STANDALONE REPORT

GLOBAL STANDARDS MAPPING INITIATIVE 4.0

NOVEMBER 2023

DIGITAL IDENTITY

GLOBAL BLOCKCHAIN BUSINESS COUNCIL

DC Location:
1629 K St. NW, Suite 300
Washington, DC 20006

Geneva Location:
Rue de Lyon 42B
1203 Geneva
Switzerland

GSMI 4.0 IN-DEPTH REPORT

DIGITAL IDENTITY

EXECUTIVE SUMMARY

In the last years, the ecosystem around digital identity and digital identifiers has seen a rapid and significant set of announcements, activity and adoption. This is reflected through pilot projects, production deployments and governments announcing extensive funding into creating the technology infrastructure and ecosystem necessary to incubate innovative approaches using digital identifiers. However, this growth has faced a fair number of challenges. The topic of digital identity is complex, and when these have been ignored, they have caused significant harm to consumers leading to reduced trust in the process. There have also been instances where the digital identity ecosystem has enhanced the level of tracking, surveillance and violation of privacy. However, the critical challenge has been the technology methods needed to design, build, implement, and maintain the infrastructure required to offer services that consume digital identifiers. Governments, systems integrators, developers, and rights activists have struggled to form a robust understanding of how open standards-based digital identity can be a way to realizse the UN SDGs.

This report is meant to focus on a number of challenging topics in this domain. It is being published as many organizations undertake similar exploratory examination and evaluation of the technology standards, domain models, and approaches. The GBBC convened a working group of experts with deep experience in digital identifiers as a critical component of digital transformation. Technology in this sector can moves faster than any documentation, and the group fully acknowledges that work on digital identity will involve continued engagement and developments.

INTRODUCTION

In any discussion around digital identity and digital identifiers, it is essential to note that nearly 1 billion people do not have legal and verifiable identity documents — the absence of such documentation results in their inability to access various public or private services. As digital identity's issuance, circulation, and exchange increase, the public and private systems that issue such IDs must be designed to respect foundational rights. Moreover, as the world is becoming more digitized, lack of identity in the digital realm can have major implications on inclusion and lifestyles, potentially aggravating the digital divide between those with access and those without access to networks of productivity and exchange to conduct activities.

Digital identity is fundamental to meet many of the UN Sustainable Development Goals (SDGs) in pursuit of reducing global inequalities. Specifically, SDG 16 on Peace, Justice, and Strong Institutions sets a target to provide a legal identity for all, including a birth registration. Otherwise there is an increasing risk of leaving entire communities disenfranchised and cut off from means of human flourishing. Advancing digital identity also requires advancing data protection, and the most promising models are inherently people-oriented. Yet in this context, there have been several approaches to digital identity, with multiple design considerations, opportunities, and risks. While there have been several approaches in development, it is fundamental to "get it right," in the sense of providing adequate identity that is also secure.

Policymakers, regulators, governments, and other stakeholders often bring their definition of digital identity and digital identifiers. This report will define identity as <insert the definition and citation>. A digital identity may entail one or more attributes associated with the individual. The process of creation and issuance of the digital identity conveys a level of assurance necessary for the ID to be used in different workflows.

When poorly designed and implemented digital identity systems can exacerbate the topics of exclusion, surveillance, and harm - designers and implementors often grapple with the challenge of adopting the best practices, standards, and technology frameworks, which could result in better outcomes for everyone. Today, sizeable digital identity systems, which include foundational IDs such as national IDs, functional IDs such as birth and death registration records, pension systems, etc, are no longer in prototype design or pilot stage - they have gone live. This presents a fundamental challenge for future implementations, as the insights and knowledge from the ongoing deployments will be used to improve and innovate incrementally.

Digital identity systems often build upon and extend existing foundational components. While this expedites the drafting of necessary changes to regulations and workflows, it also highlights the need to focus on data quality. Digital ecosystems require digital identifiers with a high level of assurance to create trustworthy interactions. These data exchanges go a long way in mitigating the risks associated with such systems. This report examines the ongoing and emerging challenges and concerns around digital identity using the identity life cycle. This lifecycle is imagined to comprise a set of processes, including registration and enrollment, issuance, use and management. Each of these processes helps bring to light some of the complex topics associated with digital identity and audit, risk management and standards.

Digital identity systems have emerged and demonstrate a set of archetypes. These system archetypes are called Centralized, Federated and Decentralized . Each archetype has specific strengths and challenges, and while this report will not provide any comparison among these systems, it is necessary to state that the discussion around digital identity will draw from the ongoing efforts around the decentralized archetype.

As this report intends to guide and aid designers of digital identity systems, it provides a set of technical and non-technical considerations that can be read as recommendations. These considerations have been put together with the intrinsic understanding that digital IDs should empower humans and not contribute to curtailing their rights in any manner.

CHALLENGES OF DIGITAL IDS

Backdrop

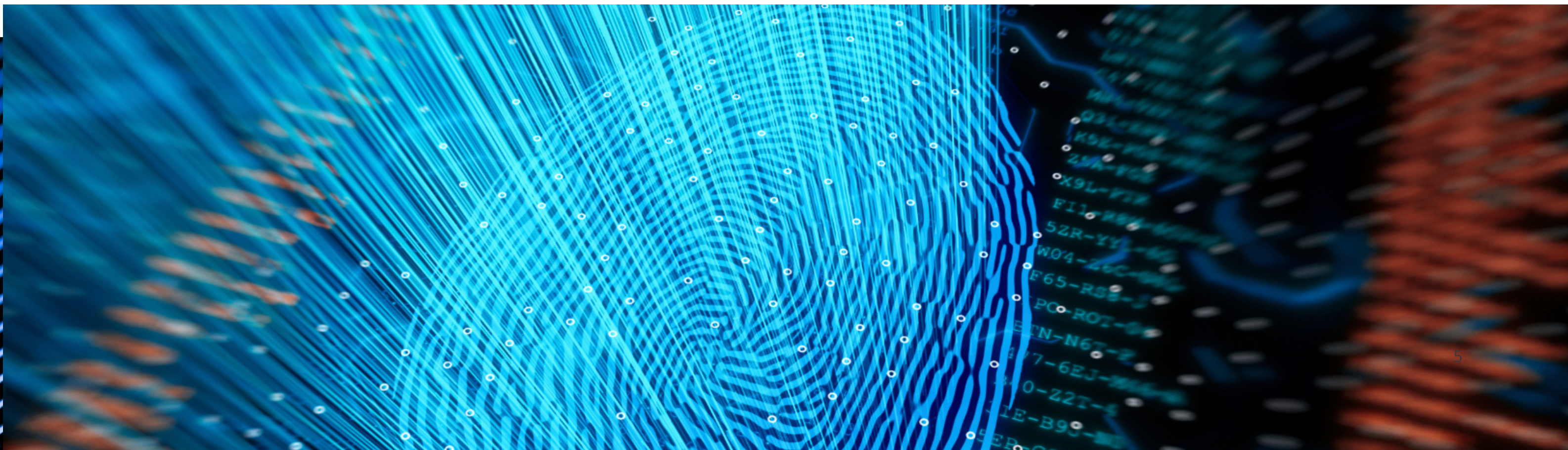
The design, development and deployment of digital identity systems bring forth complex challenges because the approach needs to consider a set of hard problems. These challenges range from synchronization and reconciliation issues of identities across disparate systems as well as being able to design robust portable IDs that do not inadvertently aggravate the digital divide. In this context, it is important to note that digital systems are relatively new. They were first created following World War II, and the earliest mainframe computers were adopted by government and industry in the 1960s. Accounts for different users were created, and these evolved over time to support employees in enterprises accessing their accounts to do their work across different applications and computers.

Many systems in enterprise and government were used to track information about people who are customers (who buy things from businesses) and citizens or residents (who pay into pension schemes and pay taxes). These people did not have their computers, but information about them lived inside these enterprise systems.

The paradigm of how to manage an employee identity in an enterprise system is widespread, and it makes sense for that context. An employer hires an employee to do work inside their enterprise. To do that work, the enterprise gives them an identifier within the context of the enterprise. To use that identifier, the employee establishes a shared secret (password) with the enterprise, and when they assert they are in control of a particular identifier, they are prompted to provide the shared secret and if they succeed in sharing that with the enterprise they are authenticated into the enterprise.

The commercial service providers in the early days of the first commercial services (like AOL, Compuserve, Prodigy) that people subscribed to used the model that employer-employee systems had - they allowed people to claim identifiers within their name spaces and then authenticate to those services and interact on the internet. This model continued with common web-mail providers like Hotmail (now MSFT), Gmail and Yahoo.

