SECTION V

# DIGITAL ID

## EXECUTIVE SUMMARY

The rapid deployment of global decentralized networks has created large gaps with respect to data disclosure, financial transactions, and the degree of privacy to which individuals are entitled regarding digital assets. Digital assets come in many forms, but the Covid pandemic and rapid development of Web 3.0 decentralized networks has incited a need for a foundational, global, interoperable framework for modern digital identity. Personal data also carries value, which can be protected and exchanged on decentralized ledger technologies (DLT) with the individual in control. Beyond that goal, decentralized exchanges (which are often autonomous with no central governing body,) in combination with non-custodial wallets, provide a major hurdle for regulatory and enforcement agencies to use existing KYC/AML frameworks to prevent illicit activity.

Decentralized identity solutions, sometimes synonymously referred to as “self-sovereign identity” (SSI) frameworks, have been recommended for many use cases and align well with the UN’s sustainable development goals (SDGs), especially SDG 16, and can serve as a foundation for Web 3.0 and beyond. Applications include globally interoperable frameworks for government, healthcare, finance, and physical interactions. In combination with biometrics, digital asset wallets, and other technologies, SSI may serve as a foundation to enhance KYC/AML integrity while affording financial access to underserved populations. It can help remedy archaic administrative costs in different verticals like healthcare and financial services. A decentralized approach to identity can also offer the least fortunate among us some form of documentation by which one can verify another for issuance of first aid, food, water, and other essentials in times of crisis. As reports suggest, over a billion people lack proper identification.[120]

Access the full version of the Digital ID report here.

| | |
|---|---|
| Government Issued/ attested primary credentials and identifiers | National IDs like SSN, Passport, Driver’s License, Standard ID, Real ID, birth certificates |
| Attestation | Acknowledged evidence or confirmation of the existence of something, whether by an individual or organization.The broader community must prioritize finding greater consensus on common definitions and taxonomy. |
| Credential | A qualification, trait, achievement, or authority assigned to a person or entity which can be issued in physical or digital form.The broader community must prioritize finding greater consensus on common definitions and taxonomy. |

**Digital Identity**

Identity issued by an organization that is considered to be either "Siloed" or "Federated."[121]

**Federated Identity**

Means of linking a person's electronic identity and attributes, stored across multiple distinct identity management systems.[122] Federated identity is related to single sign-on (SSO), in which a user's single authentication ticket, or token, is trusted across multiple IT systems or organizations. SSO is a subset of federated identity management, as it relates only to authentication and is understood on the level of technical interoperability and would be impossible without some sort of federation.

**Decentralized Identifier (DID)**

A globally unique identifier developed specifically for decentralized systems as defined by the W3C DID specification. DIDs enable interoperable decentralized Self-Sovereign Identity management: A DID is associated with exactly one DID Document.[123]

**Decentralized Identity**

A portable set of identity credentials (which may be issued or attested to by third parties) controlled by the individual owner in a digital wallet underpinned by a DLT platform.[124]

**Self-Sovereign Identity**

An identity system architecture based on the core principle that identity owners have the right to permanently control one or more identifiers together with the usage of the associated identity data.[125]

