

Human-Centric Digital Identity:

for Government Officials

v1.1

Lead Editors: Elizabeth Garber, Mark Haine

October 13, 2023

Citation:

Garber, E. and Haine, M. (eds) "Human-Centric Digital Identity: for Government Officials
OpenID Foundation, (September 25, 2023)

Date	Revision
October 13, 2023	V1.1 includes additional co-brand partners and MyData Global added to Appendix D
September 25, 2023	Final v1 version published
September 18, 2023	Public comments addressed and accepted. Pre-editorial. Graphics and tables will be formatted.
July 07, 2023	Publication of Public Comment draft
April 14, 2023	Expert Review

Contributors



We would like to acknowledge the following people whose thought leadership and content shaped the messages herein and without whom this paper would not have been possible:

- Dave Birch
- Julie Dawson
- Heather Flanagan
- Gail Hodges
- Nishant Kaushik (confirmed)
- Henk Marsman
- Nat Sakimura
- Golda Velez
- Kaliya Young

Table of Contents

EXECUTIVE SUMMARY	4
AUTHORSHIP	5
KEY TERMS	6
PART 1: IDENTITY AND THE ROLE OF GOVERNMENT	1
CONTEXT	1
WHY THIS PAPER	5
WHAT DO DIGITAL IDENTITY SYSTEMS MEAN FOR PEOPLE?	7
PART 2: TODAY'S DIGITAL IDENTITY PARADIGMS	11
PARADIGMS 1 AND 2: GOVERNMENT-ISSUED EID	17
PARADIGMS 3 AND 4: GOVERNMENT-ENABLED MARKETPLACES	23
PARADIGM 5: THE EMERGING WALLET-BASED PARADIGM	26
KEY CONSIDERATIONS	30
PART 3: RECOMMENDATIONS FOR DIGITAL IDENTITY SYSTEMS	33
A UNIFIED SET OF PRINCIPLES	33
PILLAR 1: HUMAN-CENTRICITY	34
PILLAR 2: STRATEGIC DESIGN AND GOVERNANCE	41
PILLAR 3: SECURE AND PRIVACY-PROTECTING IDENTITY SYSTEMS	47
PILLAR 4: DELIVERING INTERNATIONAL INTEROPERABILITY	50
CONCLUSION AND SUMMARY	53
APPENDIX A – EVOLVING THREAT MODELS	55
APPENDIX B – ALIGNING DIGITAL ID PRINCIPLES	57
APPENDIX C: OECD PRINCIPLES AS A CHECKLIST	59
APPENDIX D: NON-PROFITS WITH A ROLE IN HUMAN-CENTRIC DIGITAL IDENTITY	66
APPENDIX E: PRIVACY AND SECURITY BEST PRACTICES	69

Executive Summary

Legal identification systems provide individuals access to civic and economic life; they enable businesses to thrive and societies to function. They often provide crucial input to the formation of trusted relationships between people, entities, and (more recently) things. The right to “recognition as a person before the law,” Article 6 of the United Nations (UN) Universal Declaration of Human Rights,¹ effectively provides the foundations upon which governments deliver many enshrined civic, economic, political, and other rights, including education, healthcare, voting, marriage, and travel.² Even self-determination and privacy arguably depend upon the government’s recognition of each individual as distinct from the collective. This dependency is why the UN has set a Sustainable Development Goal to achieve universal Legal Identity and birth registration by 2030 (SDG 16.9).³

It is in this context that many nations (as well as supra- and sub-national entities) are now seeking to build **Digital** Identity Systems and Ecosystems, spurred by the promising analysis of organizations like McKinsey,⁴ The Bill and Melinda Gates Foundation,⁵ The World Economic Forum,⁶ and the World Bank.⁷ However, substantial risks are inherent in the design, deployment, roll-out, and ongoing management of any Identity System; digitization heightens the risk.⁸

Parts 1 and 2 of this paper explore these issues and survey the global landscape in order to distill the key trends at play across today’s Digital Identity System paradigms. Part 3 then builds on existing principles-based literature to provide recommendations to government officials as they manage the trade-offs required by the design, implementation, and management of Digital Identity Systems. Importantly, it takes the position that no one size fits all: that multiple systems may sit alongside one another and that no single technology, architecture, or governance approach provides a panacea. Instead, it builds upon the OECD’s recent Recommendations on the Governance of Digital Identity to recommend that government officials:

- Ensure that Digital Identity Systems are designed to underpin, sustain, and promote Human Rights objectives, building upon fit-for-purpose Civil Registration and Legal Identity Systems.
- Follow a Value-Sensitive Human-Centered Design (HCD) process.