This is called the two-party model. It has an identity provider (who controls an identifier) and a relying party. For an individual to use an identifier from one service at another service (relying party), they must prove it to the relying party by authenticating to them. Tokens are exchanged between these two parties. This model of identity provider and user or employee, to whom an identifier is assigned and can be revoked by the identity provider, does not align with individual autonomy and rights that we experience daily as we move about the world in other roles outside of being “an employee.” We should therefore not have a general-purpose digital identifier revocable by another party like a government or commercial entity that, in the fundamental design of the architecture, has power over us.

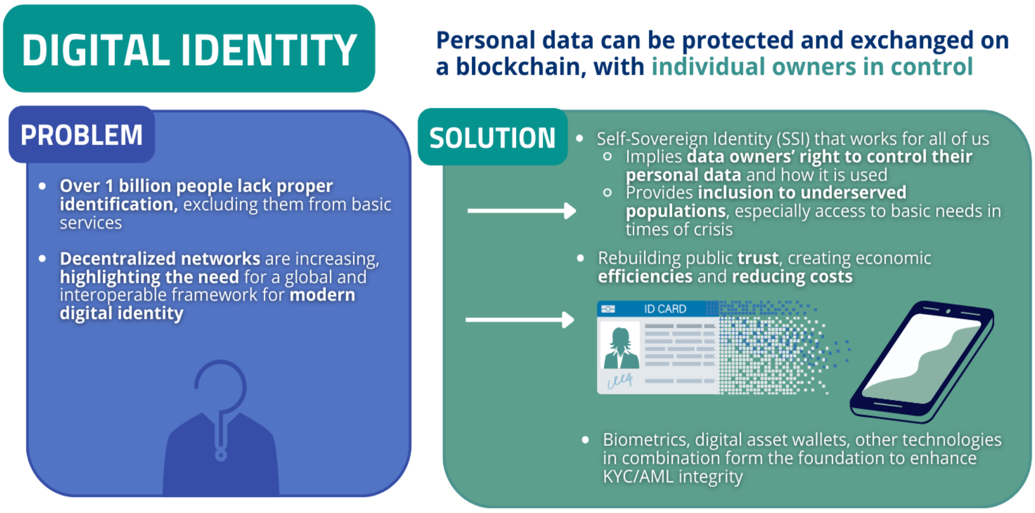


There has been a significant amount of work in the last few years by a community that has aimed to change this two-party paradigm, where there is "control over an identifier" in either a private namespace or a global registry namespace, to a model where people could create and control their identifiers. This effort spawned the Decentralized Identifier standard at the World Wide Web Consortium (W3C). Identifiers only go so far in solving identity challenges, especially ones that are very long and not humanly readable numbers. What matters to people and organizations is more information about the very people and organizations - key attributes and information. This is where work on the three-party or direct presentation model arose, where individuals are put at the center of any transaction related to identity information in a three-party model. Where issuers issue credentials (a blob of signed attributes) to holders (individuals or businesses), and then the holder can choose what relying parties (or verifiers) they want to involve, as many times as they want to, and the issuer of the credential and the verifier of that credential do not connect or talk. Hence, the three parties.

Commonly understood challenges

One of the often-quoted aspects of the challenges with digital identities is the number of individuals who do not possess any formal verifiable documentation establishing their identity and associated rights. This presents a growing challenge in addressing the inequity and denial of rights globally. Sometimes, digital identity systems are also not designed to be equitable, secure, and portable. These systems hinder the ability to use digital identity for access to services or benefits, with the holder of the ID being able to govern and manage their data.

Today, digital identity-centric systems are required as an integral part of many workflows. These range from user onboarding and KYC (Know Your Customer) flows to fraud prevention systems, electronic commerce marketplaces, delivery of healthcare and telemedicine, travel and hospitality industry, education and learning, financial services, gig economy and peer-to-peer services, etc. Delivery of citizen services by governments is one of the largest use cases of using digital identity to manage access to services for taxes, permits and document workflows.



DIGITAL IDENTITY

Personal data can be protected and exchanged on a blockchain, with individual owners in control

PROBLEM

- **Over 1 billion people lack proper identification,** excluding them from basic services
- **Decentralized networks** are increasing, **highlighting the need** for a global and interoperable framework for **modern digital identity**

SOLUTION

- Self-Sovereign Identity (SSI) that works for all of us
  - Implies **data owners' right to control their personal data** and how it is used
  - Provides **inclusion to underserved populations**, especially access to basic needs in times of crisis
- Rebuilding public **trust**, creating economic **efficiencies** and **reducing costs**
- Biometrics, digital asset wallets, other technologies in combination form the foundation to enhance KYC/AML integrity

This report will discuss specific details of the challenges in a later section. It is important to mention that an emerging discourse in digital identity and digital identity systems is the need to make them "people-oriented" and "consumer-centric". This approach enables the design and development to focus on the rights of the holders of the digital identities.

For instance, the short introduction to the UN Joint Staff Pension Fund project is provided below as an aid to conceptualize some of the complexities and the methods by which good design can help create digital trust ecosystems that are impactful, respectful of rights, and enable the delivery of services.

An Example - The UN Joint Staff Pension Fund

The United Nations Joint Staff Pension Fund (UNJSPF) supports 84,000 beneficiaries located in 192 countries. As required by its Regulations and Rules, each year, UNJSPF needs to verify the proof-of-existence and location of those receiving benefit payments through a process referred to as the "Certificate of Entitlement" exercise. For more than **70** years, this process has been conducted using a paper form and relying on **192** postal services, involving printing tens of thousands of pieces of paper, handling and processing physical mail, and sometimes multiple interactions between the beneficiaries and UNJSPF.

In 2020, COVID-19 caused widespread disruptions to postal services, negatively impacting the Certificate of Entitlement exercise. The challenge for the UNJSPF was to modernize this process and find an innovative, reliable, and environmentally sustainable solution. A digital identity solution was created to address this challenge, with a system called the "Digital Certificate of Entitlement (Digital CE)", which offers a secure and user-friendly mechanism to verify the existence of retirees and beneficiaries for the continuation of benefit payments and generates traceable, unalterable, and independently auditable evidence.

The Digital CE is a sustainable initiative, as it reduces the use of paper and global postal services. It is an application that can be loaded on mobile phones, tablets, or computers, and on average, it requires about 30 minutes to complete the initial enrollment in the first year and only 5 minutes the following years.

Aligned with the United Nations Secretary-General's vision of a digital UN, the Digital CE is part of implementing the UNJSPF strategic plan and Information and Communications Technology investment in simplifying client experiences and modernizing the Fund's services.

Compared to the paper-based proof-of-existence solution, the Digital CE application offers retirees and beneficiaries a much faster, more secure, and easier way to validate their identities and locations to meet the requirements for continued benefit payments. After downloading the application on their smartphones or tablets, they can enrol in the app in a few easy steps by filling out some personal information and taking pictures of themselves. Once enrolled, they schedule an in-person video appointment with the Fund's Call Centre to complete the identity verification process.

DESIGN AND TECHNOLOGY CHOICES

In designing the Digital CE application, the project team put clients' needs at the heart of the process and focused on simplifying the client experience. Adopting a human-centred approach, the product development team identified retirees' and beneficiaries' needs at the outset, considering the disparity in geographical location, technological ability, mobile device availability, and internet connectivity. The team used an iterative approach to build multiple proofs of concepts and ran a pilot incorporating user feedback from beneficiaries to improve product usability and design.

The project team explored new technologies to develop a user-friendly and cost-effective solution. Biometric technology, such as facial recognition, was used to authenticate beneficiaries' identities. Project team members worked hard to perfect the facial recognition functionality and improve the application's user-friendliness. After assessing existing off-the-shelf solutions, they built a custom-made biometric facial recognition solution to deliver better results. The solution is now being incorporated into other innovation plans involving digital identity within the United Nations System. In addition, the Digital CE application incorporated emerging geolocation technology that can capture beneficiaries' physical locations to validate their places of residence. The application also embedded blockchain technology to have a traceable, immutable and independently auditable record of the certification process.