**Verifiable Credential**

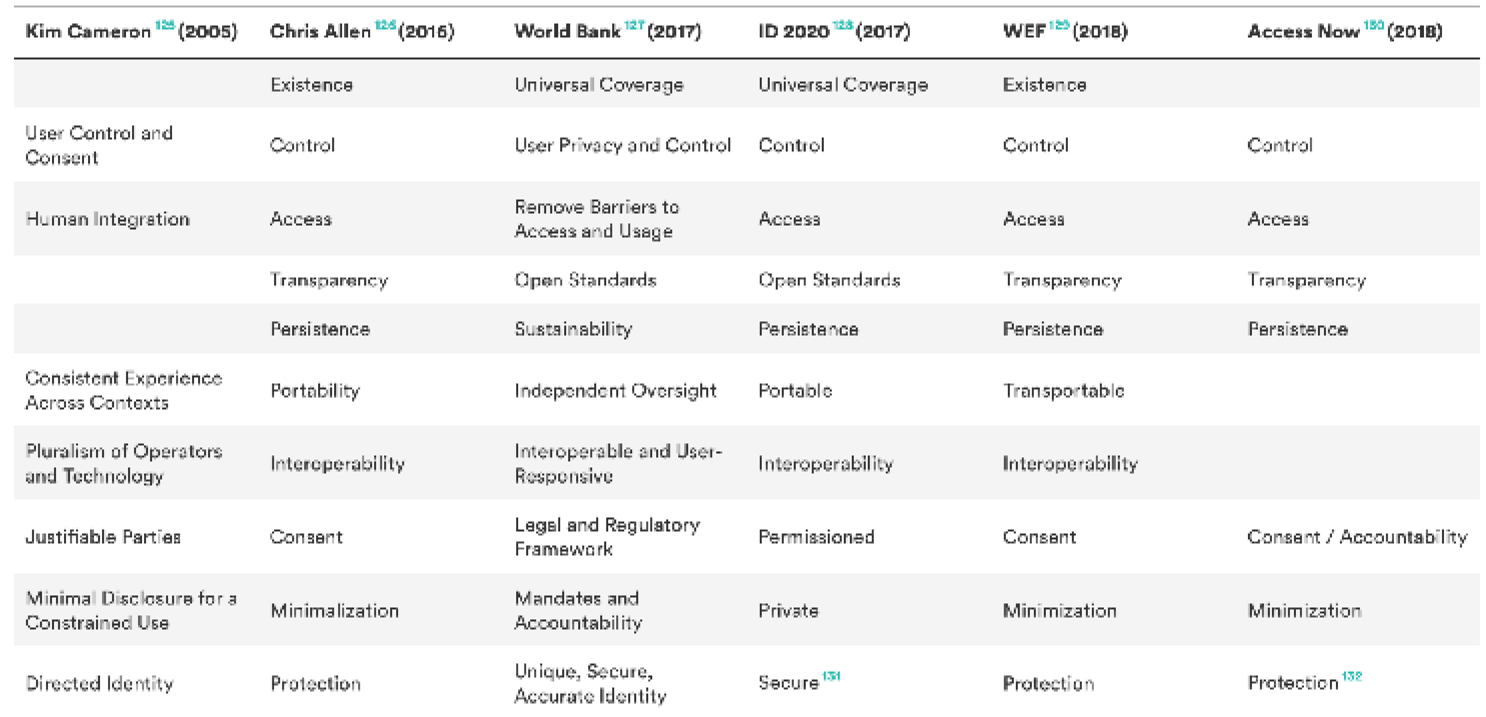
Much existing regulation and standardization focuses specifically on digital assets, as opposed to blockchain or DLT technology more broadly. As new uses for the technology continue to emerge, dynamic or principles-based guidance will be better suited to adapt. Regulators should take advantage of regulatory sandboxes and innovation hubs to create more effective regulations.

**Zero-Knowledge Proof**

A Proof that uses special cryptography and a Link Secret to support Selective Disclosure of information about a set of Claims from a set of Credentials. A Zero Knowledge Proof provides cryptographic proof about some or all of the data in a set of Credentials without revealing the actual data or any additional information, including the Identity of the Prover.

## SSI Principles Elaboration

Table 3: Various "Principles of Identity"



| Kim Cameron [125] (2005) | Chris Allen [126] (2016) | World Bank [127] (2017) | ID 2020 [128] (2017) | WEF [129] (2018) | Access Now [130] (2018) |
|---|---|---|---|---|---|
| | Existence | Universal Coverage | Universal Coverage | Existence | |
| User Control and Consent | Control | User Privacy and Control | Control | Control | Control |
| Human Integration | Access | Remove Barriers to Access and Usage | Access | Access | Access |
| | Transparency | Open Standards | Open Standards | Transparency | Transparency |
| | Persistence | Sustainability | Persistence | Persistence | Persistence |
| Consistent Experience Across Contexts | Portability | Independent Oversight | Portable | Transportable | |
| Pluralism of Operators and Technology | Interoperability | Interoperable and User-Responsive | Interoperability | Interoperability | |
| Justifiable Parties | Consent | Legal and Regulatory Framework | Permissioned | Consent | Consent / Accountability |
| Minimal Disclosure for a Constrained Use | Minimalization | Mandates and Accountability | Private | Minimization | Minimization |
| Directed Identity | Protection | Unique, Secure, Accurate Identity | Secure [131] | Protection | Protection [132] |

Table 3 courtesy of New America. View the original here.

