benefit to a range of stakeholders

Privacy-enhancing

User information is only exposed to the right entities under the right circumstances

User-centric

Users have control over their information and can determine who holds and accesses it

Viable and sustainable

The system is sustainable as a business and is resilient to shifting political priorities

Open and flexible

The system is built on open standards to allow scaling and development; standards and guidelines are transparent to stakeholders

Identity systems should provide identity to all users, serve user interests and be accessible to all entities that wish to transact within them

WORLD ECONOMIC FORUM
COMMITTED TO IMPROVING THE STATE OF THE WORLD

SOCIAL GOOD

BACKGROUND

The ability to prove identity allows users to be integrated into formal financial and social systems and engage in necessary and basic day-to-day transactions; digital identity should therefore be considered a social good to which all entities should have access.

IMPLICATIONS

- The system should be designed to scale to all users and network stakeholders who wish to participate
- The public sector should have some involvement in defining the system's operating parameters and regulatory standards to ensure user interests are protected and to increase the scale of the system
- System access mechanisms (e.g. mobile platforms) should democratize access

IMPLICATIONS FOR FIs

- FIs have relationships with a large numbers of users; this scale can act as a catalyst in driving system adoption and uptake
- FIs have a key role to play in ensuring that identity systems are a tool to increase financial inclusion

CASE STUDIES

SASSA

Public-private partnership, South Africa

The South African Social Security Agency, Grindrod Bank and MasterCard have issued biometric enabled debit cards to over 22 million social security recipients. The SASSA card holds an individual's personal information on the chip, is authenticated through biometrics (fingerprint and voice pattern) or a personal identification number (PIN), and is linked directly to a bank account where social grants are deposited.

The end result is over 5 million people becoming financially included, and huge efficiencies in the distribution of social grants in South Africa.

Identity systems should be privacy-enhancing, protecting user information from illegitimate access, accidental exposure and overexposure

PRIVACY-ENHANCING

BACKGROUND

Current identity systems put users at risk, leaving user information vulnerable to privacy infringement, data leakage and overexposure. A digital identity system should protect user information, ensuring that only what is needed is revealed to RPs, and that these parties are only using the data for the disclosed purposes.

IMPLICATIONS

- All attributes, including demonstrated behaviour and preferences, should be covered in an identity system
- Attribute transfer should use new information exchange protocols that allow endpoint blinding
- The brokerage mechanism that connects the endpoints of identity queries should allow only the minimum required information to complete attribute inquiry or attribute exposure transactions to be exposed to the RP
- Attributes should only be stored by IdPs with adequate data security (as defined by system standards)
- Users or custodians should have visibility into requested identity transactions and a defined recourse method if their information is being misused
- The storage of sensitive information should be non-centralized to reduce the severity of consequences and the impact on users in the event of a data breach

IMPLICATIONS FOR FIs

- FIs should build cyber-resilient identity systems and meet standards set by the governance body around data protection and storage
- FIs will need to seek user consent to gain access to or share attributes

CASE STUDIES

TUPAS

Private identity solution, Finland

In the Finnish TUPAS system, a set of FIs act as IdPs and transfer user information on their behalf to RPs. The user has visibility into which attributes are being requested by the RP, and must provide consent for the exchange to occur .

Drivers' Licences

Government solutions, global

Traditional drivers' licences are a commonly used form of identity. However, they compromise privacy by permitting the RP to read all the user's information, rather than just the information required for the transaction.

Identity systems should give users control over the storage and transfer of their personal information

USER-CENTRIC

BACKGROUND

Many identity systems have failed due to a lack of user uptake, driven by concerns around the function and purposes of these systems. A successful digital identity system that serves as a social good should place the user (or the user's custodians) in control over identity information.

IMPLICATIONS

- The mutuality of identity should be considered; users or custodians must have clear visibility into who is requesting their information and for what purpose
- Identity transactions should require consent; exceptions must be clearly defined and communicated, and users should be advised of when their information has been accessed
- Users should be able to revoke consent
- Users should have control over where their personal information is stored
- Users should be able to easily update their information with IdPs

IMPLICATIONS FOR FIs

- FIs will be able to request identity information from users in order to tailor products and services
- FIs will require user consent to share identity information

CASE STUDIES

ConsenSys

Private solution, USA

In the ConsenSys system, users are able to upload their information and have complete control over who their data are exposed to. Users do not choose who stores their data because all identity information is stored on uPort – a user-controlled application that operates on the blockchain.

SecureKey Concierge

Public-private solution, Canada

The SecureKey Concierge system allows Canadian citizens to access government services online by authenticating through any of a large number of FIs with which they already transact.

Identity systems should be designed as businesses that are viable and sustainable in the long term

VIABLE AND SUSTAINABLE

BACKGROUND

Implementing a digital identity system represents a significant effort for all stakeholders; stakeholders must have assurance that their investment will be worthwhile. The system must therefore be designed as a viable and sustainable project.

IMPLICATIONS

- The public sector should have some role in system development and implementation to represent user interest, to drive uptake and to ensure regulatory participation
- The private sector should be involved in system development and implementation to provide executional ability, and operational viability and ensure the system is cost-effective
- Both the public and private sectors should play a role in developing operational standards, including:
  - Liability and dispute resolution
  - Business model
  - Information collection, storage and transfer
  - Levels of assurance
  - Technical requirements
  - User consent models
  - Auditing

IMPLICATIONS FOR FIs

- FIs have a key role to play as important and trusted private entities in shaping the system's operational requirements and standards
- FIs will have the opportunity to monetize identity-as-a-service

CASE STUDIES

National ID Cards

Government solution, United Kingdom

The UK government introduced national ID cards as a personal identification document. The system was scrapped in January 2010, as the incoming government stated the system was "wasteful, bureaucratic and intrusive", posing a significant threat to the privacy and security of personal information.

Clarient Entity Hub, DTCC

Private identity solution, global

Clarient Entity Hub is a utility designed to manage data and regulatory complexity for parties engaging in financial transactions. It aims to increase transparency across financial markets and is offered as a paid service to other entities.

Identity systems should be built on open technology and data standards, and should be designed to integrate new parties and serve changing user needs

OPEN AND FLEXIBLE

BACKGROUND

Identity systems that are static and designed for a single purpose are by nature limited in scope and have low resilience to environmental changes. A resilient identity system should accommodate changing requirements and integrate new parties.

IMPLICATIONS

- The system must be built on open technology standards
- The system must be built on open data standards
- The system must have clear standards around IdPs and RPs, such that new entities can join the system and adhere to all standards and requirements
- The system must have a governance body that will continuously adapt requirements and standards and monitor system performance

IMPLICATIONS FOR FIs

- Open technology and data standards will reduce barriers to users switching institutions

CASE STUDIES

X-Road

Government solution, Estonia

The Estonian digital identity system is built on a common technology framework, called X-Road. This framework creates interoperability between different databases, hugely increasing the digital identity system's functionality and effectiveness.

European Union E-Identity Legislation

Public sector solution, EU-wide

The EU E-Identity legislation sets requirements for member states issuing identity to citizens to ensure mutual recognition and scale of identity systems across Europe.

The established implications should help guide decision-making around configuring identity systems

Building a successful identity network is difficult. A series of choices need to be made to ensure the system delivers value to all stakeholders and gains traction and acceptance.

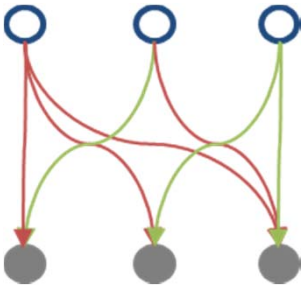
- The highest-level considerations in the development of an identity system are the user group and the need that the system will serve, and the archetype structure that should therefore be considered.
- Once these considerations have been settled, the secondary dimensions of choice should be considered against the guiding principles of digital identity.

1
Problems and user groups

The highest consideration is the user group and the problem that the identity system is designed to solve; this will determine the limits of the natural identity network

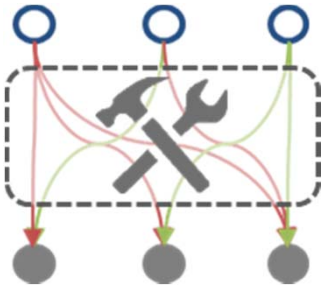
2
Primary dimensions of choice

The user group and target problem will guide the selection of an appropriate identity archetype



3
Secondary dimensions of choice

The guiding principles for identity and their implications will help determine what structural and configuration choices should be made against the secondary dimensions of choice



These implications are meaningful for entities within the digital identity network

When configuring identity systems, stakeholders will have a set of decisions to make at each stage of the process.

ILLUSTRATIVE: Some open questions for identity stakeholders

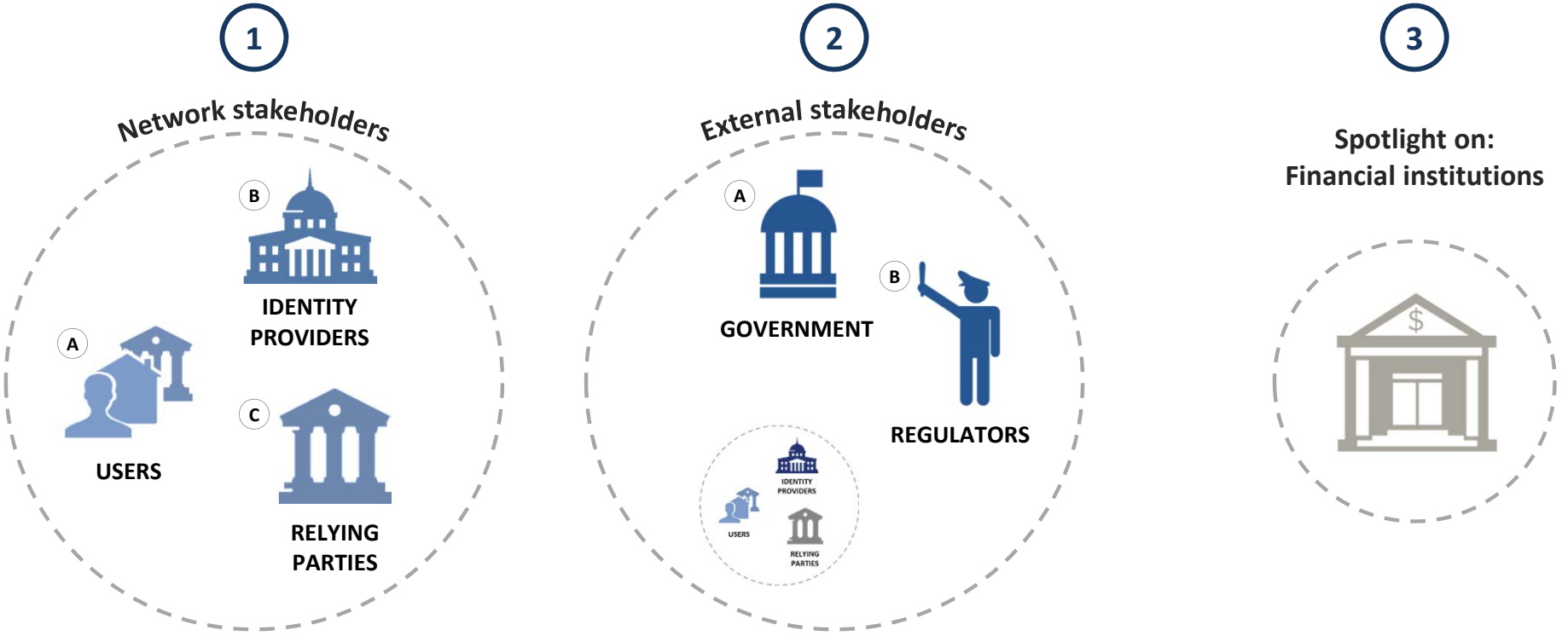
1. **Problems and user groups**
   - Which user group does this system serve? What problems will the system solve?
   - What unique characteristics will affect this user group's acceptance and use of an identity system?
   - Which archetype is best suited to solve this problem?
2. **Primary dimensions of choice**
   - Which entities should act as IdPs in this system?
   - What type of RPs should be included in this system?
   - What type of information must be transferred in the system?
3. **Secondary dimensions of choice**
   - What technology standard and trust framework will the system use?
   - What assurance model will the system use?
   - Should the system use an identity-as-a-service, fee-for-transaction business model?
   - How will the governance body be organized? What entities will be involved in system governance?
   - How will the user give consent in transactions?
   - Will any exceptions to user consent requirements be allowed?
   - How will the public sector be engaged in shaping the operational standards?

Benefits

The implementation of digital identity networks would benefit a set of different stakeholder groups

Identity systems that are constructed based on this guidance will deliver benefits both to the stakeholders involved directly in the identity network and to external stakeholders. FIs, specifically, would accrue deep benefit as a result of the implementation of digital identity.

STAKEHOLDER GROUPS



What benefits would accrue to network stakeholders?

Network stakeholders are parties who are involved in the core operation of the network itself. The network stakeholders are users, IdPs and RPs.

A

USERS

Privacy and control
Users are able to control who has access to their attributes

Security
User attributes are held in safe and secure locations

Convenience
Digital attribute transfer allows users to transact in an efficient manner

Transparency
Users have visibility into how and when their attributes are exposed

B

IDENTITY PROVIDERS

Revenue growth
IdPs can charge fees for processing identity transactions

Decreased risk and liability
IdPs understand their liability in the event of data loss or breach

Competitive positioning
IdPs can forge a strong relationship with users and position themselves as a critical part of the digital economy

Improved products and services
IdPs can use detailed and trusted customer information to deliver tailored services

C

RELYING PARTIES

Information accuracy
RPs have access to trusted, verified identity information

Decreased transaction abandonment
A streamlined user experience removes barriers to completing transactions

Service tailoring
RPs can provide more tailored products and services

Decreased risk and liability
RPs understand their liability in the event of data loss or breach

Service provision
RPs can differentiate between illicit and legitimate users

What benefits would accrue to users?

USERS

Privacy and control

1. Privacy and control

- Users would have full control over which IdPs hold their attributes
- Users consent would be required before IdPs could expose attributes to RPs
- User data would not be sold by third parties
- The minimum amount of user information required would be transferred during transactions

Security

2. Security

- User attributes would only be held by entities meeting system standards and requirements for information handling and storage
- Digital attribute storage would make identity information resistant to damage, destruction or loss
- Users would have the ability to disperse their identity information, creating contingency if an IdP suffered a data breach or data were erased or stolen, and reducing the impact of a data breach on the user

Convenience

3. Convenience

- Digital identity and digital attribute transfer would simplify and improve the user experience in transactions, eliminating the need for users to track multiple authentication methods (e.g. usernames and passwords) and manually submit personal information during transactions
- Attributes would be transferred digitally, removing the potential for human error and subsequent information remediation
- Users would be able to easily update information held with their IdPs and would not have to deal with transactions being executed based on inaccurate or out-of-date information

Transparency

4. Transparency

- Users would have visibility into which attributes would be exposed and to what entity during identity transactions

What benefits would accrue to users?

USERS: Case study

Estonia's e-government system protects citizen information, provides an extremely convenient experience for users and allows them to feel ownership over their data.

E-Government

Government solution, Estonia

- The Government of Estonia has created a digital interface between citizens and government agencies. The government holds citizen information in a centralized Population Registry and acts as the IdP and governing body, transferring reliable and trusted data to RPs.
- Citizens are each assigned an eID identifier that they can use to log on to the State Portal, which provides access to dozens of services, from voting, to updating automobile registries, to applying to universities. The government transfers the attribute information needed to complete each transaction from the Population Registry to the RP, and citizens are able to see what entities have accessed their information.
- Citizens of Estonia have the ability to view who has accessed their records, how often and for what purpose. This transparency allows citizens to feel ownership over their data, as they are able to see how the information is being used.
- A compelling example is the Electronic Health Record – a nationwide system that integrates data from various healthcare providers into a single portal. Users are able to log on to a Patient Portal to control their treatment and manage their healthcare information.

Chekk allows users to own, manage and share their personal information

Chekk

Private sector solution, Global

- Chekk is a mobile solution that provides users with a secure wallet of their personal attributes and allows them to share up-to-date information with the entities with which they transact.
- In the Chekk system, only the information required for a transaction is supplied, meaning that the user is in control and their privacy is protected.

What benefits would accrue to IdPs?

IDENTITY PROVIDERS

Revenue growth

1. Revenue growth

- IdPs would complete identity transactions for RPs; this would allow them to monetize identity-as-a-service through per-transaction fees or other business models

Defined risk and liability

2. Defined risk and liability

- Liability guidelines would be clearly defined and communicated; IdPs would be clear about their liability in the event of data loss or breach, or contravention of the standards for identity provision

Competitive positioning

3. Competitive positioning

- IdPs would be able to forge a strong relationship with users and position themselves as a critical part of the digital economy, given their unique insight into users and their established position of trust

Improved products and services

4. Improved products and services

- IdPs would have increased access to detailed and reliable user information that would allow them to better tailor processes, products and services
- IdPs could begin to draw on non-standard user attributes to better manage and evaluate risk (e.g. health records)
- Secure digital identity protocols and digital attribute transfer would improve user experience and expand the number of services that IdPs could securely provide online

What benefits would accrue to IdPs?

IDENTITY PROVIDERS: Case study

A set of banks act as IdPs in the TUPAS system, providing individuals with access to over 180 public and private services.

TUPAS

Private sector solution, Finland

- The Federation of Finnish Financial Services drove the creation of a bank identity system called TUPAS, designed to improve user access to online services.
- The RPs pay for the service (initiation fees, monthly fees and fees for set transaction volumes). Users may also be charged on a monthly basis, depending on their relationship with their bank.
- While a group of telecoms in Finland offer a competing service, as of February 2016, 95% of all online service logins were processed through TUPAS. Only 2% of online service logins were processed through the competing system. This may be due to the government's strong adoption of TUPAS, citizen loyalty towards government and banks, or the fact that it was the first successful service in the region. TUPAS has established a new revenue stream for banks as well as a strong competitive position.
- With most banks, the user must approve and certify that the data being transferred from the bank to the RP are accurate, eliminating any liability risk for the IdP.

What benefits would accrue to RPs?

RELYING PARTIES

Information accuracy

1. Information accuracy

- RPs would have access to trusted, verified identity information matched to the level of assurance required for their products or services; this would eliminate the need for information remediation and for information cross-checks through paid third-party services
- Digital attribute exchange would eliminate the potential for human error in transactions

Service tailoring

2. Service tailoring

- RPs would be able to provide more tailored products and services to users by requesting access to identity information beyond what they would traditionally require to complete transactions

Service provision

3. Service provision

- More reliable and accurate identity protocols would give RPs greater ability to differentiate between illicit and legitimate users, and to deny or provide services accordingly

Decreased transaction abandonment

4. Decreased transaction abandonment

- A more streamlined user experience would remove barriers to completing transactions (e.g. forgotten login information, required account creation, rejected billing information) and would therefore reduce the rates of users' transaction abandonment

Decreased risk and liability

5. Decreased risk and liability

- Liability guidelines would be clearly defined and communicated; RPs would be clear about their liability in the event of data loss or breach, or contravention of the standards for identity provision

What benefits would accrue to RPs?

RELYING PARTIES: Case study

The Population Registry is a central database that stores identity information – the data are trusted by many entities in Finland as a comprehensive source of up-to-date information about citizens, assets and legal entities.

Population Registry

Government programme, Finland

- The Population Registry is a national database owned and maintained by the Finnish government. The government acts as the IdP, transferring attributes to public and private RPs.
- Citizens are required to provide up-to-date information to the Population Registry, such that IdPs can trust that the information they are receiving is accurate.
- Public RPs that require attributes to complete transactions can use citizens' national ID numbers to access data held in the Population Registry. The necessary attributes are transferred digitally from the registry to the RP.
- Private RPs can also subscribe to the Population Registry and access information (with consent) to provide better products and services to their users.

What benefits would accrue to external stakeholders?

External stakeholders are parties that are not involved in the system's day-to-day operation, but are key stakeholders in the system. The external stakeholders are governments and regulators.

A

GOVERNMENTS

Process streamlining and efficiency
Governments can more efficiently interact with their citizens, saving time and money

Improved service delivery
Governments can more easily identify and deliver services to various groups of citizens

B

REGULATORS

Tracing of assets
Regulators can more effectively trace asset origination and ownership

Transparent view of entities
Regulators can access an aggregated view of legal entities across their hierarchies

Improved compliance
Regulators can access trusted, up-to-date attribute information for users, improving the effectiveness of the overall compliance process

Data standardization
Data collection and storage can be standardized across all FIs, reducing friction in data aggregation

What benefits would accrue to governments?

GOVERNMENTS

Process streamlining and efficiency

1. Process streamlining and efficiency

- Governments would be able to more efficiently interact with their citizens, saving time and money in the delivery of services such as tax filing and the distribution of social assistance

Improved service delivery

2. Improved service delivery

- Governments would be able to leverage accurate identity information to more easily identify the individuals and entities that are eligible to access given services
- Governments would be able to easily identify and deliver services to those who might be financially or socially excluded due to the lack of traditional identity information

What benefits would accrue to governments?

GOVERNMENTS: Case study

The Aadhaar programme was introduced in India to increase social and financial inclusion by providing identity for all Indians residents, many of whom previously had no means of proving their identities.

Aadhaar

Government programme, India

- The Aadhaar card was developed to improve financial inclusion in the country. The Unique Identification Authority of India (UIDAI) acts as the central IdP, controlling who has access to the data that they collect and store.
- To receive a card, individuals submit various documents to a local registrar. If they are unable to provide documentation, an "introducer", such as an elected representative or a local teacher or doctor, can vouch for the person's identity. This parallel process decreases the chance of UIDAI storing inaccurate information or providing social services to illegal immigrants or other illicit actors. The UIDAI has a database that holds information such as name, date of birth, and biometrics data that may include a photograph, fingerprint, iris scan, or other information.
- The Aadhaar program has been very effective in increasing financial inclusion with over 1 billion people enrolled for accounts, however there are still some outstanding concerns about information protection and privacy.

The Estonian e-Residency program allows non-Estonian citizens to gain digital residency in the country.

E-Residency

Government programme, Estonia

- The e-Residency program allows non-Estonian citizens to get a digital ID card that enables them to use Estonian private and public services and to use secure digital signatures. The purpose of the program is to create a virtual business environment and continue to position Estonia as a hub of the digital world
- Since its inception in December 2014, almost 10,000 people have applied for e-Residency and over 400 have established an new company domiciled in Estonia.

What benefits would accrue to regulators?

REGULATORS

Tracing of assets

1. Tracing of assets

- Regulators would be able to more effectively trace asset origination and ownership, increasing their ability to track the proceeds of criminal activity
- Asset rehypothecation could be traced, ensuring that assets would not be rehypothecated beyond their total value

Transparent view of entities

2. Transparent view of entities

- Regulators would have access to an aggregated view of legal entities across their hierarchies, increasing their ability to evaluate systemic risk and manage stability

Improved compliance

3. Improved compliance

- Access to trusted identity information would increase the ability of FIs to be compliant with anti-money laundering, know-your-customer and other regulations within their jurisdiction
- Access to trusted information on legal entity and asset identity would allow FIs to more accurately detect money laundering and other suspicious transactions
- Access to trusted digital attributes would allow FIs to automate their compliance processes to some degree, potentially allowing regulators to increase the required frequency of compliance reviews

Data standardization

4. Data standardization

- Data collection and storage could be standardized across all FIs, reducing friction in data aggregation

What benefits would accrue to regulators?

REGULATORS: Case study

GLEIF is an organization that supports the implementation of the Legal Entity Identifier standard – this standard might ultimately become a common thread between identifier systems in an effort to create a standardized global view of legal entities.