Retirees and beneficiaries can complete their annual Certificate of Entitlement exercise entirely using the digital application, even offline, without the need to print or sign any paper. The solution also eases the burden on the Fund to manually process tens of thousands of paper forms to validate beneficiaries' identities and locations. Hence it has contributed to increased efficiency in the validation process of the Certificate of Entitlement. Considering the environmental impact of the end product, the project team designed and delivered a solution that is environmentally friendly and sustainable. The employment of a digital solution prevents thousands of paper and postal mail per year, with a target population of 84,000 retirees and beneficiaries having to fulfill this requirement. It only marginally impacts the general use of mobile phones and tablets, as it requires downloading the app and, on average, 30 minutes maximum to complete the initial enrollment, and only five minutes the following years.

PRINCIPLES OF DIGITAL IDENTITY

Any discussion around digital identifiers and digital identity needs to acknowledge the potential risk of creating unintended consequences, harms, and biases through poor design choices, poor technology implementation, and poor compliance with regulatory requirements. Sometimes, a poorly constructed regulatory framework for governance also contributes to the harms resulting from deploying such IDs. It is also essential to be aware of the fact that many digital identity systems are designed to be the next generation of IDs in an ecosystem which already has a form of identifiers. Thus, these legacy systems include a set of governance and operational rules, legal frameworks, and workflows that have worked for non-digital or analog systems.

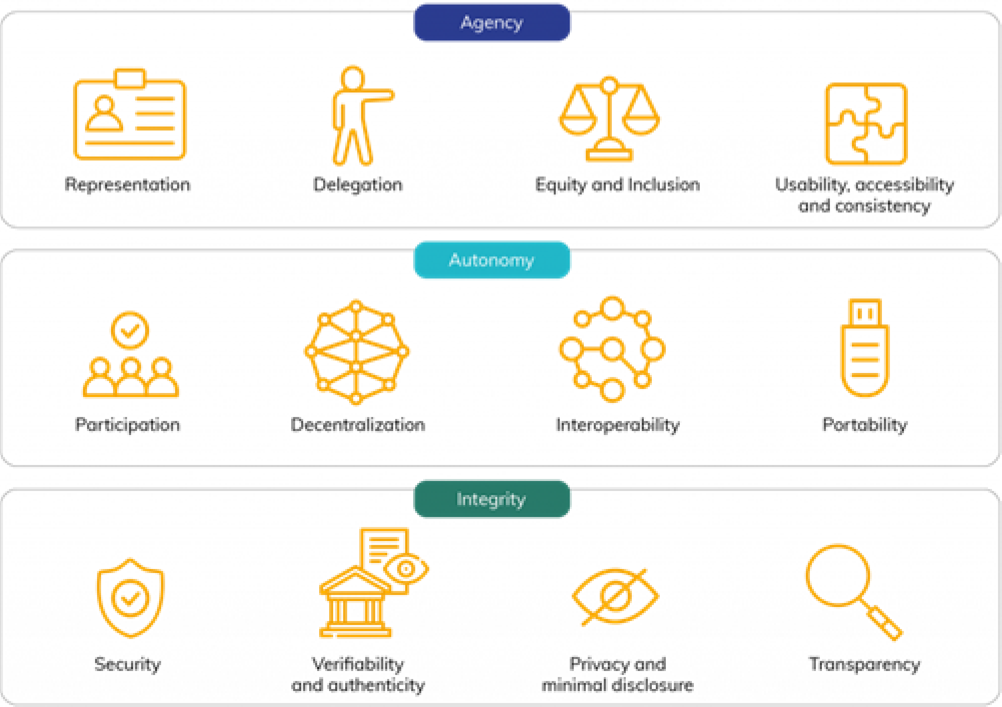
If digital identity systems are to make the expected impact, it is necessary to frame a set of principles to help design, evaluate, and assess the emerging technology patterns in digital governance. Some of the recent work in the domain of digital identity and principles come from organizations are listed below:

- **The Sovrin Foundation:** Sovrin has published[1] *The Principles of Self-Sovereign Identity (SSI)* as a set that has been organized to provide a human rights-based perspective in the context of digital identity and identity rights of holders, with the ultimate goal to enable humans to exercise their rights to work, study, and travel, while having freedom of choice and being protected.

- *Human-Centric Digital Identity for Government Officials*[2] published by the **OpenID Foundation** as a nonprofit standards body advancing identity and security specifications, with the objective of helping billions of customers, across millions of applications, to assert their identity

- The **OECD** Privacy Principles [3]which focus on collection limitation, purpose specification, security safeguards and accountability among other factors.

Figure 1: 12 Principles of SSI (Source: Sovrin Foundation)



© 12 Principles of SSI v3. Copyright CC BY SA 4.0 Sovrin Foundation

DIGITAL IDENTITY LIFECYCLE AND STANDARDS

Digital Identity Lifecycle

As new approaches to digital identities go into production, it is important to note that such identifiers create opportunities for advancing inclusion, privacy and agency over one's data. Digital identities help the holders of such identifiers to make claims about specific attributes. The digital identity has a lifecycle[4] which includes registration, issuance, exchange, and management flows. The entire lifecycle is the basis of enabling various use cases in different digital ecosystems to be designed around digital identities and the access to various services offered through exchanging such identities.

Each stage of the lifecycle includes specific tasks and activities made possible by adopting specifications, standards and guidelines.

It is important to highlight that not all stages of the lifecycle will have the same level of assurance - this is determined by the governance framework of the digital trust ecosystem where the digital identifiers are issued and the purpose. Assurance levels can be thought of as the equivalent of confidence and trust in the specific digital identifier based on the process through which the identifier was issued.

1. REGISTRATION FOR DIGITAL IDENTITY

- **Identity Claim -** Made possible by providing personal data and supporting documents as evidence
- **Proofing**
  - **Validation -** Ascertaining the evidence's authenticity, validity and provenance
  - **Deduplication -** Often undertaken through the usage of biometrics
  - **Verification -** To ascertain that the individual is the true holder of the identity

2. ISSUANCE

- **Credentialing -** Issuance of credentials and binding of identity attributes

3. EXCHANGE

- **Authentication -** Establishing a level of assurance by verification of presented credentials
- **Verification -** Verification of specific attributes presented as part of the assertion
- **Authorization -** To ascertain that the individual is the true holder of the identity

4. MANAGEMENT

- Updating, revocation, re-issuance and other operational actions on issued credentials
- Dispute resolution and handling of contestations
- Notifications

Important Standards and Specifications

Digital identifiers are issued and managed within a specific digital ecosystem. This means that the lifecycle of digital identifiers is influenced by the jurisdictions in which these are managed as well as the legal, regulatory and technical requirements in that particular jurisdiction. It is important to be mindful of this situation as often a wide range of standards, specifications and recommendations are involved in the production and circulation of digital identifiers. If these standards, specifications and recommendations are incompatible with each other, then the notion of interoperability, wider verifiability and trustworthiness breaks down. While it is impossible to list all possible standards and specifications related to digital identifiers, it is important to mention a few which are relevant to the concept of their significance in the digital identifier lifecycle.

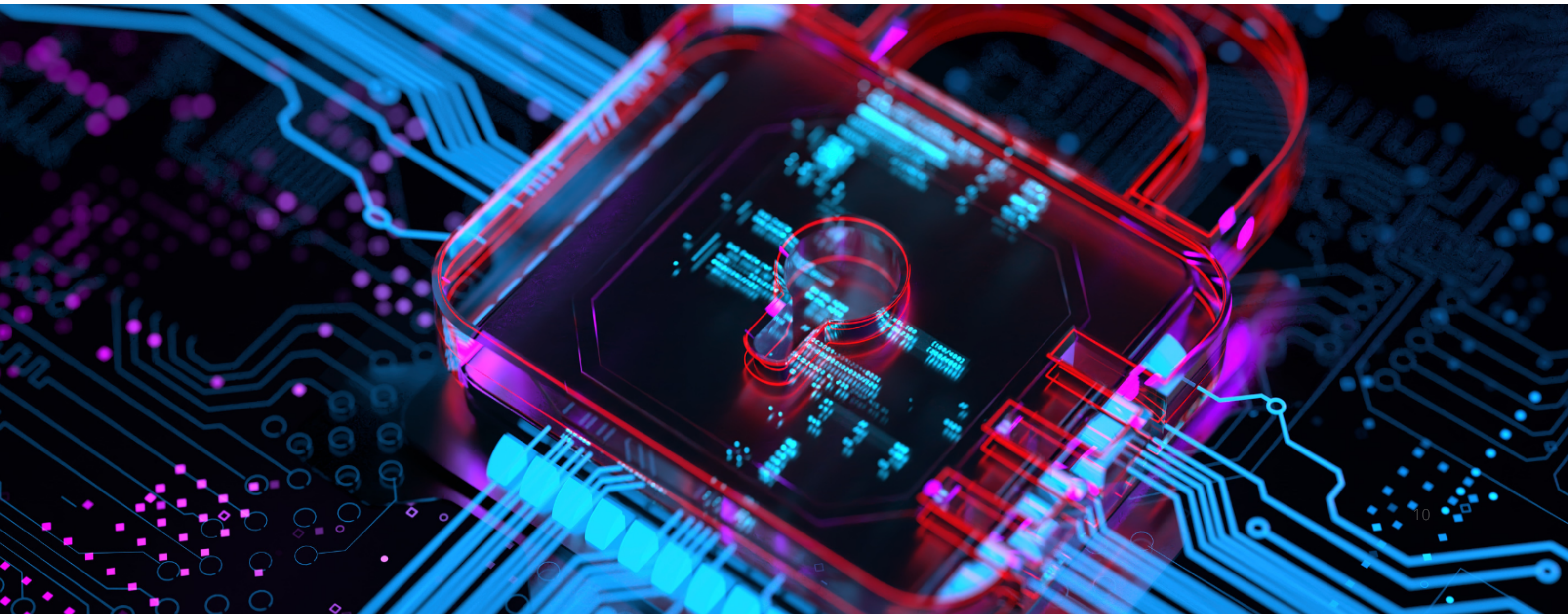
The production, management and exchange of digital information is intimately linked with the available data governance and data protection regulations.