In an increasingly complex global internet and financial system, black swan events can pose greater economic risk. The right to owner-centric control becomes a prerequisite to digital identity and its corollaries constitute basic human rights. To ensure personal identity and related data are protected, the individual should have the option to take complete ownership and custody of her data. Shifting trust to the edges of communication networks also has the potential to reduce complexity and increase security.

## PRINCIPLES AND SOLUTIONS

- Privacy
- Inclusion
- Security
- Global Interoperability and Economic Efficiencies
- Decentralization
- User Focus

## PRIVACY

Under a digital ID solution, entities should control the privacy of their information, including minimal, selective, and progressive disclosure of attributes or other data. The sheer volume of data and value in aggregate makes centralized systems much less resilient. Affording control to the user enhances privacy, which becomes especially valuable in the healthcare and financial services verticals.

## INCLUSION

Inclusion for all is the first step toward a brighter shared future. SSI technologies and principles align congruently with the Sustainable Development Goals in their unique purpose to provide irrevocable agency of an individual's identity to any human on Earth, regardless of place of birth, bank account, or social status.

## SECURITY

Cybersecurity infrastructure is an absolute prerequisite for the safe creation, issuance, storage, and transfer of all digital data for purposes of commerce or verification. Those credentials or claim sets relatable to an individual person typically carry value and are broadly disseminated and traded. Unfortunately, and ubiquitously, global data breaches have become the norm, putting identity fraud and identity-related crimes at the forefront of international economic and social threats. The need for privacy-protecting infrastructure embedded in global data transfer networks grows every second.[126]

## GLOBAL INTEROPERABILITY AND ECONOMIC EFFICIENCIES

Increasing globalization calls for frictionless trade of physical and economic resources, cross-border transactions, and valued data exchange. Thus, sound digital identity infrastructure and governance should be integrated with Web 3.0 architecture.

## DECENTRALIZATION

Decentralization can create new economic models that incentivize "good" behavior; DLT infrastructure base layers allow for security, decentralized custody, peer-to-peer transactions, a programmable spectrum of privacy, and automation of modern financial and identity data transactions.

## USER FOCUS

Personal data is currently monetized in commercial settings as well as through social media and advertising channels. Because of the ever-present tension between hacking and cybersecurity, individual ownership of identity in a decentralized framework may allow for the greatest security of our personal data. Those preparing for Web 3.0 and decentralized technology should consider a transparent and viable governance framework capable of achieving the virtues invoked by Self-Sovereign Identity principles.

# VERTICAL FOCUS #1: HEALTHCARE & TRAVEL APPLICATIONS

## CURRENT STATE OF PRACTICAL DID APPLICATION FOR CROSS-BORDER TRAVEL AND "COVID HEALTH PASSES"

- **The Commons Project Foundation and the World Economic Forum** have launched the Common Trust Network in collaboration with a broad voluntary network of public and private stakeholders. CommonPass is the traveler App, which will store, and display COVID-19 test results and eventually vaccination records. Five airlines are part of this initiative as well as the Airport Council International, representing 2000 airports globally.[127]

- **IATA Travel Pass** is a mobile application (available in March 2021) allowing travelers to store and manage certifications for COVID-19 tests or vaccines. The information provided through the IATA Travel Pass can be used by governments requiring testing or vaccination proofs as a condition of international travel during and after the COVID-19 pandemic. Emirates Airlines is one of the first Airlines to partner with IATA for the adoption of Travelpass.[128]

- **World Health Organization (WHO)**: Initiated the development of a digitally enhanced International Certificate of Vaccination, a 'smart yellow card'. WHO also set out the Smart Vaccination Certificate Working Group. It is intended to bring together experts to focus on defining specifications and standards for a digital vaccination certificate.[129]

- **International Chamber of Commerce (ICC)** has partnered with International SOS, to launch the new ICC AOKpass mobile app, to provide trusted recognition of individuals' COVID-19 compliance status. Singapore Airlines has trialed the AOKpass service for inbound travelers from Malaysia and Indonesia.[130]