- Take a strategic approach that translates Value-Sensitive HCD into technology and institutional framework requirements.
- Incentivize best practices in relation to security and privacy by design.
- Engage in the maturation of Open Standards to support fit-for-purpose Digital Identity Ecosystems.

(See [Table 5](#) for the complete set of recommendations. There are several Appendices to this paper that will remain living documents, with new non-profit organizations and emerging standards added as required.)

Authorship

The OpenID Foundation (OIDF) commissioned this paper, which has been co-published by 11 contributing organizations (see [Contributors](#)). The lead editors are members of OIDF, OIX, and other standard-setting communities. They also have for-profit businesses that leverage OIDF and non-OIDF standards. The paper, in its rigorous research and interview process, attempts to minimize bias regarding technology and architecture. With that said, the OIDF's Vision is to help people assert their identity wherever they choose, and its Mission is to lead the global community in creating identity standards that are secure, interoperable, and privacy-preserving. All the non-profits and experts contributing to this paper share a common desire to 1) ensure the use of safe, proven protocols for the transfer of identity data, 2) enable cross-border interoperability, and 3) help public and private sectors realize benefits and navigate the transition to robust digital identity infrastructure.

Key Terms

Many of the terms used in this paper have different meanings in different contexts; various fields and organizations have developed their own lexicon for the same concepts. For example, “Identity” has different meanings to a social scientist, a member of the international development community, or a Chief Information Security Officer charged with securing an enterprise. It also has different meanings across people and cultures. Yet all these groups have value to add to the development of Human-Centric Identity Systems.

This paper draws upon definitions used by the

- United Nations Department of Economic and Social Affairs in “Guidelines on the Legislative Framework for Civil Registration, Vital Statistics, and Identity Management;”⁹
- United Nations *1954 Convention relating to the Status of Stateless Persons*;¹⁰
- United Nations *1951 Refugee Convention*;¹¹
- United Nations *Guidelines on Statelessness*;¹²
- The OECD in “Recommendations on the Governance of Digital Identity.”¹³

This convention ensures consistent use of language as negotiated by cross-governmental collaboration. Some terms have been added or annotated.