The section on Principles of Digital IDs indicates some of the principles recommended to be adopted while designing digital identifier workflows. Additionally, there are standards and specifications which are necessary for good digital identifiers to be instantiated. Such standards include, but are not limited to the following:

- **ISO/IEC 29100** Privacy Framework
- **ISO/IEC 29134:2017** (Guidelines for privacy impact assessment)
- **ISO/IEC 29184:2020** (Online privacy notices and consent)
- **Blinding Identity Taxonomy**[5] from the Kantara Initiative Information Sharing Interoperability Work
- **NIST SP 800-63 Digital Identity Guidelines**[6] (includes 800-63-4, 800-63A, 800-63B and 800-63C)
- **Overlays Capture Architecture (OCA) Specification**[7] from the Human Colossus Foundation
- **Verifiable Credentials Data Model**[8] from the W3C

Digital Identifiers also include the topic of Risk Management and in later sections a few recommendations are provided for this aspect.

It is also important to note that there is an entire world of biometric standards that is beyond the scope of this paper. Biometrics in the form of photographs have been used for a long time on identity documents. Knowing the current best practices for creating templates and sampling against those biometrics is important while creating the regulatory framework and technical architecture for digital identifiers.



Standards Development Communities

A wide range of global standards power the technology designs which enable the digital identifier lifecycle. Standards Development Organizations (SDOs) and communities work to ensure that the process factors in regulatory and privacy requirements, and that it also addresses the topics emerging from preventing harm. Some of the notable SDOs and communities are listed below.

ISO

ISO (International Organization for Standardization)[9] is an independent, non-governmental international organization with a membership of 169 national standards bodies.

W3C

World Wide Web Consortium (W3C)[10] has been an international multi-stakeholder community where member organizations, a full-time staff, and public work to develop open web standards together across key stakeholders.

IETF

The Internet Engineering Task Force (IETF)[11], founded in 1986, is the premiere standards development organization (SDO) for the Internet. The IETF makes voluntary standards that are often adopted by Internet users, network operators, and equipment vendors, and it thus helps shape the trajectory of the development of the Internet. But in no way does the IETF control, or even patrol, the Internet.

Open ID Foundation

Founded in 2007, the OpenID Foundation (OIDF)[12] is a global open standards body committed to helping people assert their identity wherever they choose. It is a global vibrant community where identity peers and thought leaders convene to craft the identity ecosystems of tomorrow.

ToIP

The Trust Over IP (ToIP)[13] Foundation was launched in May 2020 with 27 original founding member organizations. It was gestated over the previous year as a confluence of multiple efforts in the digital identity space, verifiable credentials, blockchain technology, and secure communications spaces by people who saw the need to converge and create an interoperable architecture for decentralized digital trust.

DIF

DIF[14] is an engineering-driven organization focused on developing the foundational elements necessary to establish an open ecosystem for decentralized identity and ensure interoperability between all participants.

Open Wallet Foundation

The OWF[15] aims to set best practices for digital wallet technology through collaboration on standards-based OSS components that issuers, wallet providers and relying parties can use to bootstrap implementations that preserve user choice, security and privacy.

MyData

MyData[16] is a human-centric approach to personal data management, which combines industry need for data with digital human rights.

Kantara Initiative

Kantara Initiative, Inc[17] is an international ethics based, mission-led non profit industry 'commons'. Kantara's Mission is to grow and fulfill the market for trustworthy use of identity and personal data in pursuit of its Vision to see equitable and transparent exchange of identity and personal data for mutual value. Kantara's members are spread across continents and countries around the globe.

Human Colossus Foundation

The Human Colossus Foundation (HCF) [18]is a Swiss-based independent non-profit organization (IDE: CHE-441.741.202) working globally to create and foster the development of critical infrastructure for a data-agile economy, coined the Dynamic Data Economy (DDE).

The eSSIF-Lab

The European Self-Sovereign Identity Framework Lab (eSSIF-Lab)[19] views itself as an ecosystem of parties that work together to make existing (and new) Self-Sovereign Identity (SSI) technology into a scalable and interoperable infrastructure that businesses can use very easily for negotiation and execution of (business) transactions with other organizations and individuals alike, as further described in the eSSIF-Lab Vision.

The above list is not exhaustive. It presents a small snapshot of the various organizations, communities and bodies engaged in the work of creating robust technology designs and recommendations which can be adopted by organizations attempting to implement digital identifiers as part of enhancing the experience of the consumers.

Introduction to Digital Wallets

The digital revolution has seen an increased focus on the digitalization of several aspects of human life. Facilitated by incredible developments in the financial industry, wallets and conversations about wallets have transformed from a visually bulky leather pouch filled with precious stones, coins, banknotes and identification documents to versatile, functional and accessible digital wallets.

While most would associate digital wallets with electronic wallets that hold digital assets (essentially the digitalization of the traditional wallet), the past couple of years have brought interesting progress by both governments and private sector developers towards the creation of a functional digital wallet that private persons can use to store, manage and even share their personal data.

Variations of digital wallets have been introduced in countries like the Faroe Islands, India, Monaco, Thailand and the United Arab Emirates, allowing their citizens and residents to benefit from either a simple repository of immediately accessible personal data, whether for identification as is the drivers' license in the UAE or for having access to the financial system by simply scanning a QR code in Thailand.

The digital wallet concept has also raised the bar and intensified conversations around sovereignty, security and privacy issues concerning personal data. Interoperability, user-centric ergonomics, and global and personal security are factors that regulators and developers understand are and will be differentiating factors for long-term, sustainable solutions.

DESIGN CONSIDERATIONS

Technical Considerations

The technical considerations involved in the design of a robust digital identifier infrastructure follow from the Principles of Digital ID. It follows that with a human-centric approach to design the individual holder of the digital identifier must be at the critical element when examining competing design approaches. This leads to the following requirements as a necessary component in design

- Consent-based approach to the exchange of data
- Transparency in the acquisition, processing and exchange of data
- Selective disclosure of information unless required by local regulations
- Adoption of open standards in the design of systems to enable interoperability
- Handling of guardianship and dependent relationships to enable inclusivity, equity and representation
- Capability to address both onboarding and offboarding of consumers at end of natural lifecycle

In addition to the above requirements, there are two additional overarching guidelines which influence the technical choices and technology adoption. These are:

- **Security and resilience:** Digital identity systems should be secure and resilient to attacks. This means that they should be designed to protect personal data from unauthorized access, use, or disclosure.

- **Privacy by design:** Digital identity systems should be designed with privacy in mind. This means that they should minimize the amount of personal data that is collected and stored and that they should use privacy-preserving technologies.

Non-Technical Considerations

ETHICS

The UN Roadmap for Digital Cooperation [20]was adopted by the UN General Assembly in June 2020. The Roadmap laid down a vision for the responsible and inclusive development and use of digital technologies, and ethical principles on digital identity formed a key pillar of the Roadmap.