- **Vaccine Credential Initiative (VCI)** is working to enable individuals vaccinated for COVID-19 to access their vaccination records in a secure, verifiable, and privacy-preserving way. The coalition (CARIN Alliance, Cerner, Change Healthcare, The Commons Project Foundation, Epic, Evernorth, Mayo Clinic, Microsoft, MITRE, Oracle, Safe Health, and Salesforce) is developing a standard model for organizations administering COVID-19 vaccines to make digital credentials available in an accessible and interoperable.[131]

- **Good Health Pass Collaborative** is a cross-industry group, established in 2020, in response to COVID-19 shutting down international travel, to provide guidance on travel pass creation and use. The resulting Interoperability Blueprint makes recommendations for adoption that include the early standards and specifications from Trust Over IP, DIF, and W3C.[132]

## IMPACTS ON STANDARDS & INTEROPERABILITY

Despite the number of initiatives listed above, there are no unified standards to define precisely how Digital Health Credentials mechanisms — from issuance to verification — would work. For example, the Good Health Pass Interoperability Blueprint proposes a new set of interoperability specifications while acknowledging that there is a lot of work remaining to reach true standardization and interoperability.[133] Additionally, technology firms have their own way to implement standards specifications which often limit interoperability. The (limited) list below shows standards, consortiums, and foundations that are working on various technology stack layers used in a Digital Health Credentials solution (authentication protocol, communication, encryption data storage, etc.)

- **World Wide Web Consortium (W3C)** has been working on building web standards since the early 2000s. They have primarily focused on developing the browser and have been instrumental in making browser interoperability possible. They are specifically involved in a working group to specify the architecture, data model, and representation of Decentralized identifiers (DIDs) that enable verifiable, decentralized digital identity

- **JavaScript Object Notation (JSON)** is an open standard file format, and data interchange format, that uses human-readable text to store and transmit data objects. JSON is used for passenger QR code presentation. It is important to note that though JSON is a standard, the schemas required for interoperability have not been standardized.

- **Decentralized Identity Foundation (DIF)** is an engineering-driven organization acting as a center for development, discussion, and management of all activities required to create and maintain an interoperable and open ecosystem for the decentralized identity stack. DIF has the capability to set up intellectual property rights (IPR) protected working groups, deliver specs and standards, and offer infrastructure for the community.

- **Trust over IP Foundation** is an organization hosted at the Linux Foundation that is defining a complete architecture for Internet-scale digital trust that combines both cryptographic trust at the machine layer and human trust at the business, legal, and social layers.

- **Hyperledger Foundation** is an organization hosted at the Linux Foundation which promotes collaboration from a variety of industry stakeholders building implementations in open-source communities for a variety of use cases around decentralized ledgers and blockchains (Aries, Ursa, Indy).

- **The DID Communications Working Group (DIDComm)** was spun out of the Hyperledger Aries community and is now hosted at the DIF. This group develops and contributes to the standards and technology for authentication protocols. It is working to enhance and standardize protocols over the next year, with an emphasis on interoperability.

- **The Sovrin Foundation** is a 501(c)(4) non-profit entity that provides business, legal, and technical support for the Sovrin Network, an open-source project. Using DID technology, the Sovrin Network allows for digital credentials to be privately issued, controlled, managed, and shared. The growth of the Sovrin Network partly depends on contributions from an active open-source development community.

- **The Kantara Initiative** is an international ethics-based non-profit industry commons. Its mission to grow and fulfill the market for trustworthy use of identity and personal data.[134]

Currently, numerous organizations, including governments, financial institutions, and technology companies, are taking a "working code first" approach. Stakeholders recognize that the standards are not ready for broad adoption and are building out ecosystems using code that meets their needs while also shaping the standards and specifications that will be required for full interoperability. One key trend is the adoption of a consistent technology stack of Hyperledger Aries and Hyperledger Indy and the establishment of ecosystems around the globe (Canada, Finland, Germany, and more). These projects are driving several things forward:

- ### Interoperability Testing
  The Hyperledger Aries Interoperability Test[135] is being used to drive multiple areas of alignment, which is particularly crucial for governments. This approach is being used to drive other specifications such as the Wallet and Credential Interaction (WACI[136]) effort hosted at DIF.