Global Legal Entity Identifier Foundation (GLEIF)

Non-profit organization, global

- GLEIF manages a network of Local Operating Units that issue Legal Entity Identifiers (LEIs) to legal entities worldwide.
- Legal entities engaging in financial transactions submit a standard set of attributes to a Local Operating Unit, which validates them against third-party records and then issues an LEI. GLEIF holds the master file of all LEIs and associated entity information.
- The system was introduced by financial regulators to improve micro- and macro-prudential risk assessment and management, increase market transparency and improve the accuracy of financial data.
- Beyond financial services and regulation, the goal 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).
- Over 430,000 LEIs have been issued since October 2015. The LEI is intended to become the link between all other identifier systems (e.g. know-your-customer systems, business register codes, etc.). This would allow regulators to have a consistent and comprehensive view of all legal entities and financial instruments globally.

FIs have key features that would give them structural advantages within identity systems

FIs have unique advantages that make them well-suited to playing key roles in digital identity networks.

ADVANTAGES OF FIs IN DIGITAL IDENTITY

FIs are highly reliant on identity

Identity is central to the function of FIs, while they bear a large part of the cost of ineffective identity protocols

FIs are connected to many key identity stakeholders

FIs have standing relationships with users, governments, regulators and other key stakeholders, and have experience working with these groups on key concerns while balancing competing interests

FIs are trusted institutions

FIs are more trusted by consumers to hold personal information than other institutions, such as governments, telecoms and technology companies

FIs have existing business models that do not require directly monetizing customer information

CASE STUDIES

iDIN

Private sector solution, Netherlands

iDIN was created to capitalize on the large investments that banks have made in onboarding their customers; banks already collect highly trusted identity information and are well positioned to transfer it to other parties.

NemID

Private sector solution, Denmark

To maximize the adoption of NemID, the governing body wanted to cooperate with private actors who have frequently used services; banks not only interact with individuals on a regular basis, but are also seen as trusted institutions that already store user identity.

SecureKey Concierge

Public-private programme, Canada

SecureKey partnered with nine banks that are trusted and hold accurate data; this data can be used to authenticate individuals in the system.

What benefits would accrue to FIs from the implementation of digital identity?

The benefits to FIs of implementing digital identity fall into six categories:

FINANCIAL INSTITUTIONS

Improved products and services
FIs will be able to use detailed and trusted customer information to deliver tailored services to customers

Operational efficiency
Digital attribute transfer and handling will allow FIs to streamline and automate many processes, eliminating human error

Decreased fraud
The secure, digital storage of user information will reduce fraud resulting from stolen information or compromised authentication

Improved compliance
Digital attribute handling and greater access to user identity will allow FIs to complete compliance processes more easily and accurately

Revenue growth
FIs will have the opportunity to increase revenue from improved products and services as well as to offer identity-as-a-service

Better user experience and competitive positioning
FIs can offer a streamlined user experience and position themselves as a critical part of the digital economy

What benefits would accrue to FIs from the implementation of digital identity?

FINANCIAL INSTITUTIONS

Improved products and services

1. Improved products and services

- FIs would have increased access to detailed and reliable user information that would allow them to better tailor processes, products and services such as:
  - Risk scoring for insurance products
  - Financial advisory
  - Asset management
  - Credit scoring
  - Loan adjudication
- FIs could begin to draw on trusted information, with consent, to better manage and evaluate risk; secure digital identity protocols and digital attribute transfer would improve user experience and expand the number of services that FIs could securely provide online

Operational efficiency

2. Operational efficiency

- FIs would be able to access user information in a consolidated, digital form through queries in the digital identity network; having attributes in a consolidated digital form would provide a single view of the customer and allow FIs to streamline customer-facing operations, such as onboarding, as well as many back-end processes
- Digital identity for assets would allow FIs to track financial products and assets more closely, through greater visibility into ownership and the resolution of rehypothecation concerns

Decreased fraud

3. Decreased fraud

- User information would be held only by entities that follow standards around data protection; this would reduce fraud (such as card-not-present transactions made using shipping and billing information stolen in large-scale data breaches)
- Digital authentication methods would reduce fraud resulting from hacked or compromised user accounts

What benefits would accrue to FIs from the implementation of digital identity?

FINANCIAL INSTITUTIONS

Improved compliance

4. Improved compliance

- Digital identity would give FIs access to trusted, up-to-date attribute information for users, improving the accuracy of know-your-customer processes
- Digital information transfer and storage would allow FIs to complete their compliance processes more quickly and easily, allowing faster processing and reducing time spent on information remediation and correcting human error
- Compliance processes could be automated and executed on more regular cycles
- Digital identity would give FIs better visibility into corporate ownership structures and the identity of corporate directors to improve corporate know-your-customer processes
- Digital identity would give FIs better visibility into asset origination and ownership

Revenue growth

5. Revenue growth

- FIs could monetize identity-as-a-service through business models such as subscription fees with RPs or fee-for-transaction services for high-assurance identity transactions, including:
  - Authentication
  - Digital signatures
  - The completion of identity transactions for RPs, such as providing attribute information (e.g. providing shipping information to merchants) or providing information about attributes (e.g. attesting to a merchant that a user is over a certain age based on date of birth)

Better user experience and competitive positioning

6. Better user experience and competitive positioning

- By collaborating with governments, public sector entities and other private sector entities, FIs would become part of a trusted ecosystem working on developing the digital economy
- As trusted safeguards of user information, FIs would increase the strength of their relationships with users

What benefits would accrue to FIs from the implementation of digital identity?

FINANCIAL INSTITUTIONS: Case studies

Aire is able to assist individuals who lack traditional credit information by using non-traditional user attributes to build a new credit score.

Aire

Private company, United Kingdom

Aire, a UK-based start-up, offers an alternative to traditional credit-scoring techniques. Aire allows individuals to submit a wide range of materials that are used to evaluate the individual's creditworthiness; for example, a user could submit utility or Netflix bills.

Know-your-customer utilities provide FIs with access to trusted, up-to-date attribute information for users, improving the accuracy of individual and corporate know-your-customer processes.

Industry Know-Your-Customer Utilities

Private solutions, global

Industry know-your-customer utilities, such as Thomson Reuters' OrgID or DTCC's Clarient Entity Hub, are intended to serve as reliable repositories of identity information on legal entities, eliminating the need for entities to perform know-your-customer requirements on their counterparties in financial transactions and giving them access to reliable and current information.

FIs in the TUPAS system are the only entities to hold and transfer user information, allowing them to monetize identity-as-a-service through business models such as subscription or fee-for-transaction services with RPs.

TUPAS

Private sector solution, Finland

In the TUPAS system, RPs must pay IdPs (in this case, a consortium of banks) to access trusted and accurate user attributes.

Future-State Applications

Digital identity offers FIs improved and new capabilities

Beyond the first-level benefits of digital identity that FIs would receive as a result of participating in an identity system, we have explored some future-looking use cases that illustrate additional capabilities that digital identity might offer to FIs.

POTENTIAL FUTURE-STATE APPLICATIONS

1. Tailored risk profiles

2. International resettlement

3. Attributes tied to payment tokens

4. Digital tax filing

5. Determining total risk exposure

6. Identifying transaction counterparties

7. Linking individual identity to corporate identity

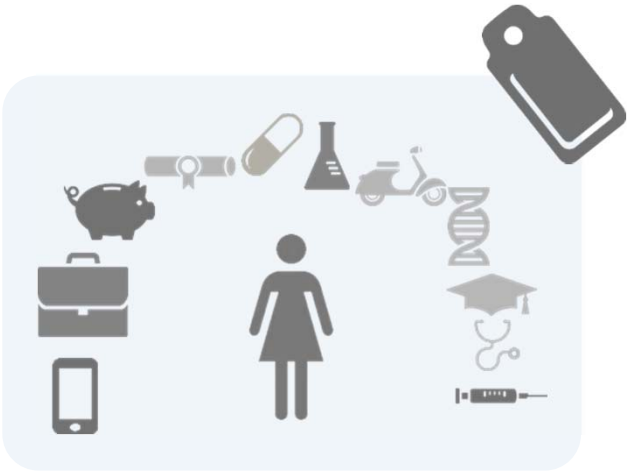
8. Tracking total asset rehypothecation

What additional capabilities can digital identity offer to FIs?

1. TAILORED RISK PROFILES

CURRENT STATE:
FIs currently create risk profiles for individuals and legal entities using the limited information that is collected when customers are onboarded and predictive algorithms to provide relevant and tailored products and services to their customers.

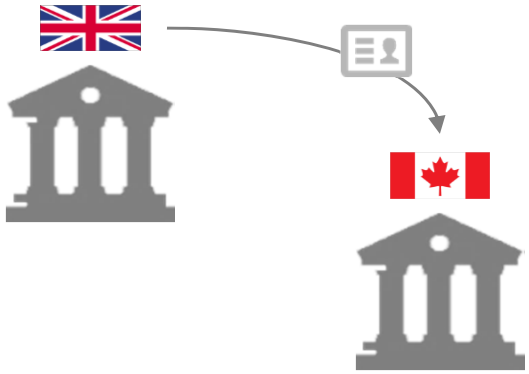
HOW WOULD DIGITAL IDENTITY HELP?
FIs could leverage trusted user attributes, with a user's consent, to more effectively build risk profiles for their customers and therefore tailor credit- and risk-based products. This enhanced user experience would ultimately lead to increased customer stickiness and offer growth opportunities for FIs.



2. INTERNATIONAL RESETTLEMENT

CURRENT STATE:
Today's onboarding processes require every FI to onboard a customer from a zero-knowledge state, resulting in difficulty opening accounts for entities that are unable to prove their identities, and disregard of financial history.

HOW WOULD DIGITAL IDENTITY HELP?
Users could transport their digital identity across jurisdictions and use it to easily gain access to financial and other services in their new place of residence; the attestations and attributes held by the user's original FI(s) would serve as the basis for new FIs to become IdPs. This would eliminate the need for the recipient FI to perform the costly and labour-intensive know-your-customer process that would otherwise be required. In addition, it would reduce the time and effort needed for FIs to onboard users, and allow them to incorporate trusted, historical information.



What additional capabilities can digital identity offer to FIs?

3. ATTRIBUTES TIED TO PAYMENT TOKENS

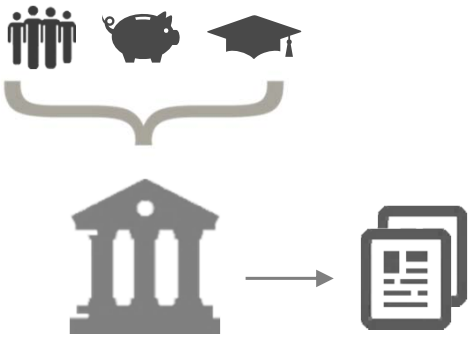
CURRENT STATE:
When completing transactions, customers are required to manually provide their attributes (e.g. confirmation of age, shipping information) or proof of attributes to merchants at the point of sale.

HOW WOULD DIGITAL IDENTITY HELP?
FIs could automatically provide customer attributes to merchants, streamlining and securing the transaction process for the merchant and customer. The digital transfer of attributes would eliminate the potential for human error in information transfer and dramatically reduce information remediation and transaction abandonment for the RP.
Note: This automatic transfer of attributes could be supported by an additional factor of authentication (e.g. mobile or behavioural authentication) to prevent fraud.

4. DIGITAL TAX FILING

CURRENT STATE:
Individuals and businesses currently file their taxes based on the aggregation of pieces of information from multiple sources (e.g. FIs, employers, educational institutions, etc.).

HOW WOULD DIGITAL IDENTITY HELP?
In collaboration with governments, taxes could be automatically completed and filings generated by customers' chosen FIs, using their complete knowledge of customers' financial holdings, assets, income and personal circumstances. With user consent, all of this information would be available through a robust digital identity network. This would allow the typically complex and tedious tax filing process to be completed efficiently and accurately.

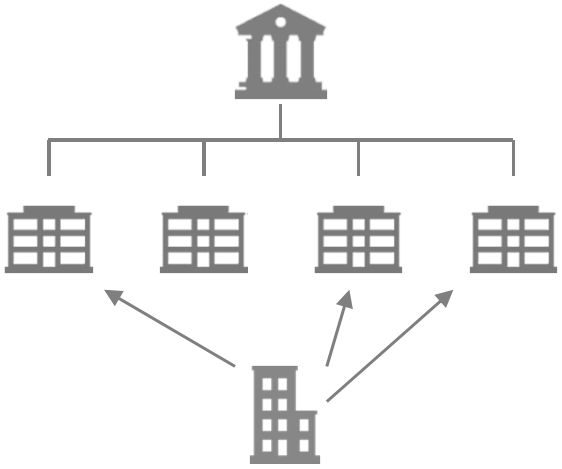


What additional capabilities can digital identity offer to FIs?

5. DETERMINING TOTAL RISK EXPOSURE

CURRENT STATE:
Legal entities are often unable to determine their total risk exposure to a given counterpart due to complicated ownership structures and difficulty aggregating a complete view of a legal entity.

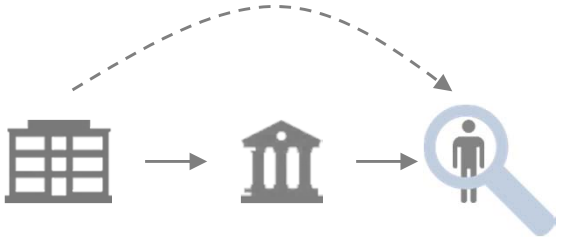
HOW WOULD DIGITAL IDENTITY HELP?
Transaction counterparties could have a consolidated view of the corporate structure of the entities with which they are transacting, allowing them to determine their total risk exposure to that entity across transactions and lines of business.



6. IDENTIFYING TRANSACTION COUNTERPARTIES

CURRENT STATE:
It is currently challenging or impossible for entities to identify all entities that are participating in a given transaction; they may not have visibility into the end customer in a transaction that is being completed by a broker or other counterparty.

HOW WOULD DIGITAL IDENTITY HELP?
Legal entities could request visibility into the consolidated identity of a third party and the ownership history of a given asset involved in a transaction. This would allow them to identify both the direct customer and the end customer in the transaction, better informing the decision of whether to complete the transaction.

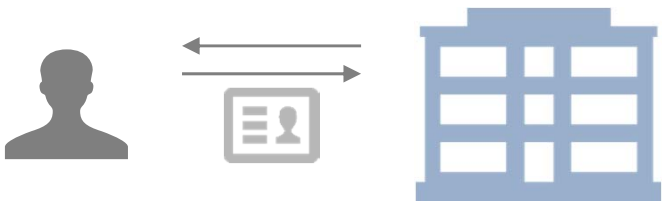


What additional capabilities can digital identity offer to FIs?

7. LINKING INDIVIDUAL IDENTITY TO CORPORATE IDENTITY

CURRENT STATE:
Individual and corporate identity information is currently not linked; it is challenging to identify individuals who are associated with corporate entities.

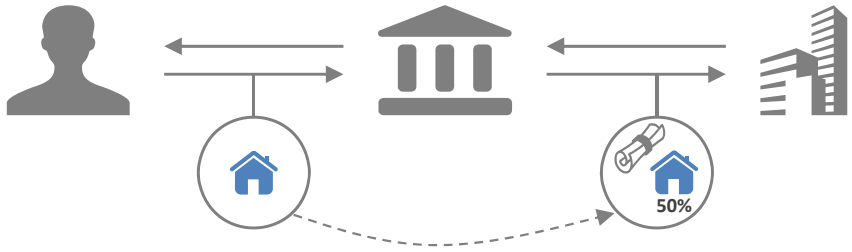
HOW WOULD DIGITAL IDENTITY HELP?
The digital and standardized collection, storage and transfer of attributes for both individuals and legal entities would ensure identity information is accurate and up-to-date. Linkages between these systems would create reliable pictures of the identities of individuals affiliated with legal entities for know-your-customer and other purposes.



8. TRACKING TOTAL ASSET REHYPOTHECATION

CURRENT STATE:
The transaction and ownership history of assets can become ambiguous as assets are rehypothecated; this exacerbates counterparty risk and asset valuation uncertainty, while the lack of a historical tracking mechanism prevents the enforcement of limits on the extent of asset rehypothecation.

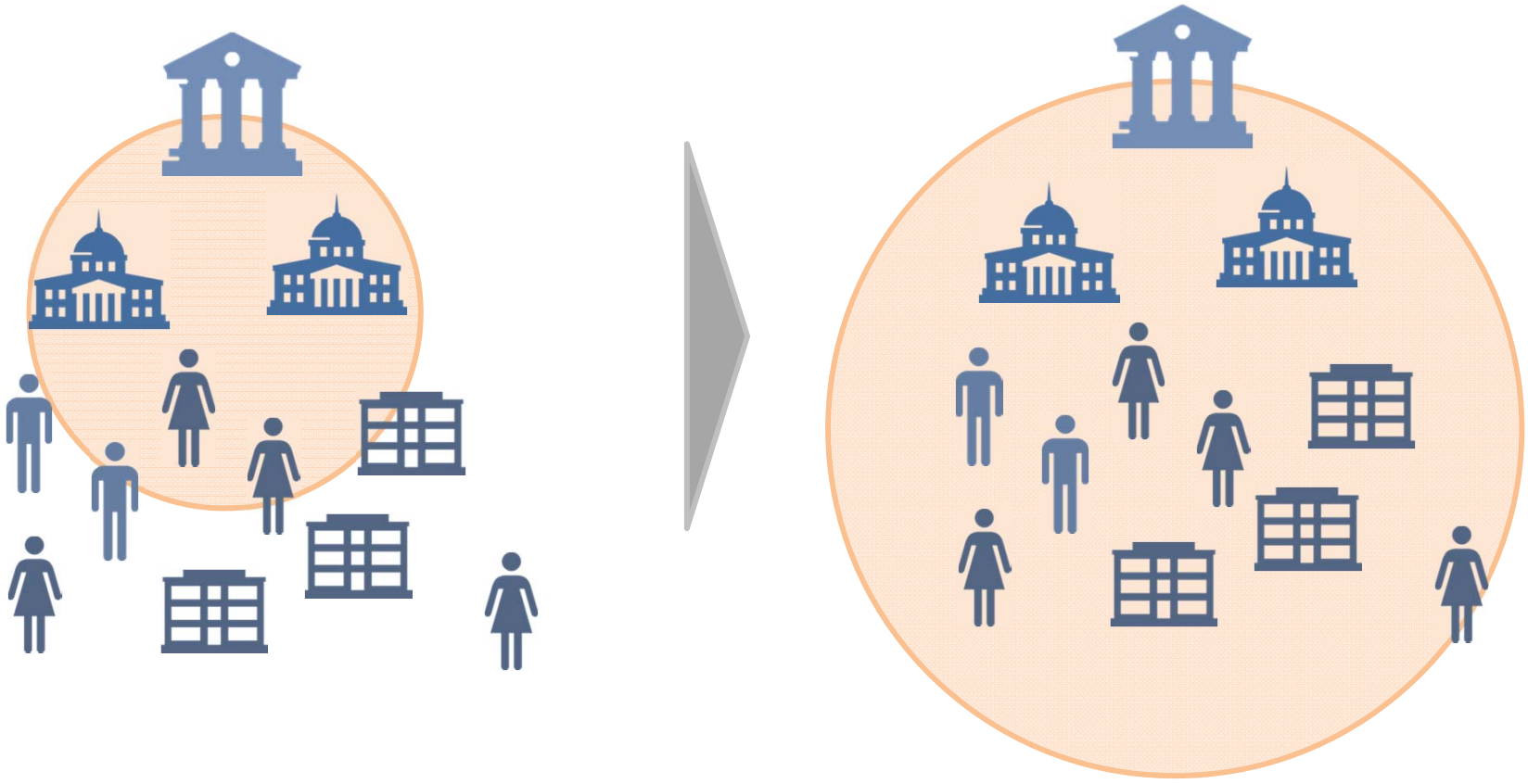
HOW WOULD DIGITAL IDENTITY HELP?
Consolidated, standardized and digital identity information for assets would be available to all entities engaging in a transaction involving that asset, giving transaction counterparties the ability to check asset information, such as issuer and transaction history; this would enable the tracking of the asset ownership structure and composition, and prevent over-rehypothecation due to the lack of visibility into past transactions involving that asset.



Implementation of Identity Systems

Implementation of a digital identity system should follow a bottom-up approach

We have outlined our perspective on the prime movers within digital identity solutions and how they should implement digital identity solutions. It is critical to observe that this is the first step in a bottom-up approach that would result in systems being scaled outwards to incorporate greater numbers of users, relying parties and identity providers as guidelines and functionality are tested and refined.



The system is launched with a critical mass of parties to test and refine

The system is scaled to increasing numbers of users, relying parties and identity providers

Global identity will never exist as a monolith

This document has laid out a principles-based approach to building effective, sustainable and bounded natural identity networks as the foundation for interconnecting individual identity networks. There will never be a single, global solution for identity.

Identity serves different needs

Different user groups have different needs and requirements for identity. Identity systems for individuals are designed to increase the ability of users to perform transactions in a safe and secure manner. Identity systems for legal entities are intended to enable comprehensive aggregation at a macro level – whether to determine total exposure to a single legal entity or manage systematic risk and stability. Identity systems for assets are designed to allow tracking and provide transparency around ownership and value. Privacy is one of the key requirements of individual identity, but is much less important in legal entity and asset identity and may even interfere with the larger purposes of these systems. Individuals have self-determination, whereas legal entities and assets have custodians who act on their behalf.

Identity is cultural

Identity is hugely affected by cultural and geopolitical factors. For example, while some populations are comfortable having a national ID card, this system has failed in other jurisdictions. Certain authorities may not be a stable government to drive the creation and adoption of digital identity.

This means that, aside from having different configurations for purely practical reasons, identity systems will differ dramatically to suit the cultural and geopolitical needs that they serve.

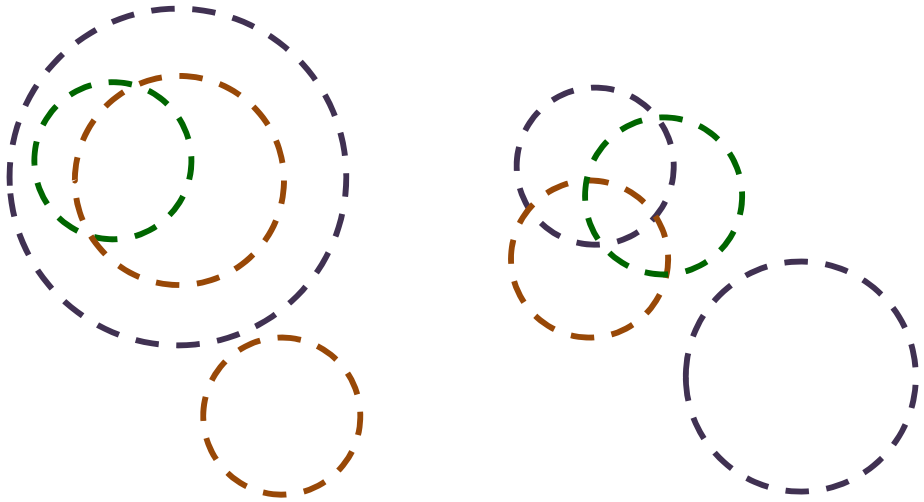
There is no one-size-fits-all for identity.

A global system for identity therefore initially requires the construction of discrete identity networks, and then the creation of rails between them

Creating a global solution for identity is a two-step process: the key to building a global system for digital identity is first building successful natural identity networks that address the unique needs and preferences of their user group and situation, and then building connective tissue that creates interoperability between these systems.