These principles are intended to guide the development and moral use of digital identity systems globally and in a way that respects human rights, promotes inclusion, and is devoid of bias that would disadvantage any ethnic or socio-economic group. Since there are only regional pockets where compliance standards, mandates and penalties exist, the recommendation included developing and advocating a shared and globally acknowledged set of ethics compliance parameters that would be set by federal mandates and or legally binding and enforced via local government agencies. These parameters are intended to be revisited annually to reflect changes in the pace of adoption and or applications of Blockchain technologies—impacting both public and private sectors. These parameters are thus empathic, based on principles of protecting human rights, freedoms and preferences to control an individual's personal information and its access and data repurposing.

The ethical compliance principles include but are not limited to

- **Human rights and inclusion:** Digital identity systems should respect and promote human rights, including the right to privacy, the right to non-discrimination, and the right to access essential services.
- **Proportionality and necessity:** Digital identity systems should be proportionate to the risks they intend to address and not be used unnecessarily or excessively.
- **Transparency and accountability:** Digital identity systems should be transparent and accountable to the public. This means that people should be able to understand how their data is being collected, used, and shared and that there should be mechanisms to hold those who control digital identity systems accountable for their actions.
- **Human-centered design:** Digital identity systems should be designed with the user in mind. This means that they should be easy to use and understand and meet the needs of all users, including those with disabilities.
- **Multi-stakeholder participation:** The development and use of digital identity systems should involve various stakeholders, including governments, businesses, civil society organizations, and individuals. This will help ensure that the systems are designed and used fairly, inclusively, and beneficial.

GOVERNANCE AND POLICY

There is significant variability in the pace of governance and compliance standards adoption by regions of the world related to digital identification. The European Union's General Data Protection Regulation (GDPR) – is the most advanced in documenting requirements for the processing and sharing of personal data. Currently, in Asia and the Americas, the federal government and private consortia are collaborating to propose nationwide data security laws and mandates. The increasing occurrences of data theft and digital data privacy in healthcare are critical drivers for building regulatory frameworks and enforcement mechanisms to deal with data security, data governance and incidents of data breaches.

Governance and policies in the future must manage across several gaps:

1. development of a consent ontology model;
2. development of a methodology for monitoring fairness on the blockchain;
3. resolution of the contradiction between auditing and obfuscation;
4. development of a methodology for tracking controllers in the blockchain; and
5. integration of the different-purposed technical solutions without conflicts.

With a few emerging deployments of digital identities using blockchain technology to create data anchoring, it is necessary to know the status of data protection approaches when blockchain is involved. Standards Development Organizations (SDOs) such as the ISO have published documents on this topic. However, there are a limited number of references related to various compliance requirements of the blockchain (ISO/TR23244:2020 provides a set of cursory guidelines for personal data protection applied to the blockchain). Since digital identities come with privacy and security risks – what adds complexity is the fact that compliance requirements will need to be auditable—taking into consideration individual rights to control the sharing of personal information.

In governance and policy-making, the two additional essential elements are

- **Regulating Verifier Collusion:** Regulators might require access to blockchain source code(s) to build data monitoring to analyze transactions and price trends to detect tacit collusion. This practice, while well-intentioned, also creates ethical concerns about what aspects of the transactions are private matters. Moreover, if this information falls into criminal hands, it could be misused for unethical purposes, including black mail or other personal reputational damage.

  Further, the unique digital identity verifier (signature) cryptographic encryption methods are not standard and require enforcement against fundamental privacy rights violations, secrecy of communications, and unauthorized or illegal use of personal information.

- **Data Broker Industry:** Data brokers or information brokers collect data and create profiles of individuals which may introduce discrimination risk and lead to harassment involving unsolicited contact based one's profile characteristics or personas. Compiling, aggregating, and selling data for marketing and other practices raises clear ethical concerns for privacy and discrimination based on race, age, and other data characteristics which may be accurate or inaccurate.

Automated Governance

Automated governance of digital identities (human or machine) relates to access and approvals rights and detection of permission discrepancies, including passwords - using business process workflows that are decentralized to manage and secure data with minimal error.

Automated governance must also protect human rights, ensuring consent, access, participation, dignity, and respect. Identity Governance and Administration (IGA) systems automate the provisioning, management, and administration of user identities and password rights today.

There is no standardized or verified national or international system for digital identity authentication and authorization compliance. There are, however, guidelines for industry best practices and innovation for surveilling user activities.

There are ethical implications today, which can lead to 1) deepening societal inequities, 2) jeopardizing data security, and 3) eroding privacy through new avenues of surveillance.

Currently, Identity Governance Access (IGA) frameworks and tools help somewhat with the management of the lifecycle of digital identities, as software platforms that control data access within an IT environment). These solutions help monitor compliance requirements and security objectives, but with minimal monetary fines and reprimands. This is a critical area for policy development and education that balances cyber threats and human privacy.

The Chartered Society of Forensic Sciences

The Chartered Society of Forensic Sciences, based in the UK, is the only international professional organization focused on global standards for blockchain data movement.

Blockchain forensics uses data analysis to monitor potential criminal activity on a blockchain – the ethical implication is whether this private data, often associated with crypto transactions, for example, can be exploited. Specifically, the metadata and smart contracts are accessible to internet service providers and law enforcement agents.

There is accelerated innovation related to new forensic software on computers, personal digital assistants (PDAs), and mobile devices. There is an increased demand for ethical standards provisions.

In both the UK and the US, Chartered Forensic Scientists focus on digital forensics to analyze forgery and data manipulation on blockchains. Although no consistent or standard regulations exist today, federal governments use existing statutes for compliance and ethics.

A note on risk management

Like any other technology infrastructure, digital identity systems are also subject to attacks. Hence, the design, development and deployment of such systems should include a systematic way to identify risks and design policies and technical requirements to mitigate such risks. While standard risk management approaches and models are well understood, domain-specific recommendations are also available to enable auditors to provide better inputs to such systems.

Provided below are some recommendations and observations related to the management of digital identity systems, surface areas of attacks and handling data governance to prevent the risk of data breaches. The last topic is almost always covered by data governance regulations available at the jurisdictional level.

US/GAO Key Audit Recommendations on Digital Identity

- Develop a comprehensive strategy for digital identity management. This strategy should include a clear vision of how digital identity will be used across governments and specific goals and objectives. It should also identify the roles and responsibilities of different agencies and stakeholders.
- Implement strong authentication and access control measures. This includes using multi-factor authentication, requiring users to provide passwords and codes from their phones to access sensitive systems and data.
- Protect personal identifiable information (PII). This includes encrypting PII when it is stored or transmitted and limiting access to PII to authorized personnel.
- Educate users about digital identity risks and best practices. This includes teaching users how to create strong passwords, spot phishing emails, and report security incidents.
- Monitor and evaluate the effectiveness of digital identity security measures. This includes conducting regular security assessments to identify and address vulnerabilities.
- With particular regard to the use of biometrics, the GAO has raised concerns about the security of biometrics because data can be spoofed or stolen and used to impersonate someone else. Accordingly, the GAO recommended US Agencies carefully consider biometrics' risks and benefits before implementing them for digital identity verification. In particular, the GAO recommended that US Agencies implement strong identity-proofing processes to verify the identity of individuals seeking access to government systems and data. These processes should include multiple authentication factors, such as passwords, security questions, and biometrics.

The Institute of Internal Auditors (IIA)

The Institute of Internal Auditors (IIA)[21] is an international professional association that provides guidance, education, and resources to internal auditors. The IIA guides digital identity in its Auditing Identity and Access Management Global Technology Audit Guide (GTAG).[22] The GTAG defines identity management (IDM) as "the set of processes and technologies used to establish and maintain the identities of individuals and systems and to control access to information and systems."

The GTAG identifies three key objectives of IDM:

- **Identity proofing:** The process of verifying the identity of an individual or system.
- **Authentication:** The process of verifying that an individual or system is who it claims to be.
- **Access control:** The process of granting or denying access to information or systems based on identity and authentication.

The GTAG recommends that internal auditors review the organization along the following aspects:

- Risk appetite for identity-related risks.
- IDM policies and procedures.
- IDM controls.
- IDM training and awareness programs.
- IDM incident response plan.
- Identity proofing processes to ensure that they are effective in verifying the identity of individuals and systems.
- Authentication processes to ensure that they are effective in verifying that individuals and systems are who they claim to be.

Information Systems Audit and Control Association (ISACA)

The Information Systems Audit and Control Association (ISACA) is an international professional association focused on information technology, assurance, security, and governance.

The ISACA *"Audit Program on Identity and Access Management"*[23] guides how to assess the effectiveness and efficiency of IAM processes and controls, identify gaps and weaknesses, and provide recommendations for improvement.