- ### Trust Over IP 4-Layer Mode
  The Aries/Indy codebases align well with the Trust Over IP 4-layer model. Aries operates at Layers 2 and 3, while Indy provides the Layer 1 utility. Each project that is operating provides the Layer 4 ecosystem.

- ### Machine Readable Governance (MRG)
  This is a way of orchestrating governance rules and the functions of a conventional trust registry at the agent software level. MRG was developed by Indicio.tech and SITA for the Cardea Project, a complete ecosystem based on Indy and Aries for sharing digital health credentials and data in a privacy-preserving way. After a successful pilot with the Aruban government and health authorities, it was donated to Linux Foundation Public Health for use by public health agencies. The key advantages of MRG are flexibility (everyone can publish their rules, and these can be incorporated and updated according to hierarchy and need), speed (there is no transaction delay required by the need to contact a Trust Registry), and the ability to cache governance rules so that the system can work offline. Critically, Indicio and SITA found that Machine Readable Governance was the most effective way for the Aruban government to exercise its sovereignty over the process of COVID testing.[137]

The adoption of Digital Health Credentials will increase if interoperability allows travelers to share, issue, hold, and verify digital credentials across multiple networks. In practice, this would allow a traveler who received their COVID-19 test result credential from a health information exchange in one country and is able to present that credential to immigration officials in another country.

Thus, it is unlikely that there will be a single, shared ledger where credentials are anchored. Many ledgers will likely be involved in exchanging verifiable credentials, often referred to as a "network of networks." The governance and technical architecture of these networks must be carefully designed for interoperability and governed by principles that are consistent with privacy, security, and individual data ownership.

# VERTICAL FOCUS #2: GOVERNMENT AND INTERNATIONAL INTEROPERABILITY

Various governments have started initiatives (some of them are listed below) in Decentralized Identity with user privacy as a key focus. Importantly, the trending privacy legislation of Europe, Canada, the U.S., and other global leaders addresses data transparency in commercial settings and the right as the data owner to have full control of their personal data and how it is used.

| | |
|---|---|
| **Canada** | Province of Ontario's Digital ID Plan<br>The Pan Canadian Trust Framework<br>Public Sector Profile of the Pan-Canadian Trust Framework<br>CIO Strategy Council - an official standards development organization |
| **Estonia** | Estonia Global ID Solution |
| **European Union** | Video Highlights of the European Commission Proposal<br>Proposal for New E.U. ID<br>News on Proposal for E.U. Digital Identity |
| **Great Britain** | Framework Solution |
| **India** | India's Digital Identity Program - Aadhar<br>Digital IDs to Land<br>Family Digital ID |
| **Adoption of VC standards and/or "progressive" or potentially Decentralized or Self-Sovereign Identity** | ISO/IEC 29794 Series<br>ISO/IEC 29109 Series<br>ISO/IEC 24745<br>ISO/IEC 24761<br>ISO/IEC 19784-1:2018<br>ISO/IEC 24709-1:2017<br>ISO/IEC TR 29194:2015<br>ISO/IEC TR 29196:2015<br>ISO/IEC TR 30125:2016<br>ISO 19792:2015<br>ISO 24714:2015<br>ISO/IEC 29100<br>Privacy ISO/IEC 27018<br>Privacy ISO/IEC 29190<br>Privacy ISO/ IEC 29184<br>Management ISO/IEC 24760 Series |

The Hindawi Survey on SSI provides a summary of the pioneering technical working groups and technology leaders in the space. But more comprehensive lists and descriptions may be found in the accompanying appendices, which may be updated.[136]

# VERTICAL FOCUS #3: FINANCIAL SERVICES AND TAXATION

DeFi platforms are built upon DLT infrastructure and many expected CBDC deployments are expected to leverage the same technologies. A universal, user-centric access point to global financial infrastructure would create efficiencies alongside the development of these transaction networks. The Institute of International Finance published a detailed framework in the Global Assured Identity Network (GAIN) white paper which also details use cases.[139] The U.S. Financial Crimes Enforcement Network (FinCEN) is also pursuing solutions, using collaboration and innovation platforms to explore the efficacy of SSI implementations for financial services.[140]

Beyond creating an interoperable global financial network which allows rapid value exchange without an expensive intermediary, privacy engineering made possible by Decentralized Public Key Infrastructure (DPKI) would allow for efficient compliance tools to be developed such that capital markets participants can protect the anonymity of holdings while still being properly identified to challenge source of funds and identity of end users. This can root out bad actors and create further safeguards to prevent illicit activity.