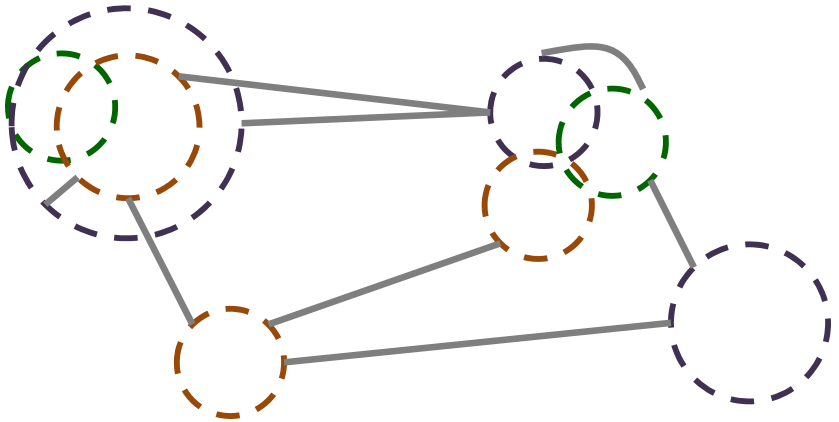
1
Implementation: Configuring natural identity networks

The configuration of natural identity networks will be guided by the decisions made against the primary and secondary dimensions of choice



2
Interconnection: Building the rails for global identity

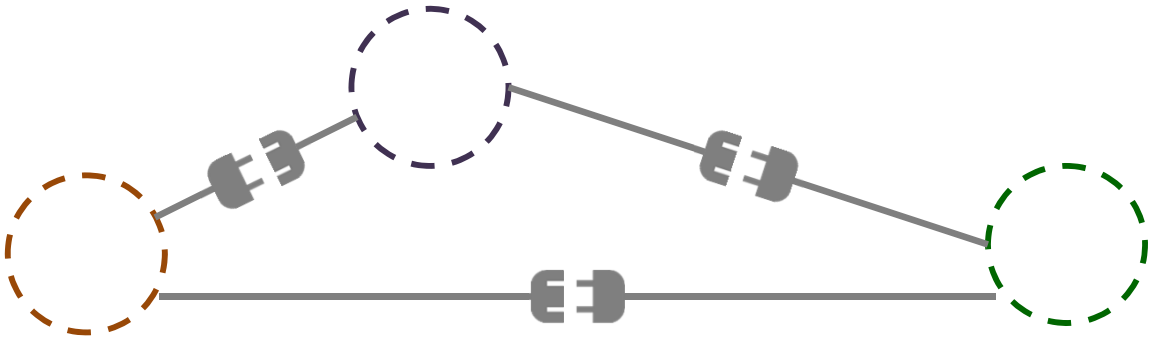
Building the rails between natural identity systems will create global interconnection and interoperability



While the rails for global identity will begin to emerge as systems develop, it is important that entities follow a guiding framework

Building identity as a two-step process enables identity systems to be built by narrowing the required stakeholders to groups that have similar needs and concerns, and therefore have relatively aligned incentives. It also ensures that these systems are tailored to the specific needs and wants of their user and stakeholder groups and will therefore gain the uptake that a top-down, one-size-fits-all system would not attain. However, these solutions should also be built following a common framework that will ensure interoperability by defining the features, attributes and requirements of the identities that are exchanged in the system. This reinforces the need for individual identity systems to be built by entities such as financial institutions that have experience working together to define standards, and then building individual systems within these standards.

Implementing discrete digital identity systems that suit the unique needs and cultural factors of users in their own jurisdictions, and designing these systems around resilience, interoperability and interconnection, will allow a global blueprint for digital identity to emerge.



There are many standing questions and uncertainties that must be considered in the creation of new identity systems

WORLD ECONOMIC FORUM
COMMITTED TO IMPROVING THE STATE OF THE WORLD

SOME THOUGHT STARTERS TO BUILDING IDENTITY SOLUTIONS

Drivers of identity systems will need to consider many detailed tactical questions in the configuration and implementation of their own identity solutions. We have provided some example questions and uncertainties below.

- Which entities need to be involved in an identity system for your area and user group – governments, regulators, financial institutions, consumer groups, others?
- What business model that will be sustainable in that situation – user pays, relying party pays, government pays? By transaction, subscription, subsidized through other services?
- What governance structure is necessary for the system – who should be involved, what should be the extent of their mandate, how will governance be renewed and refreshed?
- What is the minimum viable identity product required for that situation – what users should be involved, what services need to be covered, which entities should be involved, what metrics are being tested?
- Which frameworks and standards can be adopted for the identity system?
- Which components of the identity stack must be proprietary, and which ones can be outsourced or obtained through partnership?
- What technology platform is required for the system?
- What is the best method of communicating system functionality and benefits to users?

Contact Details

For additional information, please contact:

WORLD ECONOMIC FORUM CORE PROJECT TEAM

R. Jesse McWaters
Project Lead, Financial Services
World Economic Forum
Jesse.McWaters@weforum.org

Giancarlo Bruno
Senior Director, Head of Financial Services
World Economic Forum
Giancarlo.Bruno@weforum.org

PROFESSIONAL SERVICES SUPPORT FROM DELOITTE

Christine Robson
Deloitte Canada
crobson@deloitte.ca

Rob Galaski
Deloitte Canada
rgalaski@deloitte.ca

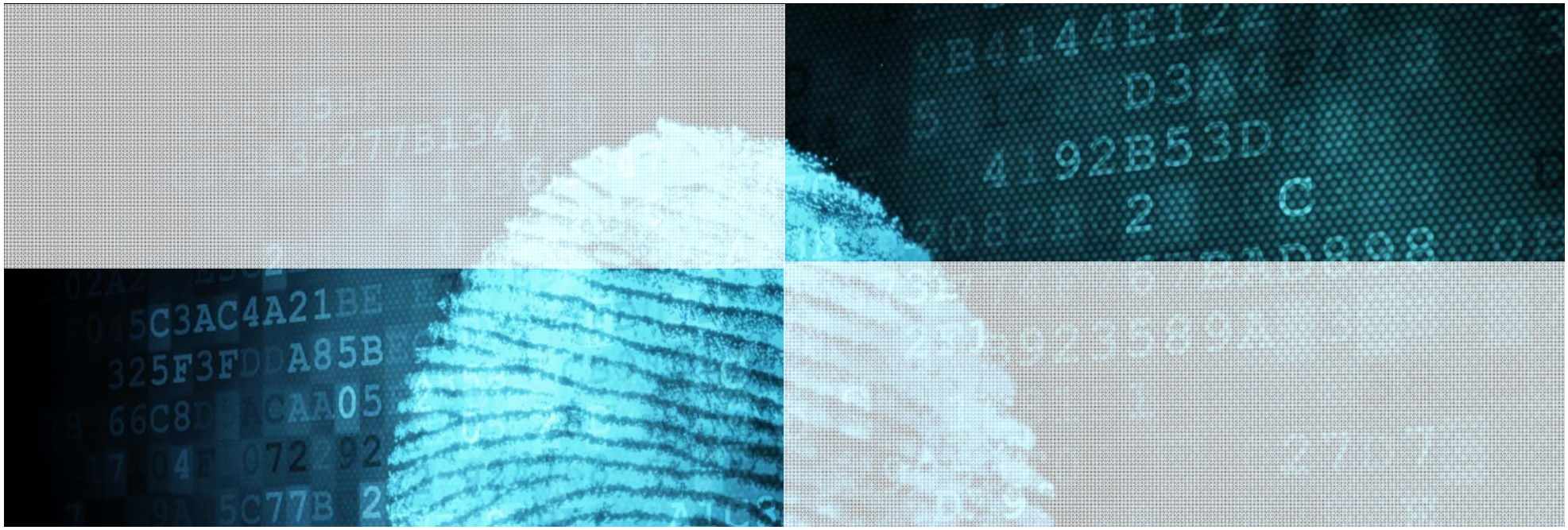
COMMITTED TO
IMPROVING THE STATE
OF THE WORLD

WORLD ECONOMIC FORUM

COMMITTED TO IMPROVING THE STATE OF THE WORLD

A Blueprint for Digital Identity

The Role of Financial Institutions in Building Digital Identity



An Industry Project of the Financial Services Community | Prepared in collaboration with Deloitte

Part of the Future of Financial Services Series • August 2016

Foreword

Consistent with the World Economic Forum's mission of applying a multi-stakeholder approach to address issues of global impact, the creation of this report involved extensive outreach and dialogue with the financial services community, innovation community, technology community, academia and the public sector. The dialogue included numerous interviews and interactive sessions to discuss the insights and opportunities for collaborative action.

We extend sincere thanks to the industry and subject matter experts who contributed their unique insights to this report. In particular, the members of the Project's Steering Committee and Working Group, who are introduced in the following pages, played an invaluable role as experts and patient mentors.

We are also very grateful for the generous commitment and support to Deloitte Consulting LLP in the U.S., an entity within the Deloitte[1] network, in its capacity as the official professional services advisor to the World Economic Forum for this project.

Contact

For feedback or questions, please contact:

R. Jesse McWaters, Lead Author
jesse.mcwaters@weforum.org
+1 (212) 703-6633

[1] Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee ("DTTL"), its network of member firms, and their related entities. DTTL and each of its member firms are legally separate and independent entities. DTTL (also referred to as "Deloitte Global") does not provide services to clients. Please see www.deloitte.com/about for a detailed description of DTTL and its member firms. Please see www.deloitte.com/us/about for a detailed description of the legal structure of Deloitte LLP and its subsidiaries. Certain services may not be available to attest clients under the rules and regulations of public accounting.

Acknowledgements

Acknowledgements

Members of the Steering Committee

The following senior leaders of global financial institutions have provided guidance, oversight and thought leadership to the “Disruptive Innovation in Financial Services” project as its Steering Committee:

Bob Contri

Vice Chairman,
Deloitte & Touche LLP

David Craig

President, Risk and Financial,
Thomson Reuters

John Flint

Chief Executive Officer, Retail Banking and Wealth Management, *HSBC*

Kim Hammond

Chief Operating Officer,
Deutsche Bank

Jason Harris

Chief Executive Officer, International Property and Casualty, *XL Group*

Michael Harte

Chief Technology Officer and Chief Operations Officer, *Barclays*

Axel Lehmann

Chief Operating Officer,
UBS

Jason Patwardhan

Chief Innovation Officer,
Standard Chartered Bank

David Puth

Chief Executive Officer,
CLS Group

William Sheedy

Global Executive, Corporate Strategy, M&A, Government Relations, *Visa*

Dietter Wemmer

Chief Financial Officer,
Allianz

Acknowledgements

Members of the Working Group

The project team would also like to acknowledge the following executives of global financial institutions who helped define the project framework and shape strategic analyses as its Working Group:

Tom Brown

Partner,
Paul Hastings

Lena Mass-Cresnik, PhD

Head of Innovation, Strategic Product Management, *BlackRock*

Christof Edel

Global Head of Trading Strategy & Business Development, *Thomson Reuters*

Rob Galaski *(Project Advisor)*

Head of Financial Services,
Deloitte

Dorothy Hillenius

Director of Corporate Strategy,
ING

Marc Lien

Director of Innovation and Digital Development, *Lloyds Banking Group*

Matthew Levin

EVP and Head of Global Strategy,
Aon

Victor Matarranz

Director of Strategy & Chief of Staff to the CEO,
Santander

Neil Mumm

VP Corporate Strategy,
Visa

Max Neukirchen

Group Head of Strategy,
JP Morgan Chase

Christine O'Connell

Global Head of Strategy & Business Development, *Thomson Reuters*

Robert Palatnick

Managing Director and Chief Technology Architect, *DTCC*

Kosta Peric

Deputy Director Financial Services for the Poor, *Bill and Melinda Gates Foundation*

Justin Pinkham

SVP and Group Head, Payments Innovation,
MasterCard

Bob Reany

SVP and Group Head, Identity Solutions,
MasterCard

Peter Rutland

Senior Managing Director,
CVC Capital Partners

Nicolas de Skowronski

Chief of Staff,
Bank Julius Baer

Huw Van Steenis

Managing Director and Head of Financial Services Research, *Morgan Stanley*

Colin Teichholtz

Partner & Co-Head of Fixed Income Trading,
Pine River Capital

Fabien Vandenreydt

Head of Markets Management, Innotribe & the SWIFT Institute, *SWIFT*

Acknowledgements

List of subject matter experts (1 / 2)

In addition, the project team expresses its gratitude to the following subject matter experts who contributed their valuable perspectives through interviews and workshops (in alphabetical order):

Mukul Ahuja	Deloitte Canada
Christoph Albers	SWIFT
Alex Batlin	UBS
Eric Benz	Credits
Peter Berg	Visa
Vikram Bhat	Deloitte & Touche LLP
David Birch	Consult Hyperion
Francis Bouchard	Hamilton Place Strategies
Andre Boysen	SecureKey
David Brewer	Digital Catapult
Ben Brophy	ENTIQ
Tom Brown	Paul Hastings
Preston Byrne	Eris Industries
Claire Calmejane	Lloyds Banking Group
Alicia Carmona	Identity 2020
Nicolas Cary	Blockchain
Shawn Chance	Nymi
Emily Clayton	Bank of England
John Clippinger	MIT Media Lab
Jeff Coleman	Ledger Labs
Wayne Crombie	Citigroup
Malcolm Crompton	Information Integrity Solutions
Stephen Cross	Aon
Mark Davies	Avox Ltd.
Howard Davis	RBS
Nicolas de Skowronski	Julius Baer
Rachel Dixon	Digital Transformation Office of Australia
Ivan Djordjevic	Deloitte UK
Justin Dombrowski	Historiocity Tech
Jon Duffy	TradeMe
Carlo Duprel	Deloitte Tax & Consulting, Luxembourg
Andre Durand	Ping Identity
John Edge	Digital Stored Value Association
Anna Ewing	Nasdaq
Daniel Feichtinger	Digital Asset Holdings
Chris Ferguson	UK Cabinet Office
Jerry Fishenden	VoeTek
Marissa Flowerday	TradeMe
Conan French	IIF
Emilio Garcia	Santander
Joe Guastella	Deloitte Consulting LLP
Alka Gupta	Global ID
Aran Hamilton	DIACC
Jonathan Hardinges	Thomson Reuters
Adrienne Harris	National Economic Council, The White House
Jonathan Hayes	Julius Baer
Dorothy Hillenius	ING
Bill Hodash	DTCC
Rainer Hoerbe	The Kantara Initiative
Chuck Hounsell	TD Canada
Arne Vidar Huag	Signicat
Afsar Hussain	GSMA
Marta Ienco	GSMA
Raj Iyer	BNY Mellon
Natasha Jackson	GSMA
Charlotte Jacoby	Agency for Digitization, Ministry of Finance, Denmark
Hyder Jaffrey	UBS
Andrew Johnston	TELUS
Tanis Jorge	Trulioo
Sean Kevelighan	Zurich Insurance Group
Alim Khalique	Bank of America Merrill Lynch
Hwan Kim	Deloitte Canada
Dan Kimerling	Standard Treasury
Philipp Kroemer	Commerzbank AG
Jaap Kuipers	Kantara Initiative
Jo Lambert	Paypal
Ian Lee	Citi
Chris Locke	Caribou Digital
Joseph Lubin	Consensys
Adam Ludwin	Chain
Christian Lundkvist	Consensys

Acknowledgements

List of subject matter experts (2 / 2)

In addition, the project team expresses its gratitude to the following subject matter experts who contributed their valuable perspectives through interviews and workshops (in alphabetical order):

Joanna Marathakis	Deloitte Transactions and Business Analytics LLP
Stephen Marshall	Deloitte UK
Simon Martin	LeapFrog Investments
Todd McDonald	R3CEV
Morgan McKenney	Citigroup
Adel Melek	Deloitte Canada
Pat Meredith	Canadian Payments Taskforce
Paul Morgenthaler	Commerzbank
Renny Narvaez	BNY Mellon
Eddie Neistat	AlixPartners
Nina Nieuwoudt	Mastercard
Pascal Nizri	Chekk
Robert Palatnick	DTCC
Cheryl Parker Rose	CFPB
Justin Pinkham	MasterCard
Rick Porter	Deloitte & Touche LLP
Reinhard Posch	Austrian Federal Government
Dan Quan	CFPB
Rhomaios Ram	Deutsche Bank
Kai Rannenberg	Goethe University
Bob Reany	Mastercard
David Richards	DIACC
Pierre Roberge	Digital and Payment Innovation Consultant
Andre Romanovskiy	Deloitte Canada
Andrew Rudd	AssureUK
Peter Rutland	CVC Capital Partners
Wiebe Ruttenberg	European Central Bank
Joel Sacmar	Daon
Jean-Louis Schiltz	Schiltz & Schiltz
Charles Schwarz	Barclays
Rocky Scopelliti	Telstra
Amy Scott	Identity2020
John Scott	2Keys Security Solutions
Anton Semenov	Commerzbank
Beth Shah	Digital Asset Holdings
Rajesh Shenoy	Citi
Nick Smaling	Deloitte Netherlands
Stan Stalnaker	HubID
Matthew Stauffer	Clarient Entity Hub
Gavin Steele	Lloyd's of London
Ashley Stevenson	ForgeRock
Matt Stroud	Digital Catapult
Paul Szurek	Blockchain
Pavlo Tanasyuk	BlockVerify
Marc Taverner	BitFury
Simon Taylor	Barclays
Adizah Tejani	Level39
Kenneth Tessem	Finansiell ID-Teknik BID AB
Don Thibeau	Open Identity Exchange (OIX)
Michael Turner	PERC
Keith Uber	GlobalSign
Eric Van der Kleij	Level39
Huw van Steenis	Morgan Stanley
Aneesh Varma	Aire.io
Ivan Vatchkov	Algebris Investments
Roy Vella	Vella Ventures Ltd.
Helene Vigue	GSMA
Franziska von Arnim	Deutsche Bank
Patrick Walker	PERC
Colin Wallis	Kantara Initiative
Peter Watkins	Government of British Columbia
Derek White	Barclays
Conor White	Daon
Greg Williamson	MasterCard
Gregory Williamson	MasterCard
Stephan Wolf	GLEIF
Kevin Young	Deloitte Canada
Fei Zhang	Allianz
Tom Zschach	CLS Bank

Acknowledgements

Project Team and Additional Thanks

Project Team

The “Disruptive Innovation in Financial Services” project team includes the following individuals:

WORLD ECONOMIC FORUM PROJECT TEAM

Jesse McWaters
Project Lead, Disruptive Innovation in Financial Services

Giancarlo Bruno
Senior Director, Head of Financial Services Industries

Michael Drexler
Senior Director, Head of Investors Industries

PROFESSIONAL SERVICES SUPPORT FROM DELOITTE

Rob Galaski
Project Advisor, Deloitte

Christine Robson
Lead Author, Deloitte

Additional Thanks

The project team expresses its gratitude to the following individuals for their contribution and support throughout the project (in alphabetical order):

Faiza Harji

Alex Rinaldi

Sabrina Sdao

And to:

The Deloitte Greenhouse (Event Facilitation & Location Services)

Level 39 (Location Services)

The Value Web (Event Facilitation)

Executive Summary

The Blueprint for Digital Identity project is the most recent phase of the Forum's ongoing Disruptive Innovation in Financial Services work

WORLD ECONOMIC FORUM
COMMITTED TO IMPROVING THE STATE OF THE WORLD

2015

THE FUTURE OF FINANCIAL SERVICES

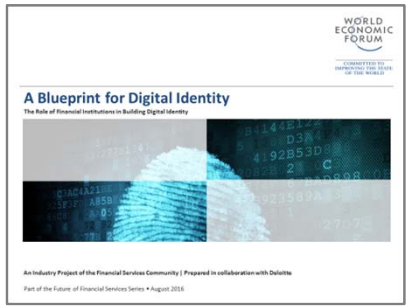
The Future of Financial Services project explored the landscape of disruptive innovations in financial services, provided the first consolidated taxonomy for these disruptions, and explored their potential impacts on the structure of the industry

2016

BEYOND THE FUTURE OF FINANCIAL SERVICES

This phase of the disruptive innovation work explores two topics with key potential as foundational enablers of future disruption

A Blueprint for Digital Identity: The role of Financial Institutions in building Digital Identity



This project explores the potential for digital identity in financial services and beyond and lays out a blueprint for the implementation of effective digital identity systems

The future of financial infrastructure: An ambitious look at how blockchain can reshape financial services

This project explores the potential for distributed ledger technology to transform the infrastructure of the financial services industry

The mandate of this project was to explore digital identity and understand the role that Financial Institutions should play in building a global standard for digital identity

WORLD ECONOMIC FORUM
COMMITTED TO IMPROVING THE STATE OF THE WORLD

PROJECT CONTEXT

Identity is a critical topic in Financial Services today. Current identity systems are limiting Fintech innovation and well as secure and efficient service delivery in Financial Services and society more broadly. Digital identity is widely recognized as the next step in identity systems. However, while many efforts are underway to solve parts of the identity challenge and create true digital identity, there is a need for a concerted and coordinated effort to build a truly transformational digital identity system.

This document is intended as a guide for Chief Strategy Officers of Financial Institutions as well as policy makers who are interested in the topic of identity and want to understand the digital identity and their own potential role in the creation of robust digital identity systems.

PROJECT SCOPE

The mandate of this project was to explore identity and its importance in Fintech, Financial Services and in developed societies broadly, the topic of digital identity, and provide a landscape scan of current efforts to build digital identity solutions.

This report will discuss different structures for identity systems and discuss which configurations are best suited to solve different problems, and provide a perspective on the role of Financial Institutions in building digital identity systems.

This report will not focus on the creation of standards around identity; much valuable work has already been done in this space and current developments such as the publication of the European Union eIDAS Regulation are moving the conversation on this front. Nor will it discuss technology solutions. Rather, it will attempt to provide clarity and direction around the structure of identity and provide a call to action for Financial Institutions to move against the identity challenge.

Over 12 months of research we engaged with subject matter experts through interviews and multi-stakeholder workshops

WORLD ECONOMIC FORUM
COMMITTED TO IMPROVING THE STATE OF THE WORLD

Industry Leaders

Guidance and thought leadership from **12 C-suite executives and 24 strategy officers** of global financial institutions

Subject Matter Experts

In-person and phone interviews with **100+ subject matter and industry experts**

Global Workshops

Four multi-stakeholder workshops at global financial hubs with 200+ total participants including industry leaders, innovators, subject matter experts, and regulators

Singapore	New York, USA	London, UK	Davos, Switzerland
Oct. 2015	Nov. 2015	Dec. 2016	Jan. 2016

This report synthesizes our findings and presents a Point of View on the role that we see for Financial Institutions in digital identity

PROJECT OUTCOMES

Our Perspective: The Role of Financial Institutions in Digital Identity

How should Financial Institutions engage with digital identity? What role can they play in the development of digital identity solutions?

1	**Introduction** What is the global identity challenge, and what problems does it pose for Financial Institutions?
2	**Digital Identity Primer** What is the purpose of identity systems, and why is digital identity the solution to the global identity challenge?
3	**The Landscape of Digital Identity** What do efforts to build digital identity systems look like globally?
4	**The Right Solution to the Right Problem** How should digital identity systems be constructed to serve different needs?
5	**Benefits of Digital Identity** Who stands to benefit from the introduction of digital identity systems?
6	**Implementation** How do you reach a global digital identity solution?

The Role of Financial Institutions in Digital Identity

Current identity systems place major limitations on Fintech innovation

Lack of digital identity limits the development and delivery of efficient, secure, digital-based Fintech offerings

Identity is currently a critical pain point for Fintech innovators. Many of these innovators are trying to deliver pure digital offerings, but the process of identifying users consistently forces them to use physical channels. These Fintech innovators now see the development of a new generation of digital identity systems as being crucial to continuing innovation and delivering efficient, secure, digital-based Fintech offerings.

Examples

Payments

Payments require validation of ACH information, meaning that digital payments innovators must either require users to provide identity information through pseudo-digital channels (such as by photographing their driver's license) or act as platforms on top of established Financial Institutions and rely on their KYC processes

Loans

Evaluating customer risk and issuing loans requires validation of basic customer information, requiring innovators to gather information from users, again through pseudo-digital channels such as photographing existing ID or gathering trusted information from an existing source, and therefore decentralizing a central piece of the product offering

Digital identity is a critical enabler of activity inside Financial Services broadly

Digital identity would allow FIs to perform critical activities with increased accuracy over that afforded by physical identity, and to streamline and partially or fully automate many processes

Identity is also central to the broader financial services industry, enabling delivery of basic financial products ands services. Reliance on physical identity protocols introduces inefficiency and error to these processes. Digital identity has great potential to improve core financial services processes and open up new opportunities.