"The Importance of a National Digital Identity System" states that the creation of a national digital identity system (NIDS) would provide a centralized repository of identity information that can be used to verify the identity of individuals and organizations and improve the security and efficiency in a variety of ways, such as by reducing fraud, streamlining government services, and making it easier to do business online. However, there are several challenges to implementing an NIDS, such as ensuring the security of the system and protecting privacy.

"The state of digital trust 2023", an ISACA global research report, identified the following best practices:

- **Several factors can erode digital trust.** These include data breaches, security incidents, and privacy concerns.
- **Organizations can build digital trust by taking several steps.** These include implementing strong security measures, protecting privacy, and being transparent about their data practices.
- **There is a growing need for international cooperation on digital trust.** As the world becomes increasingly interconnected, having common standards and practices for digital trust is important.

CENTRALIZED VS. DECENTRALIZED MODELS

While centralized digital identity models still retain a centralized repository of data, decentralized models focus on users' control of their own data. Interoperability in either case should be a prerequisite ensures equal access to platforms and services, so as to minimize inequalities.

Digital identity models that utilize blockchain technology can verify data records transparently and immutably, and deploy security enhancing tools such as zero-knowledge proofs and hashing to make data anonymous, pseudonymous, and conditionally available only to authorized parties upon request. These tools embed privacy considerations around selective disclosure and requirements. Maintaining individual control over personal data can be a major step toward preventing breaches and their harmful consequences. The following considerations should be taken into account for each model:

- **Biometric Data:** Biometric data includes unique physical or behavioral characteristics of an individual, such as fingerprints, facial features, iris scans, voice patterns, and even behavioral traits like typing patterns or gait. Biometrics provide a highly secure and difficult-to-forge method of verifying identity.

- **Personal Information:** This includes basic personal details such as name, date of birth, gender, and contact information. These attributes are commonly used for identification and verification purposes.

- **Authentication Credentials:** Authentication credentials are the means by which individuals prove their identity when accessing digital services. This includes passwords, PINs, security questions, and more advanced methods like one-time passwords (OTP), security tokens, or biometric authentication.

- **Consent Management:** Consent management involves obtaining explicit permission from individuals to access their personal data and use it for specific purposes. It's a crucial component for ensuring data privacy and compliance with regulations like GDPR.

- **Blockchain and Distributed Ledger Technology:** Blockchain can be used to securely manage and verify digital identities. It provides a tamper-proof and decentralized way to store identity-related information, enhancing security and transparency.

- **Multi-Factor Authentication (MFA):** MFA combines multiple authentication methods to increase the security of access to digital services. This might involve something the user knows (password), something the user has (a physical token), and something the user is (biometric data).

- **Single Sign-On (SSO):** SSO allows users to access multiple services using a single set of login credentials. It improves user experience and reduces the need to remember multiple passwords.

- **Identity Providers (IdPs):** Identity providers are entities that manage and verify digital identities. They play a key role in authentication and authorization processes, often using standards like OAuth and OpenID Connect.

- **Privacy Controls:** Privacy controls enable individuals to manage the sharing and exposure of their personal information. This ensures that users have control over who can access their data and under what circumstances.

USE CASES

Private and public sector implementations of digital identity can greatly improve access to services, and thus improve levels of equality and well-being for all citizens.

ACCESS TO BANKING/FINANCE

Identity verification is one of the most critical components of banking and impacts most areas of banking including account opening, KYC, credit card applications, loan originations, high-risk transactions, account closures access to services, and various other banking products. The current state of identity verification methods is ad hoc and inconsistent in most cases, resulting in friction for customer experiences and reconciliation efforts for bank employees.

Digital identity, on the other hand, enables secure and frictionless customer experiences while integrating various lines of businesses cohesively into using a single source of verification for KYC. Digital identity has several use cases in banking, including:

- **Digital identity services:** Digital identity services can help banks improve risk management through streamlined know-your-customer (KYC) processes, better fraud management, and improved protection of customer data against cyber threats. It simplifies how individuals interact with new banking products and helps banks reap tangible results such as cost reduction, better risk governance, customer profiling, paperwork reduction, and improved data management.
- **KYC automation:** Businesses often need to verify the identity of customers during onboarding or registration processes. Verified digital identity solutions streamline this process by automating identity verification, reducing manual work, and improving compliance with KYC regulations. Digital identity can allow banks to authorize identities and verify transactions in real time while streamlining the necessary customer due diligence procedures by using open banking to fetch and verify customer information. This use case is critical for smaller financial institutions that typically have limited resources for compliance operations.
- **Transaction monitoring:** Transaction monitoring is a requirement that lets payment service providers (PSPs) detect unauthorized or fraudulent transactions by looking for anomalies in the data.
- **Financial management (FM) services:** Using open banking to aggregate financial information from different accounts and banks can simplify money management for consumers and businesses. FM services ranked high in Italy, Norway, the UK, and Spain – countries characterized by significant competition for the digital customer experience.
- **Financial Inclusion and Access to Banking Services:** Extending access to banking and financial services to underserved and unbanked populations by enabling them to establish a digital identity. Providing a foundation for individuals without traditional identification documents to participate in the formal financial system and access loans, savings accounts, and other financial products.
- **Fraud Prevention and Security:** Verified digital identity helps prevent identity theft, account takeovers, and fraudulent transactions. By verifying a user's identity through multi-factor authentication, biometrics, or other means, businesses can ensure that only authorized users gain access to sensitive information or perform critical actions. Verified digital identities can also improve the security of online banking, mobile payments, and online trading platforms. This reduces the risk of fraudulent activities and unauthorized access to financial accounts.

Digital identity can significantly improve efficiency in the private financial services industry in several ways. Private sector companies such as Visa, PayPal, and Mastercard are exploring various use cases as digital identity solutions could play a crucial role in enhancing security, convenience, and efficiency. Here are four use cases specifically relevant to private-sector companies:

Enhanced Cardholder Verification and Authentication

Visa, Mastercard, and other payment card companies can leverage digital identity to enhance cardholder verification methods. This includes using biometrics such as fingerprint or facial recognition to authenticate transactions, making payments more secure and convenient. Digital identity helps reduce instances of card fraud, as biometric data linked to a cardholder's account ensures that only authorized users can make transactions, protecting both the consumer and the financial institution.

Tokenization for Secure Online and Mobile Payments

Visa and Mastercard have introduced tokenization services that replace sensitive card information (e.g., card numbers) with unique tokens for online and mobile payments. Digital identity securely links these tokens to the cardholder, ensuring that only the legitimate cardholder can use these tokens for transactions. This protects against card-not-present fraud and enhances payment security in the digital realm.

Personalized User Experiences and Loyalty Programs

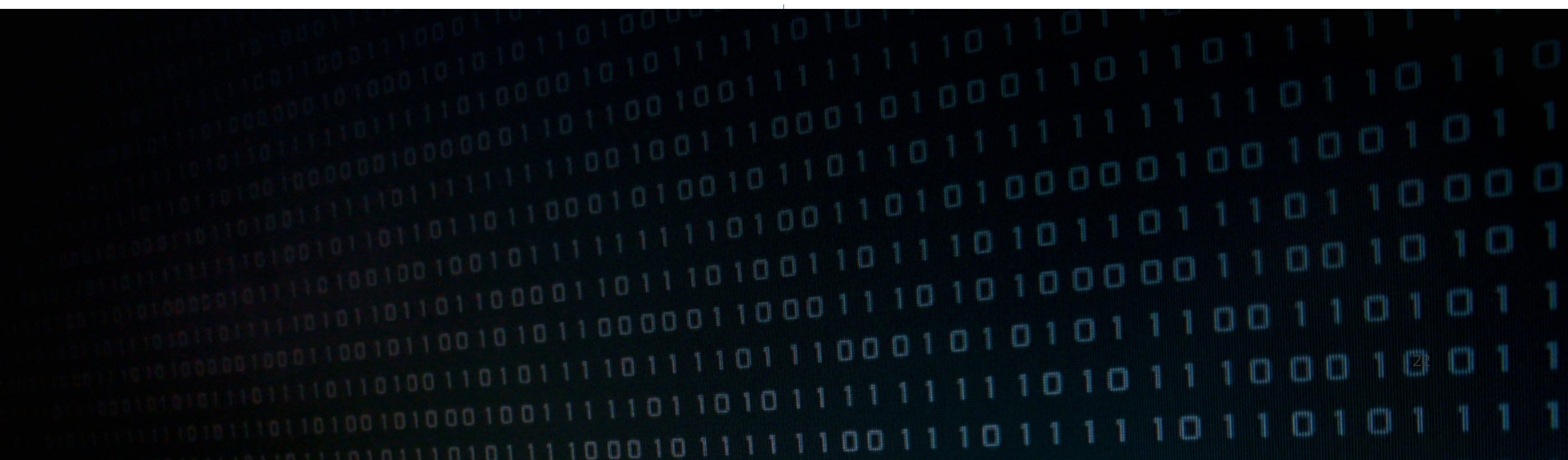
Digital identity data allows companies like Visa and Mastercard to gain insights into cardholders' spending behaviours and preferences. By analyzing this data, these companies can offer cardholders personalized promotions, discounts, and loyalty programs, enhancing their overall customer experience and incentivizing card usage.