Perhaps the most valuable application of Decentralized Identity in the long run will be the automation and standardization of tax laws. Currently, there is great political impetus to reduce tax avoidance and evasion, as evidenced by the new Global Minimum Tax proposal.[141] A more complete description of Taxation, standards, and applications can be found in the Global Taxation section of the GSMI 2.0 Report.

## GAPS AND CHALLENGES AS IDENTIFIED IN THE HINDAWI SURVEY

### Standards for Data Management and Wallets

Standard protocols, practices, and policies around user experience, data management, and data exchange should be carefully defined and implemented.

### Key Management

In the SSI model, the responsibility for key management and its associated risks are placed on the shoulders of the users.

### Consent

As stated in the General Data Protection Regulation (GDPR) consent given by the user must be meaningful, well-formed, unambiguous, specific, and freely given, specifying clear decisions.

### Access

Certain DLT systems are public, allowing any entity to read or write to the ledger, while others are permissioned and allow only a selection of authorized entities to read or write new records into the ledger. If not carefully designed, the permissioned approach possesses the risk of forming a centralized architecture similar to an oligopoly among the few authorized entities.

### Accountability and Governance

Certain identity management operations such as identity claim issuance, identity lookup, and secure storage of data may rely on some degree of centralization and dependence on trusted intermediaries.

### Trust in Data

While there may be trust in the underlying SSI network as a secure, robust, and decentralized platform, the methods to form trust among the entities, and the trust in data including the verifiable credentials exchanged must be carefully designed. The authentication and data validation may need to be done through a trusted authority and outside of the blockchain network.

### New Technology Adoption

As a new identity model, SSI requires various modifications to the existing system architectures. Particular attention must be given to the user experience, including the user interactions from the operator's perspective.

### Investment and Commercialization

Any entity intending to adopt SSI must design a strategic plan that supports the investment and risk involved in the deployment and operation of such a system. The SSI economic model may lead to the chicken and egg problem where user adoption depends on the support of the service providers and vice versa.

## RECOMMENDATIONS

- Governments are gradually adopting versions of the SSI framework, and this trend is likelyto continue. The first solutions will not be perfect, but experimentation will prove valuable. The beauty of Web 3.0 is the open-source nature of documentation, projects, pilots, and case studies made available to all who can contribute.

- Open standards and technologies will pave the way for wider adoption of decentralized identity standards globally. Stakeholders should stay informed of open-source community developments. The Hyperledger Foundation and other open-source consortiums frequently publish vast research repositories and case studies.

- Basic identifiers like national IDs, passports, etc. will always be issued by the founding authority. But in an SSI framework, the user will control their identifiers and with whom they would like to share them. Most developed nations are providing a legislative template for the rest of the world to follow.

- Interoperability and inclusion will be critical features in decentralized identity solutions going forward.

## CONCLUSION

Leveraging decentralized public key infrastructure as the basis for SSI frameworks is a frontier development. Standards for DID methods, protocols, verifiable credential formats, and other technical ambiguities are being explored through trial and error. Although the end goal involves direct interaction with the individual, enterprise and government adoption are critical for rapid iteration and proliferation.

Institutions which adopt SSI frameworks will create economic efficiencies and rebuild eroding public trust. The open-source nature of early implementations will help create a robust and interoperable framework which laggards will benefit from, but early adopters will pave the way forward. The more intangible benefits of SSI will be portrayed in human form. By providing agency, basic digital identification, the ability to prove ownership of digital property, and banking services, each human being will have greater potential to self-actualize.

Data exchange networks envisioned by leaders today will allow for the "self-sovereign individual" to monetize their own data with control, autonomy, and privacy without sacrificing convenience. Travel across borders will be seamless. Electronic healthcare records will be accessible by the user regardless of location or insurance provider.

Financial services will be accessible to more people, who will be able to prove their identity with multiple sources of attestation without recurring registration or the creation of another set of siloed credentials vulnerable to data breaches.

The combination of public communication networks and privacy-preserving identity management tools will allow frictionless flow of data and value with automated accounting trails and transactions. To learn more about Digital ID, read the full report here.