Examples

Operational decisions

Traditional FS offerings such as insurance and credit and well as customer experience such as contact centers and collections rely on accurate and detailed knowledge of the customer

Regulatory compliance

FIs are required to comply with strict regulation on identifying their customers and are liable for mistakes and inaccuracies

Customer experience and product delivery

Improved knowledge of customer preferences and habits can help FIs deliver radically better customer experience (e.g., tailor authentication requirements based on behaviour)

The relevance of digital identity stretches beyond Financial Services to society as a whole

Identity enables many societal transactions, making strong identity systems critical to the function of society as a whole

Physical identity systems currently put users at risk due to overexposure of information and the high risk of information loss or theft; they also put society at risk due to the potential for identity theft, allowing illicit actors to access public and private services. Digital identity would streamline and re-risk completion of these public and private transactions.

PUBLIC TRANSACTIONS

Entities are required to prove their identities or certain attributes to demonstrate their eligibility for public services

Examples

- *Access to social assistance (e.g., old age security, unemployment insurance)*
- *Access to education*
- *Access to healthcare*
- *Access to civic structures (e.g., voting)*

PRIVATE TRANSACTIONS

Entities are often required to prove their identities or certain attributes to participate in private transactions

Examples

- *Many basic merchant transactions (e.g., buying alcohol)*
- *Large private provider transactions (e.g., renting an apartment, buying a car)*

The need for digital identity is becoming increasingly pressing

Five key trends are increasingly the need for efficient and effective identity systems:

1 

Increasing transaction volumes
The number of identity-dependent transactions is growing through increased use of the digital channel and increasing connectivity between entities

2 

Increasing transaction complexity
Transactions increasingly involve very disparate entities without previously established relationships (e.g., customers and businesses transacting cross-border)

3 

Rising customer expectations
Customers expect seamless, omni-channel service delivery and will migrate to services that offer the best customer experience

4 

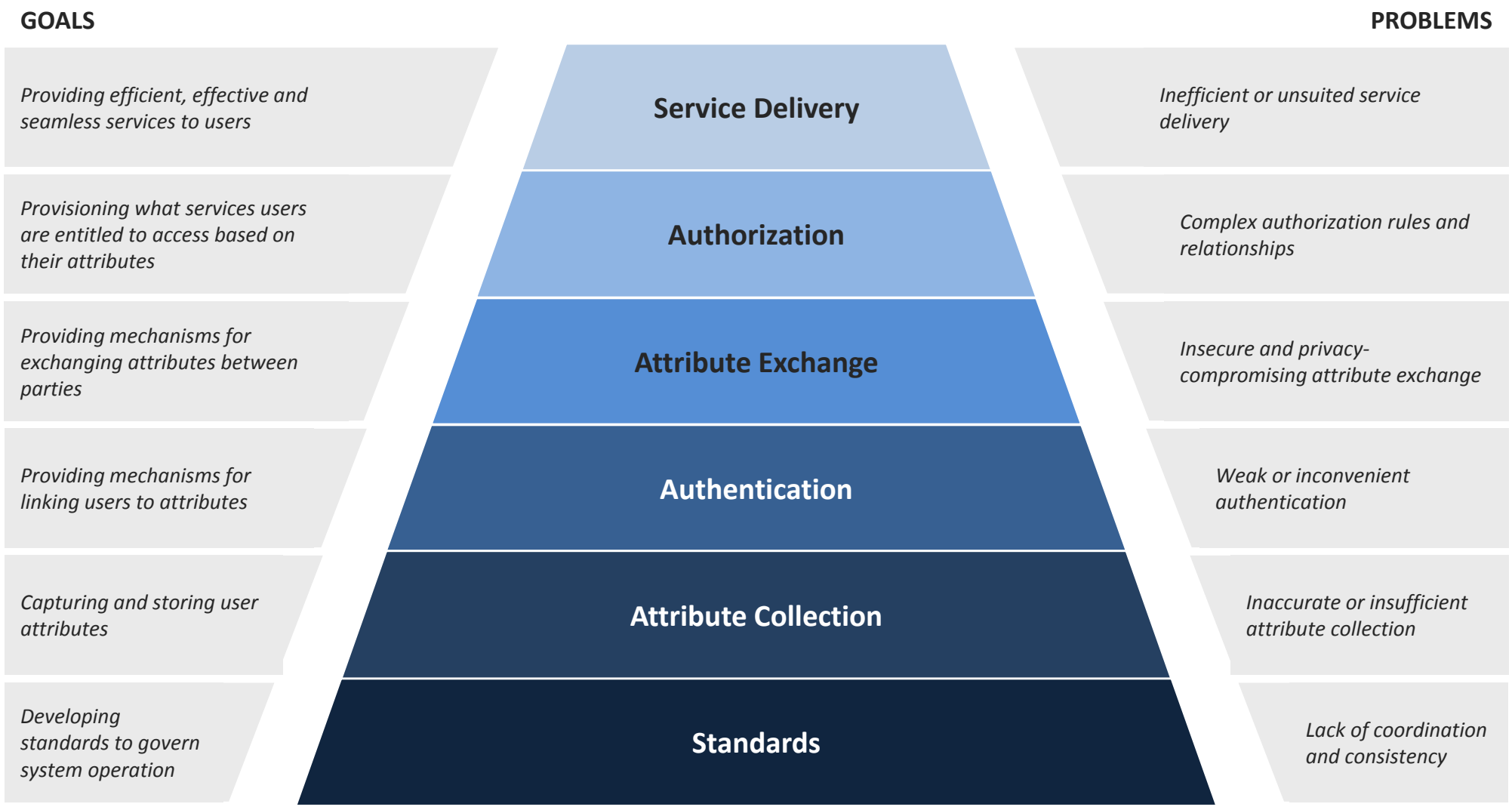
More stringent regulatory requirements
Regulators are demanding increased transparency around transactions, meaning that FIs require greater granularity and accuracy in the identity information that they capture and are increasingly being held liable for inaccurate or missing identity information

5 

Increasing speed of financial / reputational damage
Bad actors in financial systems are increasing sophisticated in the technology and tools that they use to conduct illicit activity, increasing their ability to quickly cause financial and reputational damage by exploiting weak identity systems

However, identity is a multi-layered problem making the creation of digital identity systems complex

Each layer of identity of serves a different purpose, and suffers from a distinct set of problems in today's identity landscape

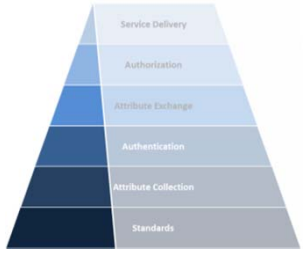


There are currently many distinct gaps in the digital identity landscape

1. Confusing authentication with identity

Many efforts today focus on authentication as a solution to the identity challenge without addressing the strength of the underlying attribute collection and authorization processes

- *Authentication technology solutions, while valuable, rely on preexisting onboarding and attribute collection processes*
- *Authentication solutions provided by global technology platforms are convenient for users but do not provide security or verification of the identity behind an account or username*



2. Enabling transaction completion rather than user activity

Many solutions are driven by the goals and perspectives of a single organization and therefore are designed to serve the needs of particular transactions rather the broader needs of users

- *eGovernment solutions are intended to make government service delivery to users more efficient, and do not enable further transactions in which users might want to participate*
- *Transaction-focussed solutions result in the repeated collection of 'tombstone' data rather than effective collection of user-centric and risk-relevant data such as transaction habits*

3. Building consensus rather than driving action

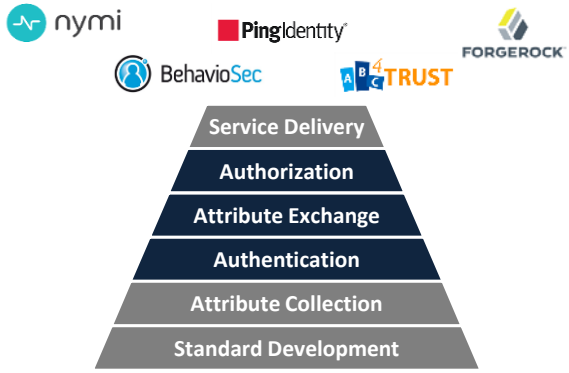
Many efforts focus on building agreement around standards and processes rather than creating a full identity solution and therefore do not result in private sector-implementable solutions

- *Utilities and standards organizations are focussed on creating consensus and a standardized view of data, rather than providing a full identity solution*
- *Multi-governmental efforts have considerable scale but are mainly focussed at the regulatory level, and do not offer a commercially viable solutions*

These gaps are a result of the crowded digital identity landscape, with many different entities building solutions

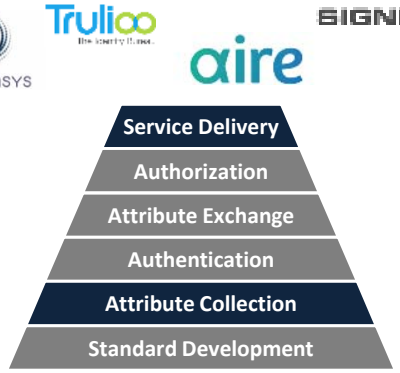
Technology solution providers

Technology solution providers focus on point solutions for authentication, attribute exchange or identity management for enterprises



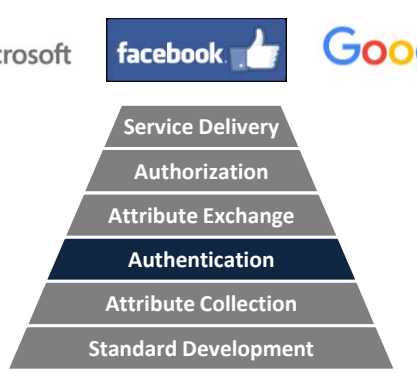
Private Service Providers

Private service providers focus on collecting the attributes they themselves need to provide specific services to users



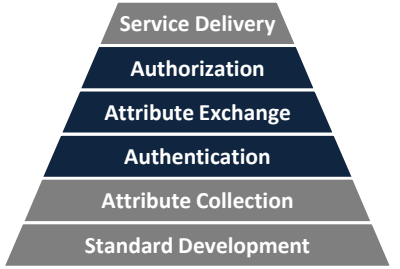
Global technology companies

Global technology companies act as platforms to authenticate users to a wide variety of other service providers



Industry Bodies

Industry bodies focus on standardizing and centralizing the collection of attributes within that specific industry



Governments

Governments focus on the provision of identity to their citizens, and providing citizens with services based on these attributes

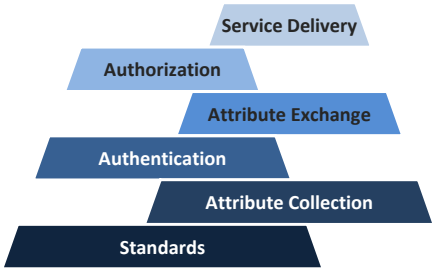
Standards Organizations

Standards organizations focus on frameworks and guidance for developing identity systems

There is an opening for new digital identity systems that can deliver scope and scale

While many ongoing efforts, such as new authentication solutions, are critical to building digital identity, there is a core need for a strong system will enable effective action against each layer of the stack

The entire stack does not need to be provided by a single entity – some components may be modular – but the entire stack must be effective and integrated to provide digital identity systems that have certain critical features



Critical characteristics of a strong identity system

1. **Operationally effective**
   The system allows digital transactions to be completed conveniently and effectively

2. **Scope & scale**
   The system enables large volumes of transactions through provision of transaction-critical attributes and connecting large numbers of users with important and frequently used service providers

3. **Security**
   The system prevents user information from being overexposed, lost or stolen

4. **User control & privacy**
   The system allows users to determine where their information is held and when it is shared or exposed

5. **Viability**
   The system delivers value to all stakeholders, creating broad support and uptake and making it a commercially viable system

Financial Institutions are well positioned to drive the creation of digital identity systems

Financial institutions are exceptionally well positioned to drive identity systems that fill the gaps left by current efforts

	STRUCTURAL
1	FIs already act as **stores of customer attributes** for their own commercial purposes, and therefore are positioned to act as identity providers without extensive incremental effort
2	FIs are one of very few types of institutions that can **verify user information**; they already perform this function for commercial and regulatory purposes
3	FIs are **incentivized to collect accurate user information** for their own commercial purposes
4	FIs have **proven executional ability** to develop new systems and standards (e.g., Interac) that have been widely adopted and effectively used within the private sector
5	The FS industry has near-complete **coverage of users** (people, legal entities, and assets) in developed economies
6	Global FIs have interconnected **operations across multiple jurisdictions**, giving them a structural advantage in enabling cross-jurisdictional identity transactions and systems

	POSITIONING
1	FI operations and use of customer data are **rigorously regulated**
2	FIs act as **established intermediaries** in many transactions and are therefore well positioned to act as identity intermediaries
3	FIs are typically **trusted by consumers** beyond other institutions to be safe repositories of information and assets

There is a strong business case for Financial Institutions to lead the development of digital identity systems

FIs could derive substantial benefit from investing in the development of digital identity solutions. We have categorized these benefits into three categories: efficiency / cost avoidance, new revenue opportunities & brand enhancement, and transformational future state opportunities

Efficiency / Cost Avoidance

Opportunities to streamline current processes, increase automation, and reduce error and human intervention

New Revenue Opportunities

Opportunities to create new revenue streams from new products and services, and to increase the positive recognition of the brand

Transformational Future State Opportunities

Opportunities to stretch outside of core business and capabilities to create transformational new business models and reach new customers

Financial Institutions could benefit from basic efficiency improvements and cost avoidance…

Efficiency / Cost Avoidance

Process streamlining & automation
Streamline and improve onboarding and compliance processes through access to a reliable and consolidated digital view of user attributes, minimizing RFIs and information remediation due to inaccuracy and human error

Improved service delivery
Provide increasingly tailored products and services to customers by leveraging non-traditional attributes
Improve process efficiency and increase STP by automating processes through use of standardized, reliable digital data

Improved customer experience
Improve customer experience by leveraging a variety of user attributes to better understanding the customer's needs and preferences

Improved risk assessment & scoring
Improve risk assessment and reduce fraud by creating more holistic and accurate customer risk profiles to inform suspicious transaction monitoring, insurance payouts, and provision of credit- and risk-based products

Develop new revenue streams…

New Revenue Opportunities

New financial products & services
Offer new products and services based on increased knowledge of customers (e.g., extended financial advisory, new insurance products such as insurance on fractionally owned assets and behaviour-based insurance)

Identity-as-a-service
Offer identity as a service to relying parties who cannot or do not wish to store customer information

Identity-only customers
Offer identity as a separate, fee-based service for individuals who do not otherwise transact with that FI

… and stretch beyond current business and markets to fundamentally transform their businesses

Transformational Future State Opportunities

Allocation of liability
Shift the liability for incorrect information, and the outcomes of holding this information, from Financial Institutions to other entities in the network (e.g., users through approval and consent requirements)

Trust brokerage
Act as a 'broker of trust' in previously trustless interactions between disparate parties in multiple industries, expanding the reach of FIs beyond the FS industry and reaching new profit pools

Disruption of the credit bureau model
Evaluate customer creditworthiness based on accurate identity data including preferences and financial history rather than relying on third parties and the mining of multiple different data sources

Refocussing around the customer
Refocus business around customer service, assisting with day-to-day decisioning and blurring the lines between financial and non-financial advisory

Public sector partnerships
Become the trusted identity provider of the public sector, assisting with social services and civic requirements such as tax filing

WORLD ECONOMIC FORUM
COMMITTED TO IMPROVING THE STATE OF THE WORLD

We are calling on FIs to champion the development of digital identity systems

FIs should champion efforts to build digital identity systems, driving the building and implementation of identity platforms through the creation of minimum viable digital identity systems

Requirements of a minimum viable identity system

1	**Identity provision** Identity provider(s) that hold trusted information and have coverage over a critical mass of users within their target area, and can therefore serve a large number of users and transactions
2	**High-transaction volume attributes** Secure storage of verified attributes that are required for common transactions (inherent attributes such as name, date of birth, nationality, national identifier number, and some assigned attributes such as address)
3	**Relying party adoption** Involvement of relying parties that offer important and frequently used user-facing services
4	**Technology platform** A technology platform that enables secure attribute exchange between identity providers and relying parties with a convenient user consent mechanism (e.g., operates on mobile and desktop)
5	**System standards** Supervisory & liability standards that guide operation and use of user information in the system and provide liability and user recourse
6	**Legal & regulatory acceptance** Legal & regulatory acceptance for using third-party verified information, attribute exchange and external use of user information

FIs could take several different approaches to creating identity systems

There are different configuration options for the development of digital identity systems, each with advantages and drawbacks

Single-Institution

Global institutions could create internal systems that stretch across the jurisdictions in which they operate

This would enable quick implementation but a single institution would likely have difficulty in gaining a critical mass of users, limiting its ability to drive system adoption and integration of relying parties

Consortium

Consortiums of financial institutions could form networks that cover large, contained oligopoly economies (such as Canada or Australia)

A consortium requires a high degree of collaboration among parties but is an effective method of getting complete coverage over a user group

Consortiums are well suited to provide identity for individuals as data storage is not centralized, increasing privacy and system resilience

Utility

Financial Institutions could create industry utilities to deliver identity services across the industry

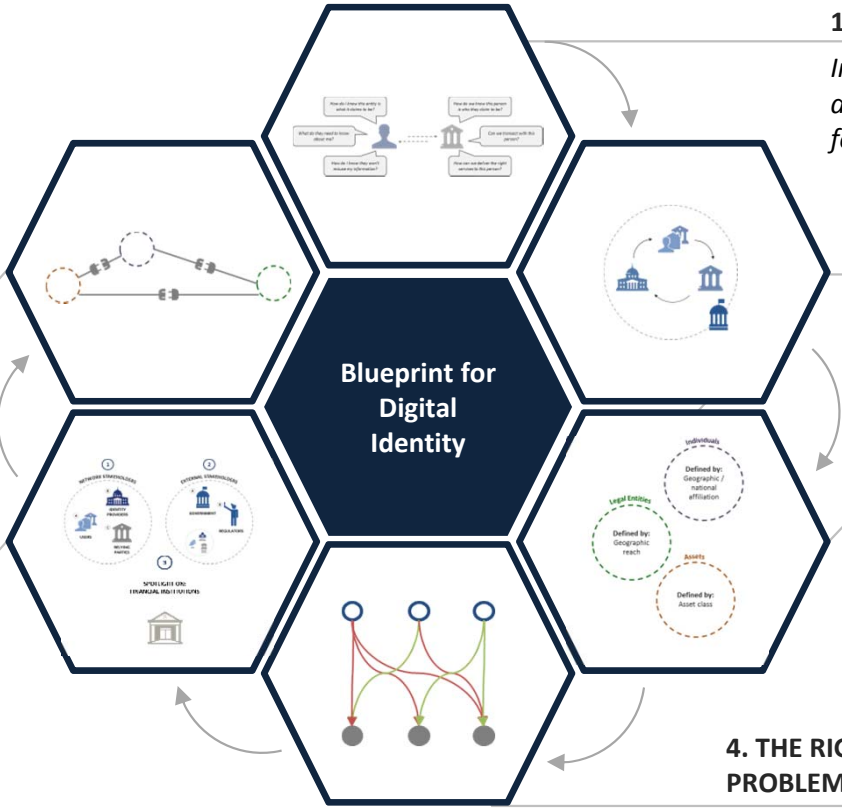
This model is effective in creating standardization and broad coverage, but implementation may be difficult due to the involvement of many different stakeholders

Utilities are a good model for legal entity and asset identity because they provide a standardized view and golden record of information

This report will provide guidance on constructing effective and robust digital identity systems while avoiding implementation pitfalls

Implementation of identity systems is extremely sensitive and therefore easy to get wrong; situational, operational and cultural factors all have important implications for identity systems, and implementation or operational failure has extremely negative consequences for both the drivers of identity system (e.g., wasted resources) and for users (e.g., data breaches).

We have studied the landscape of identity providers to understand what efforts are ongoing and which system models are best suited to different situations and to provide recommendations on system configuration and implementation.



1. INTRODUCTION

Introduces the global identity challenge and how problems with identity manifest for Financial Institutions

2. DIGITAL IDENTITY PRIMER

Summarizes key digital identity concepts

3. THE LANDSCAPE OF DIGITAL IDENTITY SYSTEMS

Describes the landscape of digital identity solutions and introduces a set of archetypes that represent the existing set of solutions

4. THE RIGHT SOLUTION TO THE RIGHT PROBLEM

Discusses how identity solutions should be configured for success

5. BENEFITS OF DIGITAL IDENTITY

Introduces the stakeholders that are involved in a digital identity network, and the types of benefits each stakeholder may derive

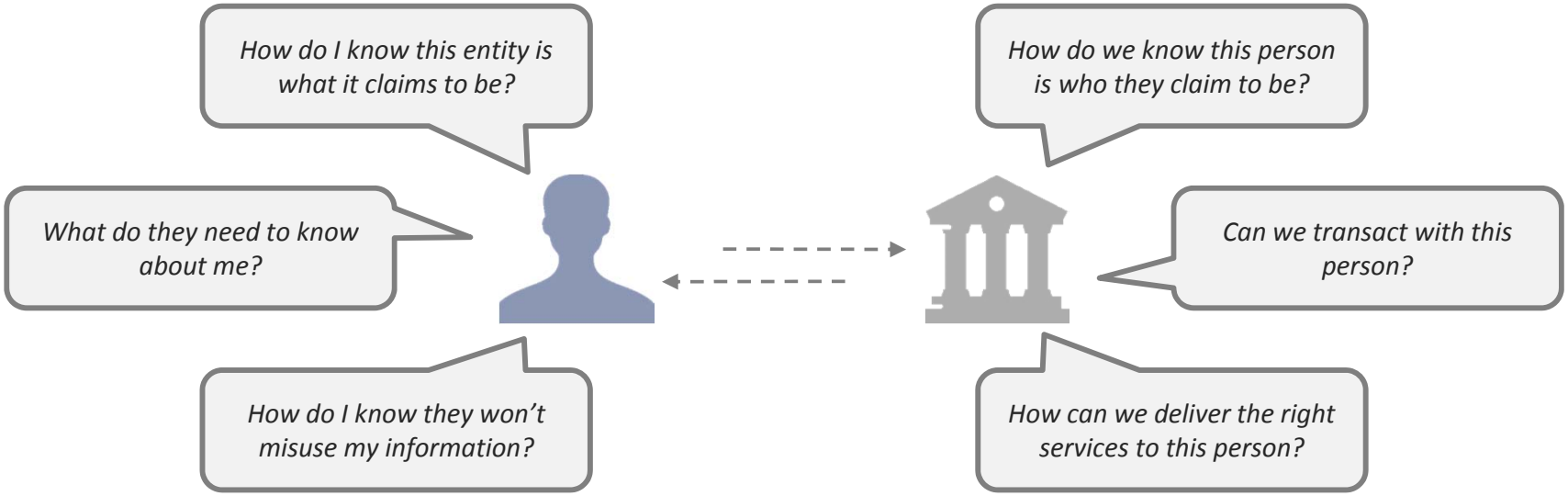
6. IMPLEMENTATION, INTERCONNECTION & CALL TO ACTION

Highlights the next steps and key stakeholders that must be involved to successfully implement a digital identity network

The Global Identity Challenge

Identity is critical to today's society

Identity is foundational to many of the transactions that occur in today's society. In any exchange with requirements about the transacting parties – they must be a certain age or reside in a certain jurisdiction – structures must be in place that allow entities to determine certain information about their counterparty, and to have confidence that the information is true.



THE ROLE OF IDENTITY IN TRANSACTIONS

Many transactions do not require identity. Some, such a crime reporting, may in fact require anonymity. However, many transactions do require identity: to determine if the necessary conditions for the transaction to occur exist, to establish a relationship for repeated transactions, or to tailor delivery of products and services.

Society requires identity systems to enable identity-requiring transactions at scale, putting methods in place that enable the formal asking and answering of identity queries at scale, to allow many day-to-day transactions to occur.

Ineffective identity systems create global challenges for people, for businesses and for society as a whole

Reliance on legacy identity systems that do not effectively enable the transactions that people and entities wish to engage in create challenges for a wide set of stakeholders.