Secure Mobile Payments and Digital Wallets

Facilitating secure and convenient mobile payments by enabling users to link their digital identity to their mobile devices. Enhancing the security of digital wallets and mobile payment apps through biometric authentication methods like fingerprint or facial recognition. One such use case is using a consumer's digital identity as a key for payment execution. This has already eroded the value of plastic cards by enabling the use of a consumer's digital identity as a key for payment execution. Another use case is the use of virtual cards, such as PayPal Key, which hides the real details associated with your payment account, providing an extra layer of protection against fraud and identity theft while you shop.

E-commerce

Online retailers can enhance user trust by implementing verified digital identity for customer accounts and transactions. This can help prevent fraud, reduce chargebacks, and provide a seamless shopping experience.



OTHER BASIC SERVICES

- **Healthcare and Telemedicine:** Verified digital identities can be used to securely access electronic health records, telemedicine services, and other healthcare-related platforms. This ensures that only authorized individuals, such as patients and healthcare providers, can access sensitive medical information.
- **Government Services:** Verified digital identities can simplify interactions with government agencies and services. Citizens can securely access and submit documents, apply for permits, pay taxes, and access public services online.
- **Travel and Hospitality:** Verified digital identities can expedite airport security processes, hotel check-ins, and car rentals. Travelers can use their digital identity to authenticate themselves and access various services quickly.
- **Education and e-Learning:** Online learning platforms can use verified digital identities to ensure the authenticity of students, prevent cheating, and protect intellectual property. This is especially important for online certification and degree programs.
- **Cybersecurity and Access Management:** Enterprises can enhance their cybersecurity posture by implementing verified digital identities for employee access to corporate networks, systems, and sensitive data. This reduces the risk of unauthorized access and data breaches.
- **Supply Chain and Logistics:** Verified digital identities can improve supply chain transparency and security by ensuring that authorized personnel access sensitive information and make critical supply chain decisions.
- **Digital Voting and Civic Engagement:** Verified digital identities can enable secure online voting and civic participation, making it easier for citizens to engage in the democratic process while preventing voter fraud.
- **Gig Economy and Peer-to-Peer Services:** Platforms in the gig economy can use verified digital identities to establish trust between service providers and customers, ensuring a safe and secure environment for transactions.

In summary, digital identity solutions are changing how financial institutions verify their consumers' identities, providing various advantages, including higher security, efficiency, and a better client experience. From adopting blockchain technology to using digital identity for inclusive growth and the evolution of business models, companies are finding new and innovative ways to leverage this technology to improve their customers' security, convenience, and efficiency.

RECOMMENDATIONS

While the scope and focus of this paper is not designed to put forward wide-ranging recommendations on digital identities, governance frameworks, and digital trust ecosystems, there are opportunities to enumerate specific recommendations because more jurisdictions are finding it necessary to implement a form of digital governance by introducing digital identities, linking services, and enabling an "update once" approach to data modification and exchange. If the ease and convenience of access to services are built around digital IDs, then it is necessary that the lifecycle of such identifiers can provide all the promised benefits.

Robust and sustainable digital trust ecosystems require high-quality digital IDs. In addition, technology designs, information technology architectures, and network protocols are some of the ways in which these governance requirements are translated into implementation details . It is also important to consider that technological innovations provide an acceptable compromise between what is possible and what is required by the regulations and laws. Digital IDs also function in cross-border transactions, thus bringing in more complexities and challenges among the various jurisdictions.

Below is a summary of the recommendations for governance authorities, system designers, implementors and operators of digital ecosystems, which include digital identities. These recommendations are not binding but provide guidelines to adopt and include in digital trust ecosystems.

- Design human-centric digital IDs aligned with the Principles of Digital ID
- Enable transparency to make systems explainable to the consumers
- Anticipate and design policies to mitigate the risks from harms
- Advocate for regulatory environments which provide protections from erosion of principles

An additional recommendation is to examine, evaluate and assess the emerging innovations in technology such as Generative AI, Large Language Models (LLMs), Synthetic Content Creation flows - all of which are capable of eroding the level of assurance of digital identities. The threats inherent in these technologies need to be thoroughly evaluated, and safeguards built into digital identity systems to prevent bypassing any existing protection mechanisms and guardrails.

Digital identities should be useful, fit for purpose, inclusive and secure . These are not new or novel requirements but must be in place to prevent the exploitation of data enabled by certain forms of digital identity. It is also necessary to be cognizant of the fact that popular messaging applications also enable the creation of portable digital identities, often bound to a combination of mobile phone numbers and mobile hardware. While such inexpensive and portable digital identities facilitate communication between individuals, there has not been extensive research on the security of the platforms enabling the creation of such digital identities, or the secure management of the same. It can be noted that individuals' activities using these platforms leave "breadcrumbs", or activity trackers, such that their personal information may not remain as private as expected or desired. Such digital identities, if found to be weak or weakly managed, can lead to data breaches, exploitation, and other harms.

CONCLUSION

A growing number of digital identifiers are issued, exchanged, and managed, with the intention of enabling better access to services for consumers. While digital identifier systems have the potential to impact consumers positively, there have been ongoing discussions about the possibility of harm originating from poorly designed systems. The worldwide standards for digital identity have a direct impact on the protection of human rights. This makes it uniquely significant that all the stakeholders focus on the necessary components of a digital identifier system to have a long-term impact. The growing number of secure, interoperable systems can unlock services such as financial inclusion, access to healthcare, and inclusion in other services. While the compliance requirements will evolve, it is necessary to be mindful of the pace of innovation and shifts in markets alongside changes in geopolitics. Bias or unfairness in the design criteria of digital identity and using and categorising personas can be inequitable - profiling or targeting people in discriminatory ways.

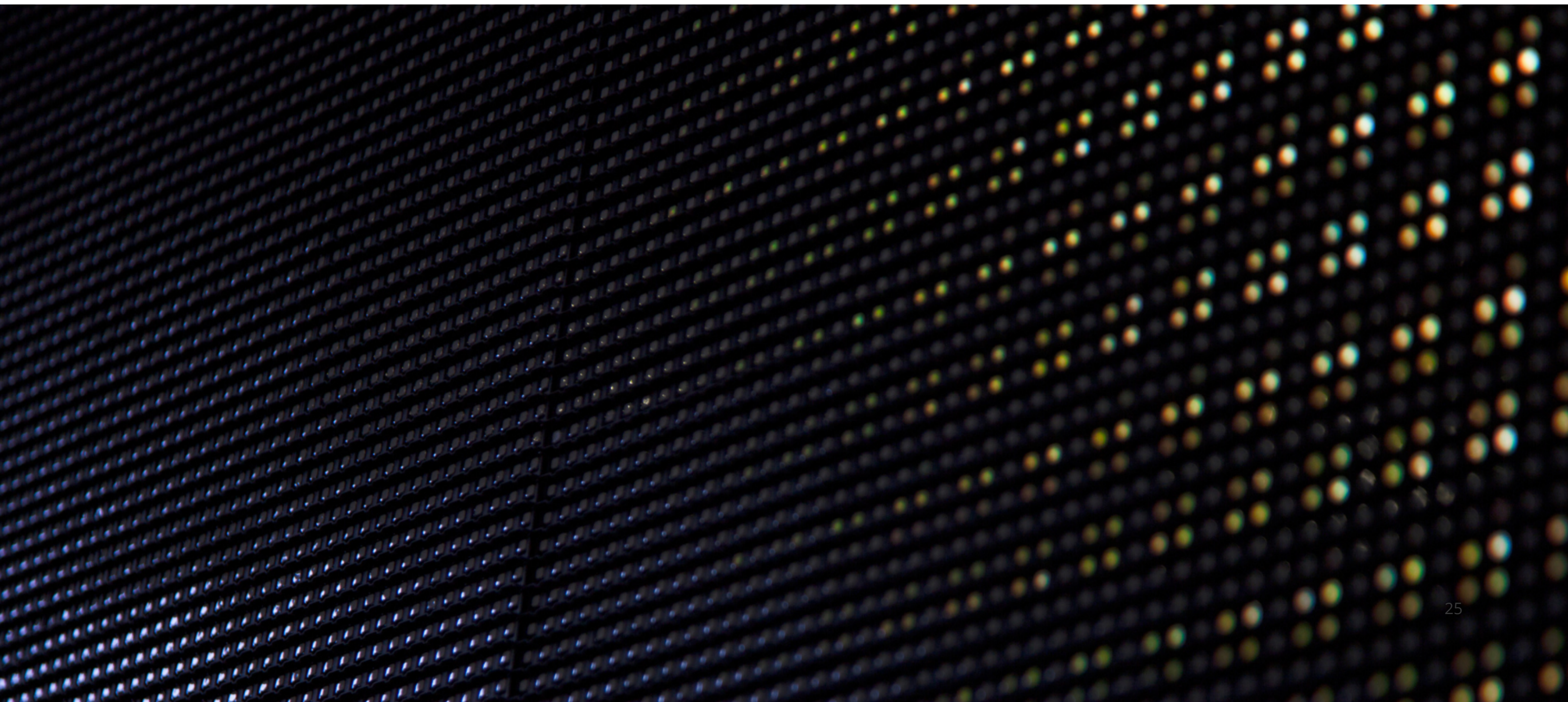
Whether intentional or not, such systemic bias has implications that may be difficult to identify, correct or equalize quickly or without debate once agreed upon.

Innovations in technology are essential to ensuring that the digital IDs being put into circulation align with the principles highlighted in this paper. The idea that digital IDs will be able to protect privacy, enable agency, and promote inclusion must be upheld and protected from being misused through poor design choices. The topic of privacy is enormous and an emerging field - and like the governance frameworks, regulations and technology enabling privacy, it is impossible to acquire a deep understanding of the topic. All the stakeholders in a digital trust ecosystem, including digital IDs, have the responsibility to examine the innovation, research and development to create guardrails against the possible misuse and abuse of the technology infrastructure powering digital IDs.

The standards-making work is necessary to create robust systems that ensure interoperability, scalability, compliance, and human-centricity. This is complemented by ethical compliance requirements built around principles and values which take into consideration the uniqueness of culture, such as language and social norms. Today, large digital identifier systems are being deployed as "Digital Public Infrastructure" (DPI), thus enabling more deployments to develop a shorter development cycle. These deployed systems should focus on consistent user experience, improved digital ecosystem governance frameworks, and sound approaches to managing personal data aligned with both legal requirements and security best practices.

International cooperation and harmonization are key. The long-term impact and consequences of digital identity systems should be carefully considered. Changes in technology, policies, and societal norms can affect how digital identities are used and interpreted over time. As for cultural sensitivity, digital identity systems should also respect cultural differences and avoid imposing a single standardized identity framework that might not resonate with all individuals, for the sake of preventing disparities and biased access to services. As for the role of government and corporate entities in managing or safeguarding digital identities in any form, the centralization of digital identity data can lead to concentrated power in the hands of governments and corporations. Ensuring checks and balances are in place to prevent abuse of this power is crucial.

Effective and secure digital infrastructures are key to moving beyond fragmented digital solutions toward broader digitization and accelerate the growth of a digital economy in a way that fosters inclusive social and economic development. As global initiatives continue to work toward access to digital identity for all, in support of the SDGs, individual governance and empowerment are at the center. While individuals can have multiple identifiers, it is the individuals themselves who matter. Safeguarding individuals' wellbeing through universal access to a digital identity that is effective and secure can greatly advance social and economic inclusion, for better outcomes.



ADDITIONAL READING

1. Blockchain for Digital Identity and Credentials | IBM. (n.d.). Retrieved September 23, 2023, from https://www.ibm.com/blockchain-identity
2. Tuchen, M. (n.d.). Council Post: How Digital Identity Can 'Amazonify' The Financial Services Industry. Forbes. Retrieved September 23, 2023, from https://www.forbes.com/sites/forbestechcouncil/2022/08/05/how-digital-identity-can-amazonify-the-financial-services-industry/
3. Importance of Digital Identity in US Banking Revolution. (2022, April 1). DIRO Original Document Verification Technology. https://diro.io/us-digital-banking-revolution-importance-of-digital-identity/
4. The top 5 open banking use cases for European bankers. (n.d.). Retrieved September 23, 2023, from https://tink.com/blog/open-banking/top-uses-cases-survey-report/
5. RISK ANALYTICS FOR FRAUD PREVENTION: TOP USE CASES IN BANKING, https://www.onespan.com/sites/default/files/2020-10/OneSpan-WhitePaper-A4-Risk-Analytics-Fraud-Prevention_20200930_1.pdf
6. UN Roadmap for Digital Cooperation (June 2020) https://www.un.org/en/content/digital-cooperation-roadmap/assets/pdf/Roadmap_for_Digital_Cooperation_EN.pdf (last accessed on Nov 7, 2023)
7. The Principles of SSI v3 published by the Sovrin Foundation https://sovrin.org/principles-of-ssi/ (last accessed on Nov 7, 2023)
8. Towards Better Ends by John Phillips on behalf of Sezoo https://www.sezoo.digital/resources/towards-better-ends/ (last accessed on Nov 7, 2023)
9. Digital Wallet Design for Guardianship by John Phillips on behalf of Sezoo https://www.sezoo.digital/resources/digital-wallet-design-for-guardianship/ (last accessed on Nov 7, 2023)
10. Digital ID At Last by David Birch https://www.linkedin.com/pulse/digital-identity-last-its-from-banks-david-birch-w9wbe/ (last accessed on Nov 7, 2023)
11. Principles of Dynamic Data Economy (DDE) v1.0 https://static1.squarespace.com/static/5ead4c8660689c348c80958e/t/62f288b25f9c364d7945e6eb/1660061875006/HCF+DDE+Principles+v1.0.0.pdf (last accessed on Nov 7, 2023)
12. The Domains of Identity: A Framework for Understanding Identity Systems in Contemporary Society by Kaliya Young
13. Standards-Based Digital Credentials: Flavors Explained: An Independent Review and Analysis https://consulting.identitywoman.net/standards-based-digital-credentials-flavors-explained (last accessed on Nov 7, 2023)

ENDNOTES

DIGITAL IDENTITY

[1] https://sovrin.org/principles-of-ssi/

[2] Garber, E. and Haine, M. (eds) "Human-Centric Digital Identity: for Government Officials

[3] OpenID Foundation, (September 25, 2023). https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0188

[4] https://id4d.worldbank.org/guide/identity-lifecycle

[5] https://docs.kantarainitiative.org/Blinding-Identity-Taxonomy-Report-Version-1.0.html

[6] https://pages.nist.gov/800-63-4/

[7] https://humancolossus.foundation/s/HCF-Overlays-Capture-Architecture-OCA-v1.pdf

[8] https://www.w3.org/TR/vc-data-model/

[9] https://www.iso.org/about-us.html

[10] https://www.w3.org/about/

[11] https://www.ietf.org/about/introduction/

[12] https://openid.net/

[13] https://trustoverip.org/about/about/

[14] https://identity.foundation/

[15] https://openwallet.foundation/

[16] https://mydata.org/about/

[17] https://kantarainitiative.org/about/

[18] https://humancolossus.foundation/

[19] https://essif-lab.github.io/framework/docs/essifLab

[20] https://www.un.org/en/content/digital-cooperation-roadmap/assets/pdf/Roadmap_for_Digital_Cooperation_EN.pdf

[21] https://www.theiia.org/en

[22] https://iia.no/wp-content/uploads/2021/08/2021-Auditing-Identity-and-Access-Management.pdf

[23] https://www.isaca.org/resources/audit-programs/identity-and-access-management-audit-program

[24] https://www.stockholmresilience.org/research/planetary-boundaries.html

[25] https://www.theguardian.com/environment/2022/aug/29/major-sea-level-rise-caused-by-melting-of-greenland-ice-cap-is-now-inevitable-27cm-climate

GLOBAL BLOCKCHAIN BUSINESS COUNCIL

DC Location:
1629 K St. NW, Suite 300
Washington, DC 20006

Geneva Location:
Rue de Lyon 42B
1203 Geneva
Switzerland