FOR PEOPLE

Service exclusion
Individuals are excluded from key services due to their inability to demonstrate identity

Poor user experience
Services provided to users do not match their needs or are delivered inconveniently

Information overexposure
User information is overexposed, putting users at risk of identity theft and privacy breach

Process inefficiency
Proving identity involves many steps and documents

FOR BUSINESSES

Inefficient service delivery
User-facing processes are cumbersome, resulting in poor customer experience

Obscure risk
Lack of reliable information prevents businesses from accurately calculating the risk of doing business

Fraud
Businesses suffer fraud resulting from stolen or incorrect customer information, or poor authentication

Process inefficiency
Processes provide out-of-date data or require checking multiple sources

FOR SOCIETY

Service exclusion
Entities may be unable to prove attributes and therefore be excluded from key social structures

Service mismatch
Services are delivered incorrectly due to the lack of information

Fraud
Entities can use false information or misrepresent information to gain illicit access to services

Process inefficiency
Processes are highly manual and paper-based, requiring human intervention and remediation

These global identity challenges manifest as specific business problems for FIs

Identity is critical to FIs; their businesses are entirely transaction-based, involving transactions with a high degree of risk and require a high degree of certainty in completion. Global problems with identity therefore manifest as specific business problems for FIs.

ILLUSTRATIVE: BUSINESS PROBLEMS IN FINANCIAL SERVICES

Business problem	Retail / small- to medium-sized enterprise banking	Corporate and investment banking
Inefficient and costly onboarding processes	✓	✓
Inefficient, costly and ineffective know-your-customer (KYC) and due diligence processes	✓	✓
Highly manual and time-consuming compliance processes	✓	✓
Difficulty aggregating information on legal entities and determining total risk exposure	✓	✓
Difficulty attaching individual identity (e.g. corporate directors) to corporate identities	✓	✓
Difficulty identifying all transaction counterparties (e.g. third parties in trading relationships)	✓	✓
Difficulty complying with regulatory standards around data handling and privacy	✓	✓
Multiple views of the customer	✓	✓
Difficulty providing effective/suitable products and services	✓	
Lack of visibility into financial history for new customers	✓	
High fraud rates	✓	
Difficulty tracking asset origination and ownership		✓
Difficulty monitoring and tracking asset rehypothecation		✓

Many of these challenges are driven by the use of physical identity protocols to serve digital transactions

Today's standard identity systems are based on physical documents and processes, which creates many limitations.

CHARACTERISTICS OF PHYSICAL IDENTITY SYSTEMS

Document-based: Identity is based on physical records – the ability to prove identity depends on access and authentication to physical documents (e.g. passports, ID cards and records)

Siloed: Identity information is held in discrete places that are not interconnected and do not enable aggregation, which may be desired by the entity itself or required for some applications

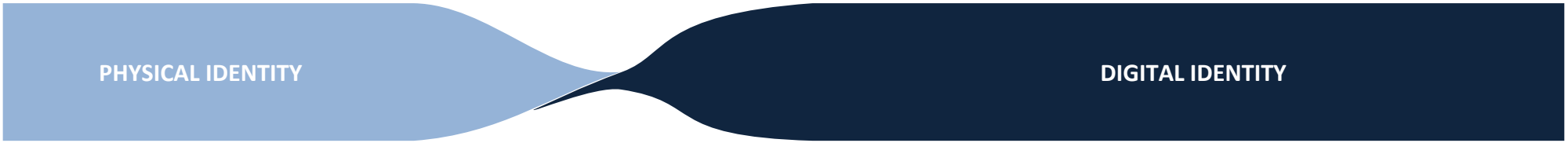
Inflexible: Identity is codified in documents as a limited and standardized set of information about an entity that cannot be easily adapted to transaction requirements

THE PROBLEMS WITH PHYSICAL IDENTITY

- *Proof of identity that is based on possession of physical documents may not require demonstration of a link between an individual and the documents (i.e., authentication), enabling use of an entity's credentials by a different user*
- *Physical identity documents can be falsified, altered or tampered with, as well as lost or stolen*
- *Physical attribute presentation and transfer create the potential for human error in transactions*

THE IDENTITY SHIFT

Identity is now at an inflection point; physical identity systems are breaking down and digital systems are emerging in response.



Physical identity *was designed to enable face-to-face transactions among entities*

The digital economy *is changing the way that identity transactions occur*

Digital identity *enables transactions in the digital world and offers improved functionality for its users*

Digital identity systems support the needs of today's world

Digital identity systems emerged as a direct response to the requirements of transactions in the digital world.

CHARACTERISTICS OF DIGITAL IDENTITY SYSTEMS

Digital-based: Identity exists as a set of digital records that the user can control and use to complete transactions

Interconnected: Proof of identity can be communicated between entities in a standardized, digital format

Flexible: Identity systems adapt to the nature of the transaction, and continuously adapt to requirements by integrating additional information to create a rich view of the user

THE PROMISE OF DIGITAL IDENTITY

- *Digital information can be protected from damage, tampering, loss and theft, with cutting-edge authentication and security protocols*
- *Digital information can be shared in streamlined, tailored and secure ways, predicated on user consent*
- *Institutions can better know and serve their customers, improving existing products and offering new products and services to the underserved*

BENEFITS

Digital identity would deliver a range of benefits to people, businesses and society.

Privacy and control
People would be able to control access to their information

Revenue growth
Financial Institutions would have opportunities to offer Identity-as-a-service

Improved compliance
Regulators would have increased access to trusted, up-to-date information

Improved service delivery
Governments could more easily and effectively deliver public services

New and maturing technologies have important implications for the creation of robust digital identity systems

These technologies may hold considerable promise for identity, and are being explored by many different players.

Data storage

New technologies may offer improved methods of storing user information and increasing user control, privacy and security

- Distributed Ledger Technology combined with encryption and cloud storage allows information to be held and transferred point-to-point in a dispersed, immutable network
- Federated identity standards, such as SAML 2.0, create interoperability between identity management networks and external applications, allowing federated identity systems to scale to large numbers of identity providers and relying parties

Data transfer

Improved attribute exchange protocols allow information to be securely shared between endpoints without risk of interception or decryption, and with more controls that create privacy for users

- Improved encryption protocols, such as Keyless Signature Infrastructure on the blockchain and hashing, provide strong protection for sensitive information and increase the reliability of digital activities
- Data transfer protocols, such as Attributed Based Credentials 4 Trust and zero-knowledge proofs, prevent the creation of metadata by concealing transaction endpoints, increasing user privacy

Authentication

Many new techniques for authenticating users are being explored for their potential to increase information security and user control in certain circumstances by linking users to their digital activities in more robust and persistent ways

- Behavioural and contextual authentication incorporate human and environmental factors to authenticate a user or device
- Biometrics, including fingerprint, retina scanning, heartbeat waveform and facial recognition based on mobile devices have potential to provide greater convenience and security and are being integrated into many anti-fraud controls

Digital identity systems have great potential but also many pitfalls in implementation

Many new identity systems are under development around the world in response to the need for digital identity and new technology capabilities. However, not all have been successful, illustrating some of the pitfalls inherent in the construction of identity systems.

PITFALLS IN IDENTITY SYSTEMS

Stakeholder rejection

- Users may not adopt the system due to poor design or distrust of the system's purpose or structure
- Stakeholders may perceive systems with limited scope and scale as valueless, and therefore not adopt them

Ineffective technology

- A poor technology platform can reduce system functionality, preventing user integration or transaction completion
- Insufficient data protection results in breaches, system compromise and data leakage

Limited support

- Systems that have support from a narrow set of interests may fail due to inconsistent efforts behind their construction and operation
- Systems that lack support from all key stakeholders may not experience sustainable and continuous uptake

Unsustainable operation

- Systems with unsustainable operating or business models will fail

Policy Changes

- Large, complex and emotive programmes such as ID cards can be susceptible to political and / or ideological shifts

Examples of identity system challenges are common…

Hack Brief: Turkey Breach Spills Info on More Than Half Its Citizens
-WIRED, April 2016

Philippine electoral records breached in 'largest ever' government hack
-The Guardian, April 2016

Aadhaar Bill passed in Lok Sabha, Opposition fears 'surveillance'
-Indian Express, March 2016

South Korea at a crossroads with ID card, data theft losses
-CBC News, October 2014

The National [UK] Identity Card scheme will be abolished within 100 days with all cards becoming invalid
-BBC News, May 2010

Identity Primer

Identity is the frontier of privacy and security in the digital world

In an increasingly borderless and digital world, privacy and security cannot be ensured through the construction of walls around sensitive information

Identity is the new frontier of privacy and security, where the very nature of entities is what allows them to complete some transactions but be denied from completing others

To understand the importance of identity and the criticality of strong identity protocols that protect against cyber-risk and suit the needs of transacting parties, it is essential to understand what identity is, and its role in enabling transactions

9-Figure Deals Lift Cybersecurity Investments To An All-Time High
-Forbes, February 2016

Cybersecurity top on government agenda
-Times of India, February 2016

In Today's Era of Data Breaches, Are You Sure Your Data Is Protected?
-Security Intelligence, January 2016

1 in 3 Americans Victim of Healthcare Data Breach in 2015
-Information Management, February 2016

U.S. presses retail banks to help millions of 'unbanked' Americans
-Reuters, February 2016

How to Fight Tax Identity Theft
-Huffington Post, February 2016

FCA fines Barclays £72 Million for poor handling of financial crime risks
-Automated Trader, November 2015

Identity is a collection of pieces of information that describe an entity

Identity is not a monolith; it is a collection of individual attributes that describe an entity and determine the transactions in which that entity can participate. While the total existing set of attributes is endless, they can be broadly categorized into three groups: inherent, inherited and assigned attributes. These attributes differ for members of three main user groups: individuals, legal entities and assets.

	For individuals:	For legal entities:	For assets:
INHERENT ATTRIBUTES Attributes that are intrinsic to an entity and are not defined by relationships to external entities.	• *Age* • *Height* • *Date of birth* • *Fingerprints*	• *Industry* • *Business status*	• *Nature of the asset* • *Asset issuer*
ACCUMULATED ATTRIBUTES Attributes that are gathered or developed over time. These attributes may change multiple times or evolve throughout an entity's lifespan.	• *Health records* • *Preferences and behaviours (e.g. telephone metadata)*	• *Business record* • *Legal record*	• *Ownership history* • *Transaction history*
ASSIGNED ATTRIBUTES Attributes that are attached to the entity, but are not related to its intrinsic nature. These attributes can change and generally are reflective of relationships that the entity holds with other bodies.	• *National identifier number* • *Telephone number* • *Email address*	• *Identifying numbers* • *Legal jurisdiction* • *Directors*	• *Identifying numbers* • *Custodianship*

Specific attributes enable entities to complete certain transactions

Identity is the total set of an entity's attributes. These attributes enable entities to participate in transactions, by proving to their counterparty that they have the specific attributes required for that transaction.

EXAMPLE: Users and transactions

Individuals	Legal entities	Assets
To purchase alcohol, users must prove that they are over the legal drinking age in that jurisdiction	*To onboard with a FI, the entity must have proof that it is a legal and non-sanctioned entity*	*Asset trading, such as trading of equities on a stock exchange, requires proof of ownership and origination*
To vote, users must prove that they are over the legal voting age, have citizenship and reside in that jurisdiction	*To transact in capital markets, the entity must have proof that it is a legal and non-sanctioned entity with an acceptable risk profile*	*Transfer of title of an asset requires proof of ownership from the entity that is transferring the asset*
To open a bank account, users must prove that they are a non-sanctioned person who is legally allowed to engage in financial transactions		

Note: Assets have identity, but are unable to act or transact on their own. Assets require custodians who are entitled to act or transact on the asset's behalf.

Identity transactions have three main aspects

Authorization	*Attributes*	*Authentication*
What must be true about the users to complete the desired transaction?	*Can users prove that they are eligible to complete this transaction?*	*Do the attributes being presented genuinely belong to the entity that is presenting them?*
Authorization is a function of the transaction and the transaction counterparty; they will determine the requirements for transaction eligibility, and make a query about certain user attributes (e.g. age, address).	Users must present their proof of attributes in response to the query. Once users present the required attributes, the counterparty must determine if they are reliable.	The counterparty will determine whether the attributes match the presenting users. If the users are able to authenticate the attributes, the transaction can proceed.

Repeated identity transactions

This model of identity transaction applies to onboarding transactions, that is, transactions where the counterparties do not have an established relationship or where the counterparty is required to gather identity information with every transaction.

Some identity relationships may have a single onboarding transaction; after initially onboarding the users and verifying them through a full identity transaction, the counterparty may use an authentication method (e.g. username and password, chip-and-PIN card) for each subsequent transaction. This allows them to verify that the same entity is transacting each time without going through the full identity transaction process.

*Note: Not all transactions require **exact knowledge** of attributes. Many transactions simply require attribute data to fall inside certain parameters (e.g. instead of knowing an individual's birthdate, a transaction may only require that the user be over a certain age); this is critical in constructing privacy-enhancing identity systems.*

Different identity transactions require different levels of assurance

The level of assurance (LoA) in an identity transaction is the degree of certainty that the transacting parties have in the veracity of the identity being presented.

ASSURANCE IN TRANSACTIONS

A high LoA in identity transactions is not always desirable, as a high LoA requires intensive onboarding and strong authentication processes that may be cumbersome for the user. The LoA required in an identity transaction should therefore generally be dependent on risk – the risk level of the transaction and the consequences of error.

DETERMING ASSURANCE LEVELS

The level of assurance of a given transaction is determined by two main factors:

1. Registration protocols: How stringently the identity provider verifies attributes when onboarding users
2. Authentication method: The strength of the authentication method used to complete transactions between the identity provider and the relying party

Low assurance transactions

Transactions that do not involve a release of information and only involve an information flow from the user to the relying party are low-assurance transactions

Examples include online registrations (e.g. signing up for a news site) and some payments (e.g. paying a parking ticket online)

High assurance transactions

Transactions that involve the release of sensitive and private information, or the transfer of money or assets, are high-assurance transactions

Examples include banking and other financial transactions, such as using an online brokerage account, and many government services

Identity systems tend to evolve inside natural boundaries…

Identity exists within networks that enable transactions between the entities inside that network. These networks tend to evolve around user groups with similar needs and characteristics. These boundaries form what are called “natural identity networks”. Every natural identity network has different needs and therefore will require different system configurations.

NATURAL IDENTITY NETWORKS

The networks that form inside the natural boundaries of identity systems for individuals are based on **geographic location** or **affiliations with a supervisory entity**

Examples include national identity systems, state or provincial identity systems, and employee management systems

The networks that form inside the natural boundaries of identity systems for legal entities are based on **national affiliation, industry** or **geographic reach**

Examples include national or global business registries and industry identifier systems

The networks that form inside the natural boundaries of identity systems for assets are based on their **asset class, origination** or **ownership**

Examples include registries of assets of a single class, or registries of assets that are all owned by a single entity

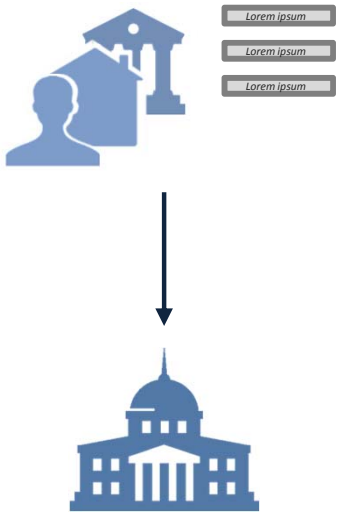
… and operate on a basic shared structure

The purpose of a formal identity system is to allow counterparties without a previously established relationship to engage in trusted transactions.

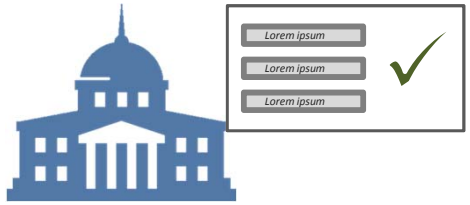
- In a formal identity system, the users' attributes are attested to by trusted third parties; these third parties issue credentials that tie their attestation to the specific attributes, with some method of authenticating the credential to the entity that is presenting it
- Users can use their wallet of credentials to engage in transactions with other entities that require some proof or knowledge of their attributes

THE STRUCTURE OF IDENTITY SYSTEMS

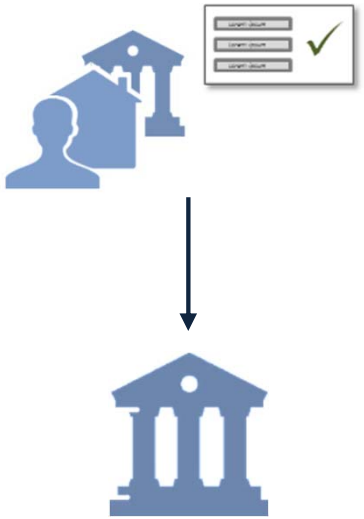
1. *The user presents a set of attributes to a third party*



2. *The third party verifies the attributes and attaches its attestation to the attributes, becoming an identity provider for the user*



3. *The user then uses the credential from the identity provider in transactions with relying parties*



Certain roles and functions must exist in every identity system

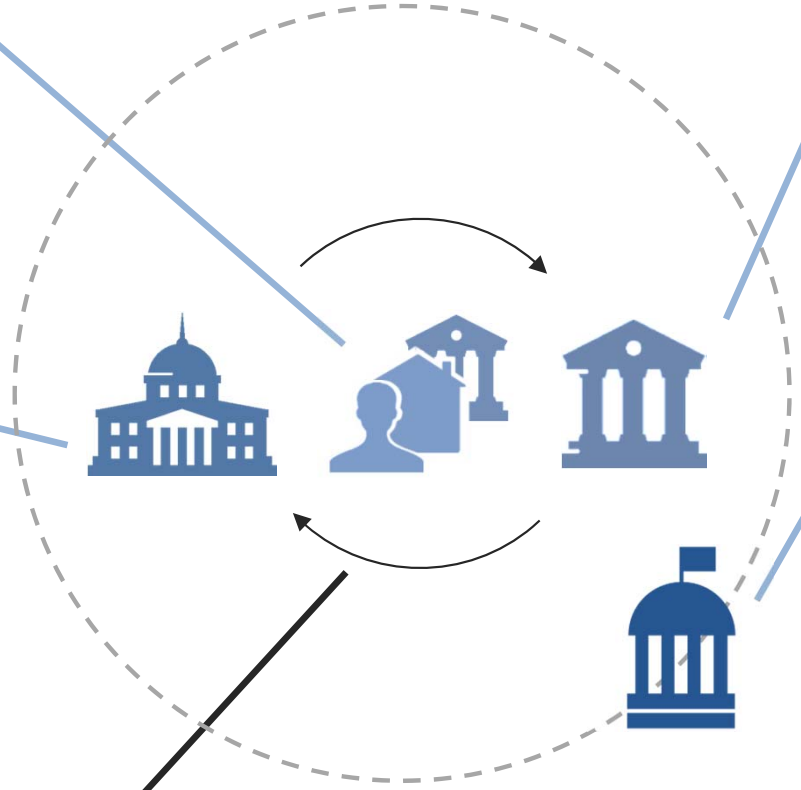
Every identity system must have four roles and one function to operate.

Users

Users are entities for which the system provides identity, for the purpose of allowing them to engage in transactions

Identity providers

Identity providers (IdPs) are entities that hold user attributes, attest to their veracity and complete identity transactions on behalf of users



Relying parties

Relying parties (RPs) are entities that accept attestations from identity providers about user identity to allow users to access their services

Governance body

The governance body provides oversight for the system and owns the operating standards and requirements

Attribute exchange platform

The attribute exchange platform completes transactions by matching identity queries from RPs with attributes from IdPs and exchanging attributes or proof of identity

Role
Function

Methods have evolved, but the concept of identity proofing has not changed over time

The fundamental concept, purpose and structure of identity systems have not changed over time, while methods and technology have made huge strides forward.

Past → **Present**

A letter of introduction is one of the oldest forms of identity documentation.

- **User:** Individuals would use a letter of introduction as an attestation of identity and character to someone they did not know
- **IdP:** The letter writers would provide attestations for various attributes of the users (e.g. that the user was a person of good character)
- **RP:** The recipients of the letter would choose whether or not to accept the attestations based on their knowledge of the IdP and their evaluation of the letter's veracity

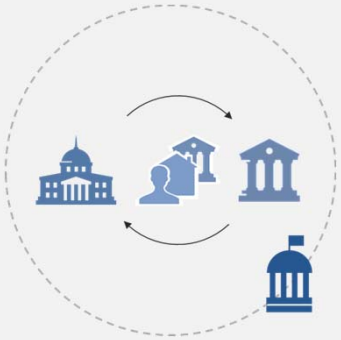
Today a passport issued by an individual's country of residence or origin is one of the most common, trusted identity documents.

- **User:** Individuals are often asked to present their passport to complete transactions that require proof of identity (e.g. entering new countries, opening a bank account, etc.)
- **IdP:** The government of that country acts as an IdP, making certain attestations about the user
- **RP:** The attestations made by the IdP are accepted by a RP based on its trust in the document, its issuer and its evaluation of whether the bearer is the true owner of the passport

Digital identity allows identity transactions to be completed through digital channels

A digital identity system has the same basic structure as a physical identity system, but attribute storage and exchange are entirely digital, removing reliance on physical documents and manual processes.

FEATURES OF DIGITAL IDENTITY SYSTEMS



Digital information storage and transfer

- User identity information is captured and stored in digital form
- User identity information is transferred between IdPs and RPs in digital form
- Form factors, such as computer or mobile devices rather than physical documents, can be used to complete transactions

Direct connectivity

- Information transfer occurs directly between IdPs and RPs, without an intermediary (although user consent can be built in) and without manual intervention (e.g. physical information entry)

THE CURRENT LANDSCAPE OF DIGITAL IDENTITY

Digital identity is not a new concept; many identity systems exist in the world today that either incorporate some digital elements or are entirely digital-based systems. The landscape of digital identity solutions is explored further in the next section of this report. These systems exist along a spectrum of maturity and degree of sophistication; however, all are designed to capture some of the benefits that digital identity brings over traditional physical-based identity systems.

Digital identity offers significant benefits over physical identity systems

Beyond offering new functionality, digital identity has significant functional benefits over physical-based identity systems.

Security

- ✗ Physical identity documents can easily be lost, stolen or replicated by illicit actors, as well as read by entities with no legitimate reason to have the user information
- ✓ Digital identity information could be stored, transferred and exposed using cutting-edge digital security protocols that would prevent against data breach, modification, loss and theft

Privacy and control

- ✗ Physical identity does not allow the release of information to be tailored to the identity transaction; identity documents display a fixed set of information that can be read by almost any entity
- ✓ Digital identity allows individuals to control the sharing of their information, to expose the minimum amount of information required for a given transaction, and shield their information from illicit access

User experience

- ✗ Physical identity requires users to manually show documents or enter identity information in transactions, resulting in a cumbersome user experience and creating potential for human error in transactions
- ✓ Digital information transfer would streamline the transaction process for users and RPs across all channels, increasing the ease of transacting for both parties and removing the potential for human error

Flexibility

- ✗ Physical identity results in the crystallization of user identity in physical documents, and a fixed view of identity that cannot be expanded to cover additional user attributes
- ✓ Digital identity would provide a flexible and scalable system that could incorporate a greater richness of identity information than is currently possible

The Landscape of Digital Identity Systems

WORLD ECONOMIC FORUM

COMMITTED TO IMPROVING THE STATE OF THE WORLD

Many digital identity systems exist in the world today, serving various natural networks

The digital identity systems that exist today fall across broad ranges of purpose, scope and sophistication. Some systems have a digital element bolted onto what is still fundamentally a physical identity system, while others are fully digital and are built to scale and expand as user needs evolve.

Disparate identity systems were studied, including systems for all user groups, to understand the landscape of digital identity solutions, categorize these systems and draw high-level conclusions on which systems best suit different needs.

TYPES OF DIGITAL IDENTITY SYSTEMS

Systems for individuals

The majority of identity systems are designed for individuals, and are often government-driven systems

Purpose:

Designed to increase financial or social inclusion and streamline the delivery of services, or to control access to internal systems for a single organization

Systems for legal entities

Identity systems for legal entities often take the form of centralized registries of information that are owned by a single government or utility

Purpose:

Intended to standardize data across entities, streamline processes and enable data aggregation at a macro level

Systems for assets

Identity systems for assets often take the form of a centralized registry or an internal system for a single organization

Purpose:

Intended to clarify ownership, standardize data or enable the operation of networked systems

The most significant differences in identity systems fall across three primary dimensions

Primary dimensions of choice are the set of choices that must be made in the design of a digital identity system that have the greatest impact on the system's function and structure.

These are not always conscious choices; they are often a natural outcome of the setting in which the system is being implemented, and the problem that the system is intended to solve or the needs that it is intended to serve. The three primary dimensions of choice are:

Nature of identity provision

Is there a single source of identity information? Are there a limited set of parties who provide attributes? Is identity provision distributed across many different entities?

Centralized: One entity stores and provides the identity information

Federated: A limited number of entities store and provide identity information

Distributed: Many different entities store and provide identity information

Number of relying parties

Is there a single RP that can access user attributes, or are there many RPs that can access user information?

One: The system has a single RP that is able to access identity information

Many: The system incorporates many RPs that are able to access identity information

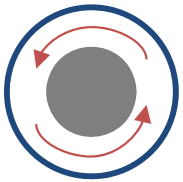
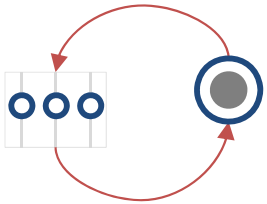
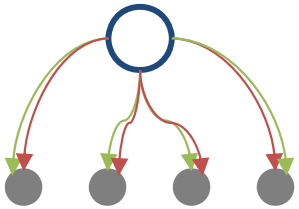
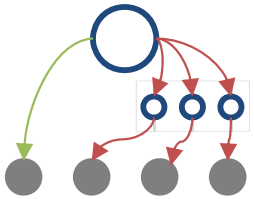
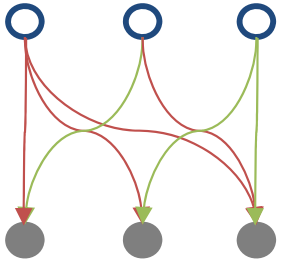
Nature of information transfer

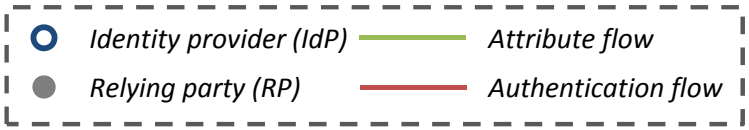
Is information transferred from the IdP to the RP for the purpose of authenticating a user, or is there a transfer of user attributes that the RP requires to execute a given transaction?

Authentication: The IdP authenticates the user for the RP, allowing the RP to complete transactions using information or records that the RP holds

Transaction: The RP requires information from the IdP for the purposes of completing a transaction for the user

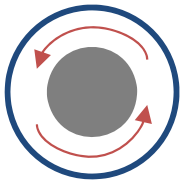
We have defined five distinct archetypes that exhibit significant differences in structure and purpose

	Internal identity management	External authentication	Centralized identity	Federated authentication	Distributed identity
Structure	 One entity acts as both the IdP and RP	 Many IdPs authenticate users to a single RP	 One IdP serves many RPs	 A set number of IdPs authenticate users to many RPs	 Many IdPs serve many different RPs
Flow of information	• The system provides users within a single network access to services that they are permissioned to access based on their attributes • All user attributes are held inside the single entity and are used to permission users to either grant or deny access to a given service or pathway	• The system authenticates users to the RP based on their authentication to one of a set of IdPs • No attributes are transferred between the IdPs and the RP; the authentication transaction is used to simply grant or deny the user access to the services offered by the RP	• The system has a single IdP that authenticates users and transfers or exposes attributes to many different RPs	• The system has a single IdP that stores user information, while a separate set of IdPs authenticate users who are attempting to transact with RPs • After authentication, the requested attributes are transferred from the IdP that holds attributes to the RP with which the user is transacting	• The system involves multiple IdPs that authenticate users and transfer attributes to many different RPs



Internal identity management solutions are designed for use by one entity

INTERNAL IDENTITY MANAGEMENT



In internal identity management systems, the same entity acts as an IdP and a RP. The entity uses information that it holds on users to permission them to access various internal services.

A good example of an internal identity management system would be a company or a government that permissions its employees or citizens to access different services based on their attributes.

KEY ARCHETYPE FEATURES

- The IdP/RP owns the required attributes needed to determine user permissions within the organization
- The system is used to control which users within a single organization or entity have permission to access certain services
- These types of solutions are generally developed by private organizations and sold as a product or service to various entities and institutions

CASE STUDIES

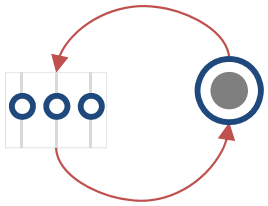
Closed Internal Management Systems

Private solutions, global

Leading software as a solution (SaaS) providers such as Salesforce, Oracle, SAP and Microsoft provide solutions that help their customers better understand, manage and interact with a set of users. SaaS has become a common delivery model for many business, as these solutions help keep users, data and applications within a closed system secure. These solutions serve a variety of industries and user groups (e.g. customers, employees, citizens, etc.).

External authentication systems facilitate access to high-traffic services

EXTERNAL AUTHENTICATION



In external authentication systems, one entity acts as both the IdP and the RP but uses an additional external set of IdPs to authenticate its users. The purpose of this system is to improve user experience for individuals or businesses when accessing online services; these users can use existing logins rather than maintaining multiple usernames and passwords for each service.

KEY ARCHETYPE FEATURES

- The system has one RP, often a government, that holds user information and leverages a set of established institutions as IdPs (e.g. FIs, telecom providers)
- The IdPs are usually trusted entities that perform strong authentication in user onboarding and are therefore trusted to provide a high level of assurance in identity transactions
- Users can use their existing authentication methods through this group of IdPs to gain access to the RP's services
- Both the RP and IdPs store user attributes – the authentication system is used to verify that the entity authenticating through the IdP should be permitted to transact with the RP
- No attributes are transferred from IdPs to the RP

CASE STUDIES

GOV.UK Verify

Public-private programme, United Kingdom

The GOV.UK Verify programme is an external authentication system that allows UK citizens to access government services online. Users verify their identity online with one of nine IdPs. Once the users are authenticated through one of these providers, they are granted access to the government service they are trying to access.

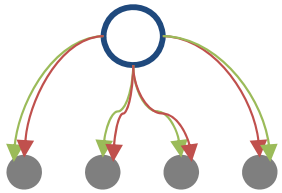
SecureKey Concierge

Public-private solution, Canada

SecureKey Concierge is a digital authentication system that allows individuals to choose a trusted credential they already have with one of a set of FIs to access government services online. The users log in with their online banking username and password and are authenticated by their bank. Once authenticated, the users are granted access to the service. No attributes are transferred in the system.

Centralized identity systems use one IdP as a single source of truth

CENTRALIZED IDENTITY



In centralized identity systems, a single entity acts as an IdP that authenticates users to RPs and transfers their attributes. These systems are often designed to streamline service delivery, enable data aggregation and provide a single view of users across multiple RPs.

KEY ARCHETYPE FEATURES

- A single IdP holds all user attributes and owns the identity system; this is often the government or another central governing body
- The IdP authenticates the user to the RP and transfers either a fixed or a tailored set of attributes to the RP to enable it to complete a transaction on behalf of the user
- Some systems require RPs to pay a fee to use the system and to gain access to user attributes
- Identity information can be transferred directly through a physical form factor (e.g. a smart card) or through a digital brokerage system

CASE STUDIES

DigID

Government programme, Netherlands

DigID is a digital authentication system for Dutch residents who are accessing government services online. Individual attributes are held in a national citizen registry; these attributes are used to authenticate users when they apply for a DigID. Individuals can then use their DigID username and password to authenticate themselves to government agencies. Their national identifier number is transferred from the national citizen registry to the RP.

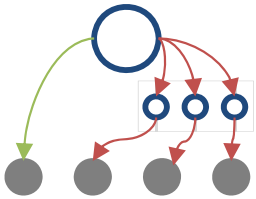
Population Registry

Government programme, Finland

The Population Registry is a national database that is owned and maintained by the Finnish government. The government acts as the IdP, transferring attributes to public and private RPs. The purpose of the system is to collect data that can be used for elections, tax filing, judicial administration, etc. Private RPs may also access this data if they pay a fee and have received user consent.

Federated authentication systems rely on third parties to grant user access to services

FEDERATED AUTHENTICATION



In federated authentication systems, one IdP uses a set of third parties to authenticate users to a range of RPs. The primary IdP is the entity that stores and transfers user attributes. These systems are designed to improve the login and transaction processes for users who are accessing online services by allowing them to use a single set of credentials to authenticate, and transferring attributes to RPs on their behalf.

KEY ARCHETYPE FEATURES

- Identity information is stored centrally by one IdP
- A set of third-party IdPs act as brokers that authenticate users to the RPs with which they are attempting to transact
- RPs are able to access user attributes from the primary IdP, often for a fee; many systems also require explicit user consent for attributes to be transferred
- In systems that allow for the discretionary transfer of attributes rather than a fixed set of attributes, the user must explicitly consent to the transfer of specified attributes from the primary IdP to the RP
- These systems are often government-driven, and the government acts as the central IdP that holds citizen or entity data

CASE STUDIES

NemID

Private sector solution, Denmark

NemID is an electronic ID, digital signature and secure email solution that provides individuals access to public and private services. The government tendered the system to the private sector. Users use a common NemID login and password, as well as unique one-time passwords to authenticate themselves to online services. User attributes are stored in a central registry.

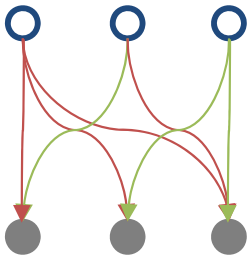
Sweden BankID

Public-private service, Sweden

Sweden has established an eID system that provides citizens and businesses access to over 300 public and private services. Digital identities are issued by a set of private entities, including large banks and a major telecommunications provider. The public sector buys identity validation services from the private sector. Private sector service providers can join the BankID system by signing contracts with eID providers for authentication. The solution has been very successful; over 9 million citizens currently use the service.

Distributed identity systems connect many IdPs and RPs

DISTRIBUTED IDENTITY



In distributed identity systems, many IdPs collect, store and transfer user attributes to many RPs. These systems are notable in that they do not rely on attributes from a single IdP. The purpose of these systems is to allow users to interact easily with many different entities in an online environment by giving them a digital "wallet" of credentials.

KEY ARCHETYPE FEATURES

- Identity information may be stored by multiple IdPs, on a distributed protocol (e.g. blockchain), or may be collected from a variety of sources and aggregated by a single entity that operates the system
- Attributes can be transferred from IdPs to RPs through a variety of methods, including smart cards or digital/mobile protocols
- These systems are often privately owned and funded; governments or other public sector bodies may not play an active role within the network
- Users own their own identities and often control which transactions occur and what attributes are transferred from one or more IdPs to the RP
- These systems may not have a governance body and instead rely on common operating standards for interoperability

CASE STUDIES

TUPAS

Private sector solution, Finland

TUPAS is an identity system in which over 10 banks act as IdPs. Individuals can log into a wide range of services with credentials from their bank. The users' full names and National ID numbers are transferred from the IdP to the RP.

Global Legal Entity Identifier Foundation (GLEIF)

Non-profit organization, global

GLEIF supports the implementation of the Legal Entity Identifier (LEI) standard. This system assigns LEIs to every entity that engages with FIs; entities can use their counterparty's LEI to access their identity information from the GLEIF's partner network.

Mobile Connect

GSMA, global

Mobile Connect is a digital identity system that authenticates the users through their device, allowing users to access a variety of services. This eliminates the need for users to have many usernames and passwords to access online services.

The potential of blockchain technology in identity

Blockchain, or distributed ledger technology (DLT), is a technology protocol that allows data to be shared directly between entities in a network, without intermediaries. DLT has certain key features that hold potential for identity systems:

FEATURES OF DISTRIBUTED LEDGER TECHNOLOGY

Low transaction cost

Distributed ledgers eliminate the need for intermediaries and therefore lower the cost of completing transactions

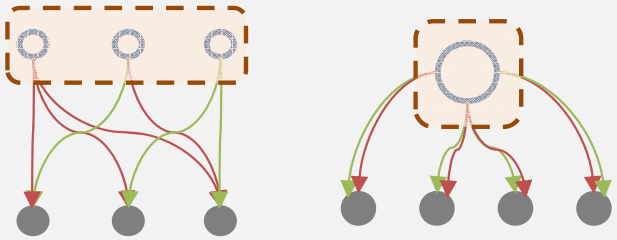
Immutability

Transaction history is maintained and verified through the network, preventing the falsification of information

Convenience

Record-keeping and transactions can be executed from any device, on- or offline

Illustrative: Applications of DLT in digital identity



DLT has potential in identity applications as an information storage and transfer mechanism within different archetypes. DLT could be applied as a distributed protocol, giving users the ability to store their identity attestations on a ledger and expose them to different RPs, or in a centralized system where the ledger would be owned by a single entity that would provide a consolidated view of the users' attestations for use in transactions, but would not reveal the nature of the credentials.

Many initiatives are currently underway that explore the true potential for DLT in identity systems; this report will not explore this topic in detail.

The Right Solution for the Right Problem

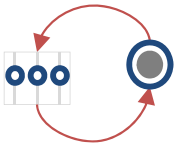
The archetypes of digital identity are built to serve very different needs

Internal identity management

Best suited to: manage user permissions inside a single entity based on internal information, to ensure the right individuals have access to the right resources and endpoints

Example: Large organizations that need an identity access and management solution to control access to their internal services with a select user group (e.g., employees, customers, etc.)

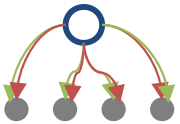
External authentication



Best suited to: streamline user access to a suite of services that are offered by a single entity and eliminate proprietary logins

Example: A government offering its citizens online services that are critical but infrequently used

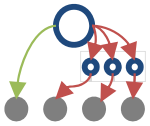
Centralized identity



Best suited to: provide a single version of the truth and a complete, accurate and standardized view of non-confidential data across different users

Example: An industry utility offering a comprehensive view of the entities in that industry to manage risk and exposure

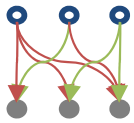
Federated authentication



Best suited to: provide a single version of the truth and a complete, accurate and standardized view of data while allowing users to authenticate to a set of third parties, thereby eliminating proprietary logins

Example: A government enabling identity transactions for its citizens through collaboration with third parties

Distributed identity



Best suited to: incorporate large numbers of IdPs and RPs, providing user convenience, control and privacy in an online environment

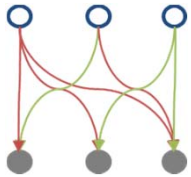
Example: A full digital economy requiring multiple independent connections between IdPs and RPs to enable user transactions

Two of these archetypes are well suited to solve broad identity problems

Centralized and distributed identity systems are best suited to provide digital identity at scale; however, these two archetypes are not equally well suited to provide identity for different user groups.

FOR INDIVIDUALS

Distributed identity

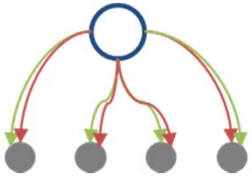


Distributed identity systems are the best fit to provide identity for **individuals** at large scale

- Distributed identity systems are built to scale to large numbers of IdPs and RPs, enabling a full set of convenient and efficient transactions for users
- These systems protect user privacy and increase control by allowing users to choose which entities hold their information, and by removing a single point of failure from the system

FOR LEGAL ENTITIES AND ASSETS

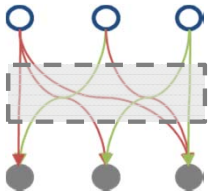
Centralized identity



Centralized identity systems are suitable to provide identity for **legal entities** and **assets** on a large scale

- Centralized identity systems offer a consolidated and standardized view of identity information, and offer the single source of truth that is required for transactions involving legal entities and assets to deliver key value to external stakeholders such as regulators

Distributed identity



Distributed identity systems are also suited to provide identity for **legal entities** and **assets** on a large scale; however, these identity systems should have a “wallet” or aggregation layer that can provide a consolidated view of the user

- Distributed identity solutions offer identity at scale, and an aggregation layer provides the single view of the user required for legal entities and assets

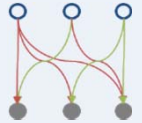
The centralized and distributed identity archetypes would also solve many of the business challenges that FIs are currently experiencing

IN RETAIL / SMALL- TO MEDIUM-SIZED ENTERPRISE BANKING

The need:

- Trusted, up-to-date individual identity information
- Ability to access additional user attributes with consent
- Ability to internally link identity information to provide a single view of the customer
- Secure repositories for user information to prevent identity theft due to stolen data

Distributed identity



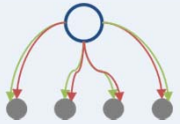
Distributed identity for individuals would allow FIs to access trusted user information and link it back to a single user identity; it would also ensure that user information would be securely stored with redundancy in the case of breach.

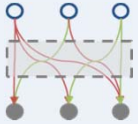
IN CORPORATE AND INVESTMENT BANKING

The need:

- Trusted, up-to-date user identity information
- Visibility into asset and user identity information
- Ability to link asset, entity identity and individual information
- Ability to aggregate identity information across entities

Centralized identity | **Distributed identity**



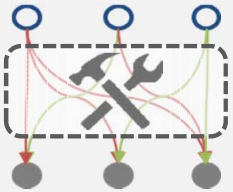


Centralized identity and **distributed identity with an aggregation layer** for legal entities and assets would allow FIs to have a consolidated, trusted source of digital attributes for these users.

Configuring and implementing an identity system require many additional choices beyond archetype selection

Configuring an identity system requires choices to be made against a secondary set of dimensions that do not have the key functional and structural importance of the primary dimensions, but have strong impact on how the system will operate. The choices made against the secondary dimensions should therefore be tailored to suit the specific needs and requirements of the natural identity network.

ILLUSTRATIVE: SECONDARY DIMENSIONS OF CHOICE



Types of IdPs and RPs: What types of entities are allowed to act as IdPs and RPs in the identity system?

Broker mechanism: How are RP queries connected with IdP attestations? Can the system support attribute exposure and attribute inquiry transactions? Does the system support transaction blinding?

Data management: Where are data stored - in a central database, on a smart card, on a distributed protocol (e.g. blockchain)? Are user attributes aggregated by a third party?

Scaling: Is the system designed to scale beyond its initial set of applications?

Business model: What is the business model that supports the system? Who funds the system?

Governance: Who is responsible for system governance and oversight? Who is responsible for system operation?

User rights: What level of control do users have over the information that is held on the system, who holds it, and when and how it is shared?

Note: This is not an exhaustive list of choices; many further choices must be made

It is impossible to provide an exhaustive list of the secondary dimensions of choice in the configuration and implementation of an identity system, or to give recommendations against each. A set of guiding principles has therefore been developed to steer secondary decision-making and to assist in delivering a robust identity system that suits the needs of its stakeholders.

Guiding Principles

The guiding principles shape the choices that need to be made against the secondary set of dimensions

A successful natural identity network is a product of the choices made against the secondary dimensions. Five principles inform decision-making around these choices and guide the development of robust, value-accretive systems.

GUIDING PRINCIPLES FOR DIGITAL IDENTITY

Social good

The system is designed as a social good that is available to all users and will deliver maximum benefit to a range of stakeholders

Privacy-enhancing

User information is only exposed to the right entities under the right circumstances

User-centric

Users have control over their information and can determine who holds and accesses it

Viable and sustainable

The system is sustainable as a business and is resilient to shifting political priorities

Open and flexible

The system is built on open standards to allow scaling and development; standards and guidelines are transparent to stakeholders

Identity systems should provide identity to all users, serve user interests and be accessible to all entities that wish to transact within them

WORLD ECONOMIC FORUM
COMMITTED TO IMPROVING THE STATE OF THE WORLD

SOCIAL GOOD

BACKGROUND

The ability to prove identity allows users to be integrated into formal financial and social systems and engage in necessary and basic day-to-day transactions; digital identity should therefore be considered a social good to which all entities should have access.

IMPLICATIONS

- The system should be designed to scale to all users and network stakeholders who wish to participate
- The public sector should have some involvement in defining the system's operating parameters and regulatory standards to ensure user interests are protected and to increase the scale of the system
- System access mechanisms (e.g. mobile platforms) should democratize access

IMPLICATIONS FOR FIs

- FIs have relationships with a large numbers of users; this scale can act as a catalyst in driving system adoption and uptake
- FIs have a key role to play in ensuring that identity systems are a tool to increase financial inclusion

CASE STUDIES

SASSA

Public-private partnership, South Africa

The South African Social Security Agency, Grindrod Bank and MasterCard have issued biometric enabled debit cards to over 22 million social security recipients. The SASSA card holds an individual's personal information on the chip, is authenticated through biometrics (fingerprint and voice pattern) or a personal identification number (PIN), and is linked directly to a bank account where social grants are deposited.

The end result is over 5 million people becoming financially included, and huge efficiencies in the distribution of social grants in South Africa.

Identity systems should be privacy-enhancing, protecting user information from illegitimate access, accidental exposure and overexposure

PRIVACY-ENHANCING

BACKGROUND

Current identity systems put users at risk, leaving user information vulnerable to privacy infringement, data leakage and overexposure. A digital identity system should protect user information, ensuring that only what is needed is revealed to RPs, and that these parties are only using the data for the disclosed purposes.

IMPLICATIONS

- All attributes, including demonstrated behaviour and preferences, should be covered in an identity system
- Attribute transfer should use new information exchange protocols that allow endpoint blinding
- The brokerage mechanism that connects the endpoints of identity queries should allow only the minimum required information to complete attribute inquiry or attribute exposure transactions to be exposed to the RP
- Attributes should only be stored by IdPs with adequate data security (as defined by system standards)
- Users or custodians should have visibility into requested identity transactions and a defined recourse method if their information is being misused
- The storage of sensitive information should be non-centralized to reduce the severity of consequences and the impact on users in the event of a data breach

IMPLICATIONS FOR FIs

- FIs should build cyber-resilient identity systems and meet standards set by the governance body around data protection and storage
- FIs will need to seek user consent to gain access to or share attributes

CASE STUDIES

TUPAS

Private identity solution, Finland

In the Finnish TUPAS system, a set of FIs act as IdPs and transfer user information on their behalf to RPs. The user has visibility into which attributes are being requested by the RP, and must provide consent for the exchange to occur .

Drivers' Licences

Government solutions, global

Traditional drivers' licences are a commonly used form of identity. However, they compromise privacy by permitting the RP to read all the user's information, rather than just the information required for the transaction.

Identity systems should give users control over the storage and transfer of their personal information

USER-CENTRIC

BACKGROUND

Many identity systems have failed due to a lack of user uptake, driven by concerns around the function and purposes of these systems. A successful digital identity system that serves as a social good should place the user (or the user's custodians) in control over identity information.

IMPLICATIONS

- The mutuality of identity should be considered; users or custodians must have clear visibility into who is requesting their information and for what purpose
- Identity transactions should require consent; exceptions must be clearly defined and communicated, and users should be advised of when their information has been accessed
- Users should be able to revoke consent
- Users should have control over where their personal information is stored
- Users should be able to easily update their information with IdPs

IMPLICATIONS FOR FIs

- FIs will be able to request identity information from users in order to tailor products and services
- FIs will require user consent to share identity information

CASE STUDIES

ConsenSys

Private solution, USA

In the ConsenSys system, users are able to upload their information and have complete control over who their data are exposed to. Users do not choose who stores their data because all identity information is stored on uPort – a user-controlled application that operates on the blockchain.

SecureKey Concierge

Public-private solution, Canada

The SecureKey Concierge system allows Canadian citizens to access government services online by authenticating through any of a large number of FIs with which they already transact.

Identity systems should be designed as businesses that are viable and sustainable in the long term

VIABLE AND SUSTAINABLE

BACKGROUND

Implementing a digital identity system represents a significant effort for all stakeholders; stakeholders must have assurance that their investment will be worthwhile. The system must therefore be designed as a viable and sustainable project.

IMPLICATIONS

- The public sector should have some role in system development and implementation to represent user interest, to drive uptake and to ensure regulatory participation
- The private sector should be involved in system development and implementation to provide executional ability, and operational viability and ensure the system is cost-effective
- Both the public and private sectors should play a role in developing operational standards, including:
  - Liability and dispute resolution
  - Business model
  - Information collection, storage and transfer
  - Levels of assurance
  - Technical requirements
  - User consent models
  - Auditing

IMPLICATIONS FOR FIs

- FIs have a key role to play as important and trusted private entities in shaping the system's operational requirements and standards
- FIs will have the opportunity to monetize identity-as-a-service

CASE STUDIES

National ID Cards

Government solution, United Kingdom

The UK government introduced national ID cards as a personal identification document. The system was scrapped in January 2010, as the incoming government stated the system was "wasteful, bureaucratic and intrusive", posing a significant threat to the privacy and security of personal information.

Clarient Entity Hub, DTCC

Private identity solution, global

Clarient Entity Hub is a utility designed to manage data and regulatory complexity for parties engaging in financial transactions. It aims to increase transparency across financial markets and is offered as a paid service to other entities.

Identity systems should be built on open technology and data standards, and should be designed to integrate new parties and serve changing user needs

OPEN AND FLEXIBLE

BACKGROUND

Identity systems that are static and designed for a single purpose are by nature limited in scope and have low resilience to environmental changes. A resilient identity system should accommodate changing requirements and integrate new parties.

IMPLICATIONS

- The system must be built on open technology standards
- The system must be built on open data standards
- The system must have clear standards around IdPs and RPs, such that new entities can join the system and adhere to all standards and requirements
- The system must have a governance body that will continuously adapt requirements and standards and monitor system performance

IMPLICATIONS FOR FIs

- Open technology and data standards will reduce barriers to users switching institutions

CASE STUDIES

X-Road

Government solution, Estonia

The Estonian digital identity system is built on a common technology framework, called X-Road. This framework creates interoperability between different databases, hugely increasing the digital identity system's functionality and effectiveness.

European Union E-Identity Legislation

Public sector solution, EU-wide

The EU E-Identity legislation sets requirements for member states issuing identity to citizens to ensure mutual recognition and scale of identity systems across Europe.

The established implications should help guide decision-making around configuring identity systems

Building a successful identity network is difficult. A series of choices need to be made to ensure the system delivers value to all stakeholders and gains traction and acceptance.

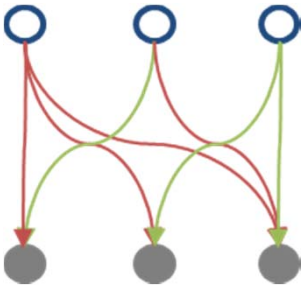
- The highest-level considerations in the development of an identity system are the user group and the need that the system will serve, and the archetype structure that should therefore be considered.
- Once these considerations have been settled, the secondary dimensions of choice should be considered against the guiding principles of digital identity.

1
Problems and user groups

The highest consideration is the user group and the problem that the identity system is designed to solve; this will determine the limits of the natural identity network

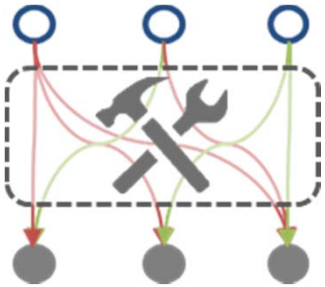
2
Primary dimensions of choice

The user group and target problem will guide the selection of an appropriate identity archetype



3
Secondary dimensions of choice

The guiding principles for identity and their implications will help determine what structural and configuration choices should be made against the secondary dimensions of choice



These implications are meaningful for entities within the digital identity network

When configuring identity systems, stakeholders will have a set of decisions to make at each stage of the process.

ILLUSTRATIVE: Some open questions for identity stakeholders

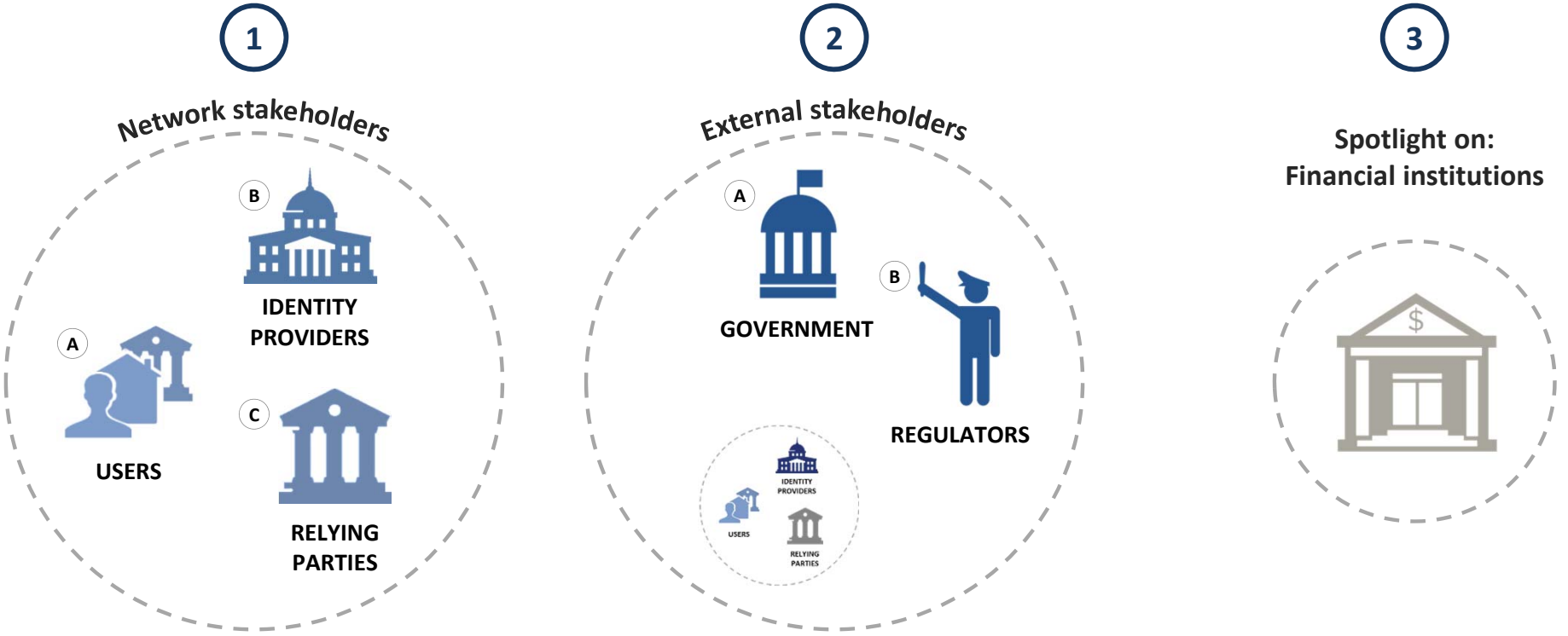
1. **Problems and user groups**
   - Which user group does this system serve? What problems will the system solve?
   - What unique characteristics will affect this user group's acceptance and use of an identity system?
   - Which archetype is best suited to solve this problem?
2. **Primary dimensions of choice**
   - Which entities should act as IdPs in this system?
   - What type of RPs should be included in this system?
   - What type of information must be transferred in the system?
3. **Secondary dimensions of choice**
   - What technology standard and trust framework will the system use?
   - What assurance model will the system use?
   - Should the system use an identity-as-a-service, fee-for-transaction business model?
   - How will the governance body be organized? What entities will be involved in system governance?
   - How will the user give consent in transactions?
   - Will any exceptions to user consent requirements be allowed?
   - How will the public sector be engaged in shaping the operational standards?

Benefits

The implementation of digital identity networks would benefit a set of different stakeholder groups

Identity systems that are constructed based on this guidance will deliver benefits both to the stakeholders involved directly in the identity network and to external stakeholders. FIs, specifically, would accrue deep benefit as a result of the implementation of digital identity.

STAKEHOLDER GROUPS



What benefits would accrue to network stakeholders?

Network stakeholders are parties who are involved in the core operation of the network itself. The network stakeholders are users, IdPs and RPs.

A

USERS

Privacy and control
Users are able to control who has access to their attributes

Security
User attributes are held in safe and secure locations

Convenience
Digital attribute transfer allows users to transact in an efficient manner

Transparency
Users have visibility into how and when their attributes are exposed

B

IDENTITY PROVIDERS

Revenue growth
IdPs can charge fees for processing identity transactions

Decreased risk and liability
IdPs understand their liability in the event of data loss or breach

Competitive positioning
IdPs can forge a strong relationship with users and position themselves as a critical part of the digital economy

Improved products and services
IdPs can use detailed and trusted customer information to deliver tailored services

C

RELYING PARTIES

Information accuracy
RPs have access to trusted, verified identity information

Decreased transaction abandonment
A streamlined user experience removes barriers to completing transactions

Service tailoring
RPs can provide more tailored products and services

Decreased risk and liability
RPs understand their liability in the event of data loss or breach

Service provision
RPs can differentiate between illicit and legitimate users

What benefits would accrue to users?

USERS

Privacy and control

1. Privacy and control

- Users would have full control over which IdPs hold their attributes
- Users consent would be required before IdPs could expose attributes to RPs
- User data would not be sold by third parties
- The minimum amount of user information required would be transferred during transactions

Security

2. Security

- User attributes would only be held by entities meeting system standards and requirements for information handling and storage
- Digital attribute storage would make identity information resistant to damage, destruction or loss
- Users would have the ability to disperse their identity information, creating contingency if an IdP suffered a data breach or data were erased or stolen, and reducing the impact of a data breach on the user

Convenience

3. Convenience

- Digital identity and digital attribute transfer would simplify and improve the user experience in transactions, eliminating the need for users to track multiple authentication methods (e.g. usernames and passwords) and manually submit personal information during transactions
- Attributes would be transferred digitally, removing the potential for human error and subsequent information remediation
- Users would be able to easily update information held with their IdPs and would not have to deal with transactions being executed based on inaccurate or out-of-date information

Transparency

4. Transparency

- Users would have visibility into which attributes would be exposed and to what entity during identity transactions

What benefits would accrue to users?

USERS: Case study

Estonia's e-government system protects citizen information, provides an extremely convenient experience for users and allows them to feel ownership over their data.

E-Government

Government solution, Estonia

- The Government of Estonia has created a digital interface between citizens and government agencies. The government holds citizen information in a centralized Population Registry and acts as the IdP and governing body, transferring reliable and trusted data to RPs.
- Citizens are each assigned an eID identifier that they can use to log on to the State Portal, which provides access to dozens of services, from voting, to updating automobile registries, to applying to universities. The government transfers the attribute information needed to complete each transaction from the Population Registry to the RP, and citizens are able to see what entities have accessed their information.
- Citizens of Estonia have the ability to view who has accessed their records, how often and for what purpose. This transparency allows citizens to feel ownership over their data, as they are able to see how the information is being used.
- A compelling example is the Electronic Health Record – a nationwide system that integrates data from various healthcare providers into a single portal. Users are able to log on to a Patient Portal to control their treatment and manage their healthcare information.

Chekk allows users to own, manage and share their personal information

Chekk

Private sector solution, Global

- Chekk is a mobile solution that provides users with a secure wallet of their personal attributes and allows them to share up-to-date information with the entities with which they transact.
- In the Chekk system, only the information required for a transaction is supplied, meaning that the user is in control and their privacy is protected.

What benefits would accrue to IdPs?

IDENTITY PROVIDERS

Revenue growth

1. Revenue growth

- IdPs would complete identity transactions for RPs; this would allow them to monetize identity-as-a-service through per-transaction fees or other business models

Defined risk and liability

2. Defined risk and liability

- Liability guidelines would be clearly defined and communicated; IdPs would be clear about their liability in the event of data loss or breach, or contravention of the standards for identity provision

Competitive positioning

3. Competitive positioning

- IdPs would be able to forge a strong relationship with users and position themselves as a critical part of the digital economy, given their unique insight into users and their established position of trust

Improved products and services

4. Improved products and services

- IdPs would have increased access to detailed and reliable user information that would allow them to better tailor processes, products and services
- IdPs could begin to draw on non-standard user attributes to better manage and evaluate risk (e.g. health records)
- Secure digital identity protocols and digital attribute transfer would improve user experience and expand the number of services that IdPs could securely provide online

What benefits would accrue to IdPs?

IDENTITY PROVIDERS: Case study

A set of banks act as IdPs in the TUPAS system, providing individuals with access to over 180 public and private services.

TUPAS

Private sector solution, Finland

- The Federation of Finnish Financial Services drove the creation of a bank identity system called TUPAS, designed to improve user access to online services.
- The RPs pay for the service (initiation fees, monthly fees and fees for set transaction volumes). Users may also be charged on a monthly basis, depending on their relationship with their bank.
- While a group of telecoms in Finland offer a competing service, as of February 2016, 95% of all online service logins were processed through TUPAS. Only 2% of online service logins were processed through the competing system. This may be due to the government's strong adoption of TUPAS, citizen loyalty towards government and banks, or the fact that it was the first successful service in the region. TUPAS has established a new revenue stream for banks as well as a strong competitive position.
- With most banks, the user must approve and certify that the data being transferred from the bank to the RP are accurate, eliminating any liability risk for the IdP.

What benefits would accrue to RPs?

RELYING PARTIES

Information accuracy

1. Information accuracy

- RPs would have access to trusted, verified identity information matched to the level of assurance required for their products or services; this would eliminate the need for information remediation and for information cross-checks through paid third-party services
- Digital attribute exchange would eliminate the potential for human error in transactions

Service tailoring

2. Service tailoring

- RPs would be able to provide more tailored products and services to users by requesting access to identity information beyond what they would traditionally require to complete transactions

Service provision

3. Service provision

- More reliable and accurate identity protocols would give RPs greater ability to differentiate between illicit and legitimate users, and to deny or provide services accordingly

Decreased transaction abandonment

4. Decreased transaction abandonment

- A more streamlined user experience would remove barriers to completing transactions (e.g. forgotten login information, required account creation, rejected billing information) and would therefore reduce the rates of users' transaction abandonment

Decreased risk and liability

5. Decreased risk and liability

- Liability guidelines would be clearly defined and communicated; RPs would be clear about their liability in the event of data loss or breach, or contravention of the standards for identity provision

What benefits would accrue to RPs?

RELYING PARTIES: Case study

The Population Registry is a central database that stores identity information – the data are trusted by many entities in Finland as a comprehensive source of up-to-date information about citizens, assets and legal entities.

Population Registry

Government programme, Finland

- The Population Registry is a national database owned and maintained by the Finnish government. The government acts as the IdP, transferring attributes to public and private RPs.
- Citizens are required to provide up-to-date information to the Population Registry, such that IdPs can trust that the information they are receiving is accurate.
- Public RPs that require attributes to complete transactions can use citizens' national ID numbers to access data held in the Population Registry. The necessary attributes are transferred digitally from the registry to the RP.
- Private RPs can also subscribe to the Population Registry and access information (with consent) to provide better products and services to their users.

What benefits would accrue to external stakeholders?

External stakeholders are parties that are not involved in the system's day-to-day operation, but are key stakeholders in the system. The external stakeholders are governments and regulators.

A

GOVERNMENTS

Process streamlining and efficiency
Governments can more efficiently interact with their citizens, saving time and money

Improved service delivery
Governments can more easily identify and deliver services to various groups of citizens

B

REGULATORS

Tracing of assets
Regulators can more effectively trace asset origination and ownership

Transparent view of entities
Regulators can access an aggregated view of legal entities across their hierarchies

Improved compliance
Regulators can access trusted, up-to-date attribute information for users, improving the effectiveness of the overall compliance process

Data standardization
Data collection and storage can be standardized across all FIs, reducing friction in data aggregation

What benefits would accrue to governments?

GOVERNMENTS

Process streamlining and efficiency

1. Process streamlining and efficiency

- Governments would be able to more efficiently interact with their citizens, saving time and money in the delivery of services such as tax filing and the distribution of social assistance

Improved service delivery

2. Improved service delivery

- Governments would be able to leverage accurate identity information to more easily identify the individuals and entities that are eligible to access given services
- Governments would be able to easily identify and deliver services to those who might be financially or socially excluded due to the lack of traditional identity information

What benefits would accrue to governments?

GOVERNMENTS: Case study

The Aadhaar programme was introduced in India to increase social and financial inclusion by providing identity for all Indians residents, many of whom previously had no means of proving their identities.

Aadhaar

Government programme, India

- The Aadhaar card was developed to improve financial inclusion in the country. The Unique Identification Authority of India (UIDAI) acts as the central IdP, controlling who has access to the data that they collect and store.
- To receive a card, individuals submit various documents to a local registrar. If they are unable to provide documentation, an "introducer", such as an elected representative or a local teacher or doctor, can vouch for the person's identity. This parallel process decreases the chance of UIDAI storing inaccurate information or providing social services to illegal immigrants or other illicit actors. The UIDAI has a database that holds information such as name, date of birth, and biometrics data that may include a photograph, fingerprint, iris scan, or other information.
- The Aadhaar program has been very effective in increasing financial inclusion with over 1 billion people enrolled for accounts, however there are still some outstanding concerns about information protection and privacy.

The Estonian e-Residency program allows non-Estonian citizens to gain digital residency in the country.

E-Residency

Government programme, Estonia

- The e-Residency program allows non-Estonian citizens to get a digital ID card that enables them to use Estonian private and public services and to use secure digital signatures. The purpose of the program is to create a virtual business environment and continue to position Estonia as a hub of the digital world
- Since its inception in December 2014, almost 10,000 people have applied for e-Residency and over 400 have established an new company domiciled in Estonia.

What benefits would accrue to regulators?

REGULATORS

Tracing of assets

1. Tracing of assets

- Regulators would be able to more effectively trace asset origination and ownership, increasing their ability to track the proceeds of criminal activity
- Asset rehypothecation could be traced, ensuring that assets would not be rehypothecated beyond their total value

Transparent view of entities

2. Transparent view of entities

- Regulators would have access to an aggregated view of legal entities across their hierarchies, increasing their ability to evaluate systemic risk and manage stability

Improved compliance

3. Improved compliance

- Access to trusted identity information would increase the ability of FIs to be compliant with anti-money laundering, know-your-customer and other regulations within their jurisdiction
- Access to trusted information on legal entity and asset identity would allow FIs to more accurately detect money laundering and other suspicious transactions
- Access to trusted digital attributes would allow FIs to automate their compliance processes to some degree, potentially allowing regulators to increase the required frequency of compliance reviews

Data standardization

4. Data standardization

- Data collection and storage could be standardized across all FIs, reducing friction in data aggregation

What benefits would accrue to regulators?

REGULATORS: Case study

GLEIF is an organization that supports the implementation of the Legal Entity Identifier standard – this standard might ultimately become a common thread between identifier systems in an effort to create a standardized global view of legal entities.

Global Legal Entity Identifier Foundation (GLEIF)

Non-profit organization, global

- GLEIF manages a network of Local Operating Units that issue Legal Entity Identifiers (LEIs) to legal entities worldwide.
- Legal entities engaging in financial transactions submit a standard set of attributes to a Local Operating Unit, which validates them against third-party records and then issues an LEI. GLEIF holds the master file of all LEIs and associated entity information.
- The system was introduced by financial regulators to improve micro- and macro-prudential risk assessment and management, increase market transparency and improve the accuracy of financial data.
- Beyond financial services and regulation, the goal 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).
- Over 430,000 LEIs have been issued since October 2015. The LEI is intended to become the link between all other identifier systems (e.g. know-your-customer systems, business register codes, etc.). This would allow regulators to have a consistent and comprehensive view of all legal entities and financial instruments globally.

FIs have key features that would give them structural advantages within identity systems

FIs have unique advantages that make them well-suited to playing key roles in digital identity networks.

ADVANTAGES OF FIs IN DIGITAL IDENTITY

FIs are highly reliant on identity

Identity is central to the function of FIs, while they bear a large part of the cost of ineffective identity protocols

FIs are connected to many key identity stakeholders

FIs have standing relationships with users, governments, regulators and other key stakeholders, and have experience working with these groups on key concerns while balancing competing interests

FIs are trusted institutions

FIs are more trusted by consumers to hold personal information than other institutions, such as governments, telecoms and technology companies

FIs have existing business models that do not require directly monetizing customer information

CASE STUDIES

iDIN

Private sector solution, Netherlands

iDIN was created to capitalize on the large investments that banks have made in onboarding their customers; banks already collect highly trusted identity information and are well positioned to transfer it to other parties.

NemID

Private sector solution, Denmark

To maximize the adoption of NemID, the governing body wanted to cooperate with private actors who have frequently used services; banks not only interact with individuals on a regular basis, but are also seen as trusted institutions that already store user identity.

SecureKey Concierge

Public-private programme, Canada

SecureKey partnered with nine banks that are trusted and hold accurate data; this data can be used to authenticate individuals in the system.

What benefits would accrue to FIs from the implementation of digital identity?

The benefits to FIs of implementing digital identity fall into six categories:

FINANCIAL INSTITUTIONS

Improved products and services
FIs will be able to use detailed and trusted customer information to deliver tailored services to customers

Operational efficiency
Digital attribute transfer and handling will allow FIs to streamline and automate many processes, eliminating human error

Decreased fraud
The secure, digital storage of user information will reduce fraud resulting from stolen information or compromised authentication

Improved compliance
Digital attribute handling and greater access to user identity will allow FIs to complete compliance processes more easily and accurately

Revenue growth
FIs will have the opportunity to increase revenue from improved products and services as well as to offer identity-as-a-service

Better user experience and competitive positioning
FIs can offer a streamlined user experience and position themselves as a critical part of the digital economy

What benefits would accrue to FIs from the implementation of digital identity?

FINANCIAL INSTITUTIONS

Improved products and services

1. Improved products and services

- FIs would have increased access to detailed and reliable user information that would allow them to better tailor processes, products and services such as:
  - Risk scoring for insurance products
  - Financial advisory
  - Asset management
  - Credit scoring
  - Loan adjudication
- FIs could begin to draw on trusted information, with consent, to better manage and evaluate risk; secure digital identity protocols and digital attribute transfer would improve user experience and expand the number of services that FIs could securely provide online

Operational efficiency

2. Operational efficiency

- FIs would be able to access user information in a consolidated, digital form through queries in the digital identity network; having attributes in a consolidated digital form would provide a single view of the customer and allow FIs to streamline customer-facing operations, such as onboarding, as well as many back-end processes
- Digital identity for assets would allow FIs to track financial products and assets more closely, through greater visibility into ownership and the resolution of rehypothecation concerns

Decreased fraud

3. Decreased fraud

- User information would be held only by entities that follow standards around data protection; this would reduce fraud (such as card-not-present transactions made using shipping and billing information stolen in large-scale data breaches)
- Digital authentication methods would reduce fraud resulting from hacked or compromised user accounts

What benefits would accrue to FIs from the implementation of digital identity?

FINANCIAL INSTITUTIONS

Improved compliance

4. Improved compliance

- Digital identity would give FIs access to trusted, up-to-date attribute information for users, improving the accuracy of know-your-customer processes
- Digital information transfer and storage would allow FIs to complete their compliance processes more quickly and easily, allowing faster processing and reducing time spent on information remediation and correcting human error
- Compliance processes could be automated and executed on more regular cycles
- Digital identity would give FIs better visibility into corporate ownership structures and the identity of corporate directors to improve corporate know-your-customer processes
- Digital identity would give FIs better visibility into asset origination and ownership

Revenue growth

5. Revenue growth

- FIs could monetize identity-as-a-service through business models such as subscription fees with RPs or fee-for-transaction services for high-assurance identity transactions, including:
  - Authentication
  - Digital signatures
  - The completion of identity transactions for RPs, such as providing attribute information (e.g. providing shipping information to merchants) or providing information about attributes (e.g. attesting to a merchant that a user is over a certain age based on date of birth)

Better user experience and competitive positioning

6. Better user experience and competitive positioning

- By collaborating with governments, public sector entities and other private sector entities, FIs would become part of a trusted ecosystem working on developing the digital economy
- As trusted safeguards of user information, FIs would increase the strength of their relationships with users

What benefits would accrue to FIs from the implementation of digital identity?

FINANCIAL INSTITUTIONS: Case studies

Aire is able to assist individuals who lack traditional credit information by using non-traditional user attributes to build a new credit score.

Aire

Private company, United Kingdom

Aire, a UK-based start-up, offers an alternative to traditional credit-scoring techniques. Aire allows individuals to submit a wide range of materials that are used to evaluate the individual's creditworthiness; for example, a user could submit utility or Netflix bills.

Know-your-customer utilities provide FIs with access to trusted, up-to-date attribute information for users, improving the accuracy of individual and corporate know-your-customer processes.

Industry Know-Your-Customer Utilities

Private solutions, global

Industry know-your-customer utilities, such as Thomson Reuters' OrgID or DTCC's Clarient Entity Hub, are intended to serve as reliable repositories of identity information on legal entities, eliminating the need for entities to perform know-your-customer requirements on their counterparties in financial transactions and giving them access to reliable and current information.

FIs in the TUPAS system are the only entities to hold and transfer user information, allowing them to monetize identity-as-a-service through business models such as subscription or fee-for-transaction services with RPs.

TUPAS

Private sector solution, Finland

In the TUPAS system, RPs must pay IdPs (in this case, a consortium of banks) to access trusted and accurate user attributes.

Future-State Applications

Digital identity offers FIs improved and new capabilities

Beyond the first-level benefits of digital identity that FIs would receive as a result of participating in an identity system, we have explored some future-looking use cases that illustrate additional capabilities that digital identity might offer to FIs.

POTENTIAL FUTURE-STATE APPLICATIONS

1. Tailored risk profiles

2. International resettlement

3. Attributes tied to payment tokens

4. Digital tax filing

5. Determining total risk exposure

6. Identifying transaction counterparties

7. Linking individual identity to corporate identity

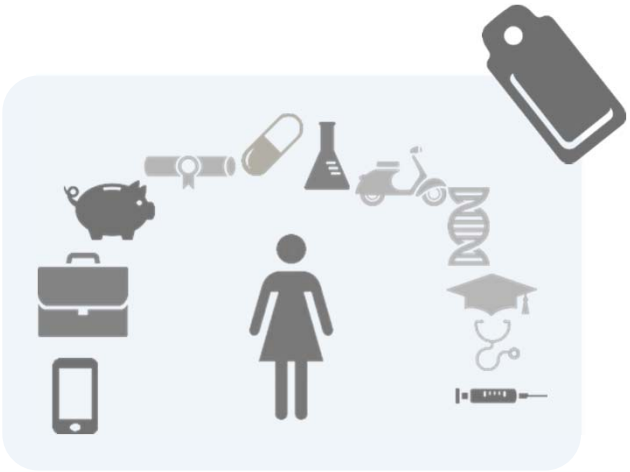
8. Tracking total asset rehypothecation

What additional capabilities can digital identity offer to FIs?

1. TAILORED RISK PROFILES

CURRENT STATE:
FIs currently create risk profiles for individuals and legal entities using the limited information that is collected when customers are onboarded and predictive algorithms to provide relevant and tailored products and services to their customers.

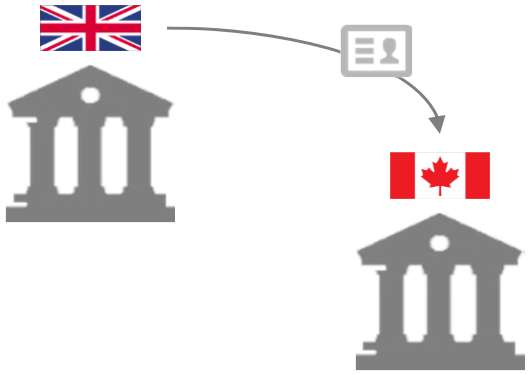
HOW WOULD DIGITAL IDENTITY HELP?
FIs could leverage trusted user attributes, with a user's consent, to more effectively build risk profiles for their customers and therefore tailor credit- and risk-based products. This enhanced user experience would ultimately lead to increased customer stickiness and offer growth opportunities for FIs.



2. INTERNATIONAL RESETTLEMENT

CURRENT STATE:
Today's onboarding processes require every FI to onboard a customer from a zero-knowledge state, resulting in difficulty opening accounts for entities that are unable to prove their identities, and disregard of financial history.

HOW WOULD DIGITAL IDENTITY HELP?
Users could transport their digital identity across jurisdictions and use it to easily gain access to financial and other services in their new place of residence; the attestations and attributes held by the user's original FI(s) would serve as the basis for new FIs to become IdPs. This would eliminate the need for the recipient FI to perform the costly and labour-intensive know-your-customer process that would otherwise be required. In addition, it would reduce the time and effort needed for FIs to onboard users, and allow them to incorporate trusted, historical information.



What additional capabilities can digital identity offer to FIs?

3. ATTRIBUTES TIED TO PAYMENT TOKENS

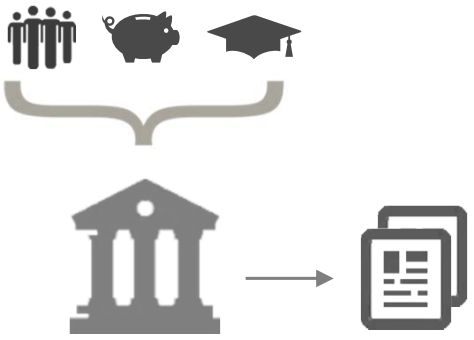
CURRENT STATE:
When completing transactions, customers are required to manually provide their attributes (e.g. confirmation of age, shipping information) or proof of attributes to merchants at the point of sale.

HOW WOULD DIGITAL IDENTITY HELP?
FIs could automatically provide customer attributes to merchants, streamlining and securing the transaction process for the merchant and customer. The digital transfer of attributes would eliminate the potential for human error in information transfer and dramatically reduce information remediation and transaction abandonment for the RP.
Note: This automatic transfer of attributes could be supported by an additional factor of authentication (e.g. mobile or behavioural authentication) to prevent fraud.

4. DIGITAL TAX FILING

CURRENT STATE:
Individuals and businesses currently file their taxes based on the aggregation of pieces of information from multiple sources (e.g. FIs, employers, educational institutions, etc.).

HOW WOULD DIGITAL IDENTITY HELP?
In collaboration with governments, taxes could be automatically completed and filings generated by customers' chosen FIs, using their complete knowledge of customers' financial holdings, assets, income and personal circumstances. With user consent, all of this information would be available through a robust digital identity network. This would allow the typically complex and tedious tax filing process to be completed efficiently and accurately.

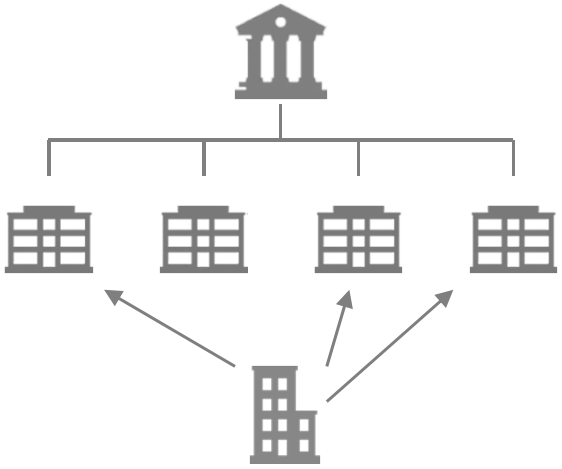


What additional capabilities can digital identity offer to FIs?

5. DETERMINING TOTAL RISK EXPOSURE

CURRENT STATE:
Legal entities are often unable to determine their total risk exposure to a given counterpart due to complicated ownership structures and difficulty aggregating a complete view of a legal entity.

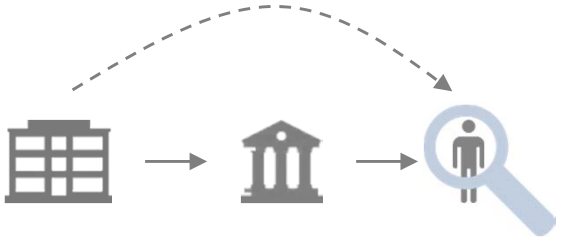
HOW WOULD DIGITAL IDENTITY HELP?
Transaction counterparties could have a consolidated view of the corporate structure of the entities with which they are transacting, allowing them to determine their total risk exposure to that entity across transactions and lines of business.



6. IDENTIFYING TRANSACTION COUNTERPARTIES

CURRENT STATE:
It is currently challenging or impossible for entities to identify all entities that are participating in a given transaction; they may not have visibility into the end customer in a transaction that is being completed by a broker or other counterparty.

HOW WOULD DIGITAL IDENTITY HELP?
Legal entities could request visibility into the consolidated identity of a third party and the ownership history of a given asset involved in a transaction. This would allow them to identify both the direct customer and the end customer in the transaction, better informing the decision of whether to complete the transaction.

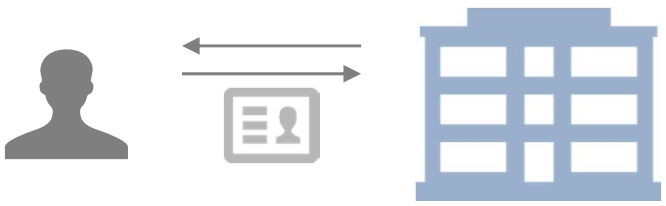


What additional capabilities can digital identity offer to FIs?

7. LINKING INDIVIDUAL IDENTITY TO CORPORATE IDENTITY

CURRENT STATE:
Individual and corporate identity information is currently not linked; it is challenging to identify individuals who are associated with corporate entities.

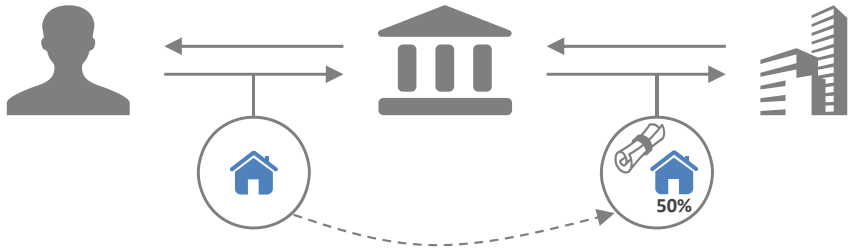
HOW WOULD DIGITAL IDENTITY HELP?
The digital and standardized collection, storage and transfer of attributes for both individuals and legal entities would ensure identity information is accurate and up-to-date. Linkages between these systems would create reliable pictures of the identities of individuals affiliated with legal entities for know-your-customer and other purposes.



8. TRACKING TOTAL ASSET REHYPOTHECATION

CURRENT STATE:
The transaction and ownership history of assets can become ambiguous as assets are rehypothecated; this exacerbates counterparty risk and asset valuation uncertainty, while the lack of a historical tracking mechanism prevents the enforcement of limits on the extent of asset rehypothecation.

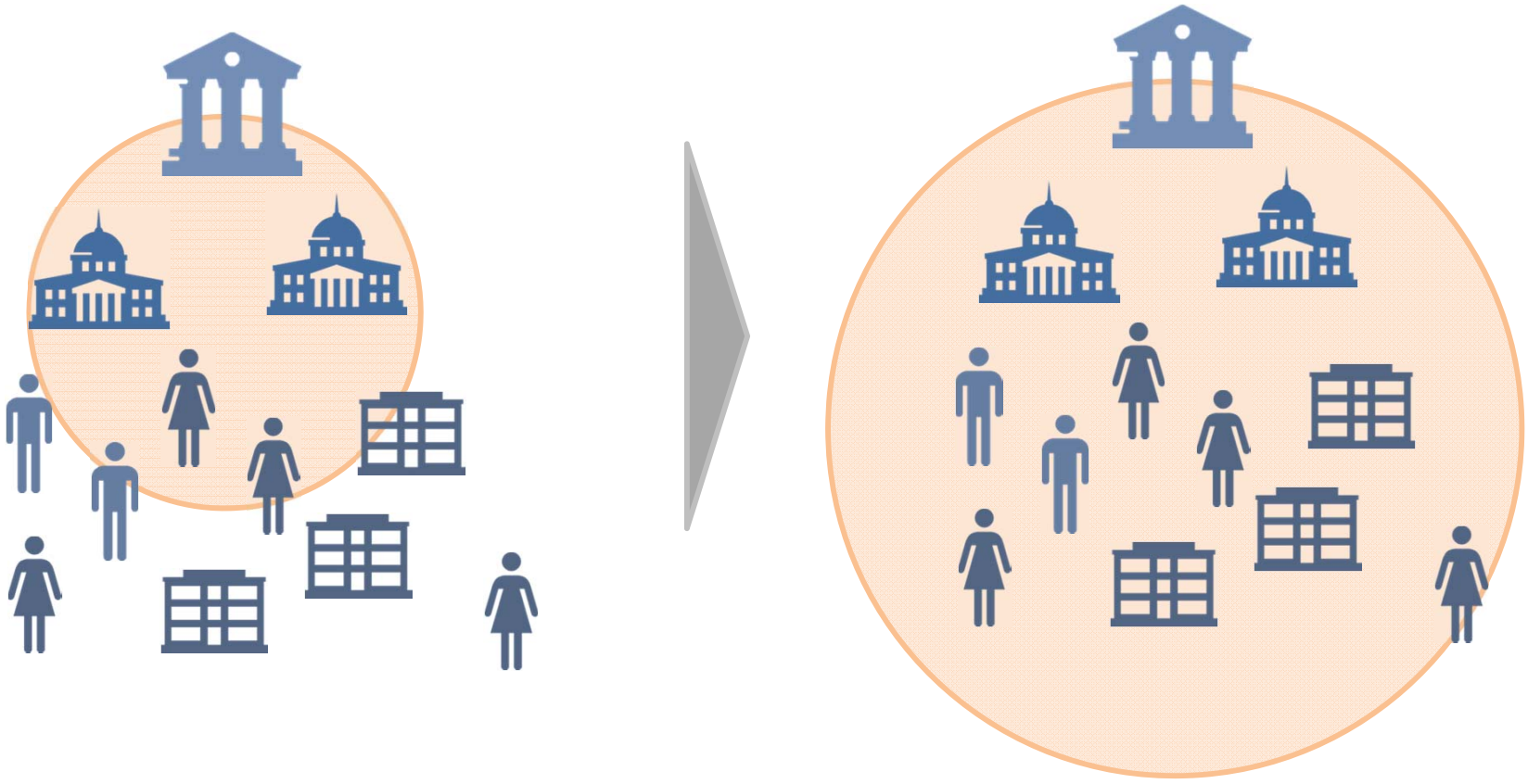
HOW WOULD DIGITAL IDENTITY HELP?
Consolidated, standardized and digital identity information for assets would be available to all entities engaging in a transaction involving that asset, giving transaction counterparties the ability to check asset information, such as issuer and transaction history; this would enable the tracking of the asset ownership structure and composition, and prevent over-rehypothecation due to the lack of visibility into past transactions involving that asset.



Implementation of Identity Systems

Implementation of a digital identity system should follow a bottom-up approach

We have outlined our perspective on the prime movers within digital identity solutions and how they should implement digital identity solutions. It is critical to observe that this is the first step in a bottom-up approach that would result in systems being scaled outwards to incorporate greater numbers of users, relying parties and identity providers as guidelines and functionality are tested and refined.



The system is launched with a critical mass of parties to test and refine

The system is scaled to increasing numbers of users, relying parties and identity providers

Global identity will never exist as a monolith

This document has laid out a principles-based approach to building effective, sustainable and bounded natural identity networks as the foundation for interconnecting individual identity networks. There will never be a single, global solution for identity.

Identity serves different needs

Different user groups have different needs and requirements for identity. Identity systems for individuals are designed to increase the ability of users to perform transactions in a safe and secure manner. Identity systems for legal entities are intended to enable comprehensive aggregation at a macro level – whether to determine total exposure to a single legal entity or manage systematic risk and stability. Identity systems for assets are designed to allow tracking and provide transparency around ownership and value. Privacy is one of the key requirements of individual identity, but is much less important in legal entity and asset identity and may even interfere with the larger purposes of these systems. Individuals have self-determination, whereas legal entities and assets have custodians who act on their behalf.

Identity is cultural

Identity is hugely affected by cultural and geopolitical factors. For example, while some populations are comfortable having a national ID card, this system has failed in other jurisdictions. Certain authorities may not be a stable government to drive the creation and adoption of digital identity.

This means that, aside from having different configurations for purely practical reasons, identity systems will differ dramatically to suit the cultural and geopolitical needs that they serve.

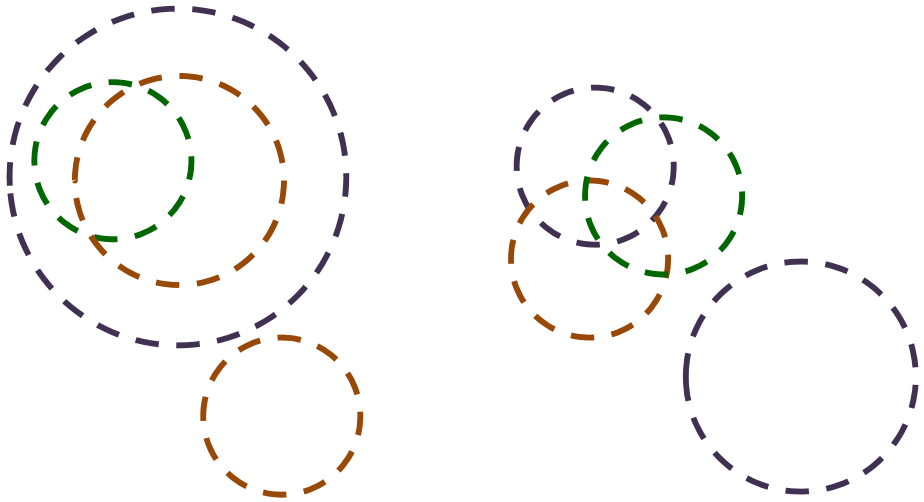
There is no one-size-fits-all for identity.

A global system for identity therefore initially requires the construction of discrete identity networks, and then the creation of rails between them

Creating a global solution for identity is a two-step process: the key to building a global system for digital identity is first building successful natural identity networks that address the unique needs and preferences of their user group and situation, and then building connective tissue that creates interoperability between these systems.

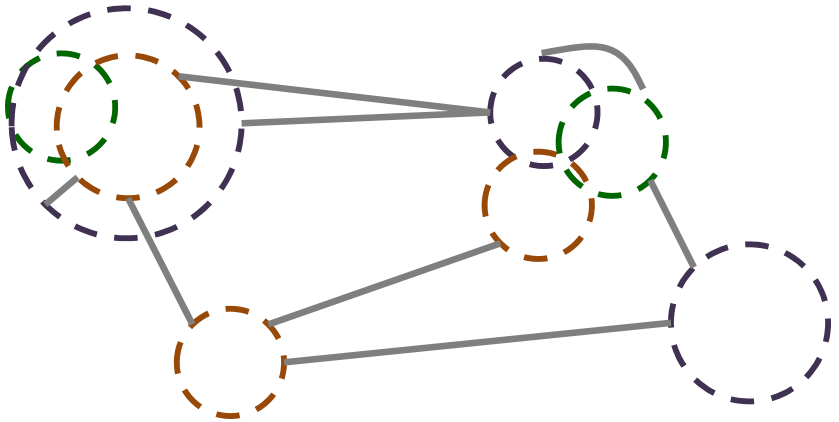
1
Implementation: Configuring natural identity networks

The configuration of natural identity networks will be guided by the decisions made against the primary and secondary dimensions of choice



2
Interconnection: Building the rails for global identity

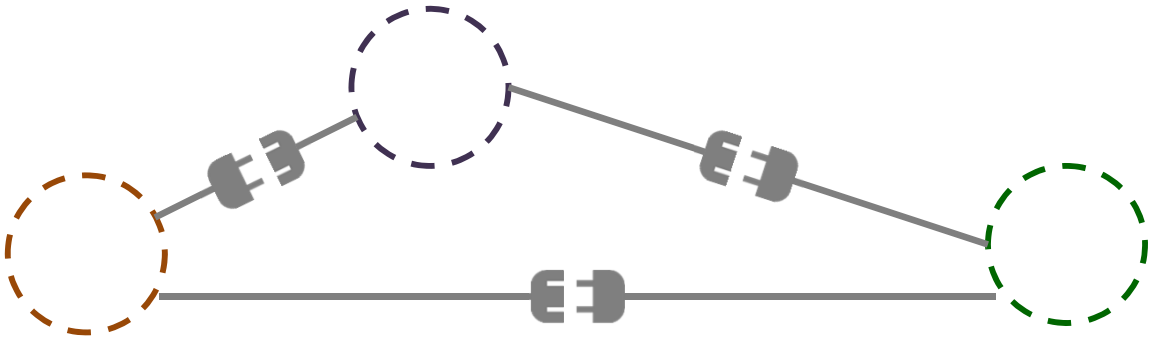
Building the rails between natural identity systems will create global interconnection and interoperability



While the rails for global identity will begin to emerge as systems develop, it is important that entities follow a guiding framework

Building identity as a two-step process enables identity systems to be built by narrowing the required stakeholders to groups that have similar needs and concerns, and therefore have relatively aligned incentives. It also ensures that these systems are tailored to the specific needs and wants of their user and stakeholder groups and will therefore gain the uptake that a top-down, one-size-fits-all system would not attain. However, these solutions should also be built following a common framework that will ensure interoperability by defining the features, attributes and requirements of the identities that are exchanged in the system. This reinforces the need for individual identity systems to be built by entities such as financial institutions that have experience working together to define standards, and then building individual systems within these standards.

Implementing discrete digital identity systems that suit the unique needs and cultural factors of users in their own jurisdictions, and designing these systems around resilience, interoperability and interconnection, will allow a global blueprint for digital identity to emerge.



There are many standing questions and uncertainties that must be considered in the creation of new identity systems

WORLD ECONOMIC FORUM
COMMITTED TO IMPROVING THE STATE OF THE WORLD

SOME THOUGHT STARTERS TO BUILDING IDENTITY SOLUTIONS

Drivers of identity systems will need to consider many detailed tactical questions in the configuration and implementation of their own identity solutions. We have provided some example questions and uncertainties below.

- Which entities need to be involved in an identity system for your area and user group – governments, regulators, financial institutions, consumer groups, others?
- What business model that will be sustainable in that situation – user pays, relying party pays, government pays? By transaction, subscription, subsidized through other services?
- What governance structure is necessary for the system – who should be involved, what should be the extent of their mandate, how will governance be renewed and refreshed?
- What is the minimum viable identity product required for that situation – what users should be involved, what services need to be covered, which entities should be involved, what metrics are being tested?
- Which frameworks and standards can be adopted for the identity system?
- Which components of the identity stack must be proprietary, and which ones can be outsourced or obtained through partnership?
- What technology platform is required for the system?
- What is the best method of communicating system functionality and benefits to users?

Contact Details

For additional information, please contact:

WORLD ECONOMIC FORUM CORE PROJECT TEAM

R. Jesse McWaters
Project Lead, Financial Services
World Economic Forum
Jesse.McWaters@weforum.org

Giancarlo Bruno
Senior Director, Head of Financial Services
World Economic Forum
Giancarlo.Bruno@weforum.org

PROFESSIONAL SERVICES SUPPORT FROM DELOITTE

Christine Robson
Deloitte Canada
crobson@deloitte.ca

Rob Galaski
Deloitte Canada
rgalaski@deloitte.ca

COMMITTED TO
IMPROVING THE STATE
OF THE WORLD