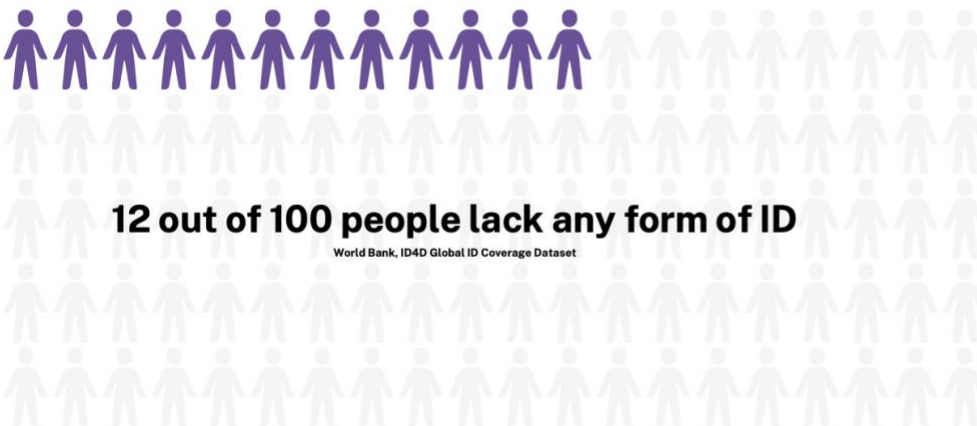
Legal Identity (United Nations)	<p>The basic characteristics of an individual's identity, for example, name, sex, place, and date of birth conferred through registration and the issuance of a certificate by an authorized Civil Registration authority following the occurrence of birth. In the absence of birth registration, Legal Identity may be conferred by a legally recognized identification authority ... it is required by the issuance of a death certificate by the Civil Registration authority.</p> <p>[UN] Member States are primarily responsible for conferring Legal Identity and issuing identity papers. The responsibility for conferring Legal Identity on refugees may also be entrusted to an internationally recognized and mandated authority.</p>
Digital Identity (OECD)	<p>A set of electronically captured and stored attributes and/or credentials that can be used to prove a quality, characteristic, or assertion about a user and, when required, support the unique identification of that user.</p> <p>Note that while it is not contained in the OECD definition, legal entities, devices, and other non-humans must also be identified.</p>
Digital Identity Ecosystem (OECD)	<p>The different actors involved in the digital identity system such as policymakers, regulators, government supervisory bodies, digital identity solution providers, credential issuers, service providers, and users. The ecosystem may include different domain-specific solutions and their associated actors.</p>
Digital Identity System (OECD)	<p>The entirety of the system under which digital identity solutions, credentials, and attributes are provided to users and relied upon by service providers, including the policies, regulatory frameworks, trust frameworks, technical standards, and roles and responsibilities.</p>
Civil Registration (United Nations)	<p>The continuous, permanent, compulsory, and universal recording of the occurrence and characteristics of vital events pertaining to the population, as provided through decree or regulation in accordance with the legal requirements ... The process establishes the fact of occurrence of vital events and provides legal documentation for such events in the form of a certificate ... a document, in paper or electronic format, issued by the registrar...</p>
Legal Status	<p>No single definition for "Legal Status" was identified in the UN or OECD documents. However, this paper uses the term to convey concepts relating to Nationality Status, Civil Status, Refugee Status, and Stateless Person (defined below),</p>
Nationality Status (United Nations Guidelines on Statelessness)	<p>"Nationality status is relevant when individuals apply for passports or identity documents, seek legal residence or employment in the public sector, want to exercise their voting rights, perform military service, or attempt to access government services."</p> <p>Note that each state has its own legal basis for conferring nationality; this is not defined internationally.</p>
Civil Status	<p>Generally refers to a person's legal status in a society, including marital status and</p>

(United Nations)	age. Civil Status may determine a person's legal capacity to act ... and obligations, rights, and duties between persons.
Stateless Person (United Nations 1954 Convention)	A person who is not considered as a national by any State under the operation of its law.
Credential (OECD)	A set of one or more electronically recorded and trusted assertions about a user made by a credential issuer, such as a driver's license, ID card, permit, or qualification. Note that though the OECD definition states that the assertions are "trusted," this may not always be true. Credentials may be issued by any number of organizations or even self-issued. Trust is not implicit in the term.
Digital Identity Solution (OECD)	Material and/or immaterial unit allowing users to store, retrieve, and/or share attributes and/or credentials, and which is used for authentication for an online or offline service.
Attribute (OECD)	A verified quality or characteristic ascribed to a user, for example, name, date of birth, place of birth, uniqueness identifier (e.g., personal ID number, social security number, company registration number), and address.
Authentication (OECD)	A function for establishing the validity and assurance of a claimed identity of a user, device, or another entity in an information or communications system.
Trust Framework (OECD)	A set of common requirements that digital identity solution providers follow for the purpose of facilitating trust within a Digital Identity Ecosystem. The requirements can be divided into different Levels of Assurance (LoA).
Credential Issuer (OECD)	Refers to any entity, public or private, that issues credentials to users.
Refugee (United Nations 1951 Refugee Convention)	Someone who is unable or unwilling to return to their country of origin owing to a well-founded fear of being persecuted for reasons of race, religion, nationality, membership of a particular social group, or political opinion.



Everyone
has the right to recognition
everywhere
as a person before the law

Article 6 of the Universal Declaration on Human Rights (1948)



At least 10 million people are stateless

United Nations Refugee Agency

- 1
- 2
- 3 See Endnotes^{14 15 16 17}

Figure 1: Identity in the Context of Human Rights

Part 1: Identity and the Role of Government

Context

Governments and intergovernmental organizations have long been aware of the crucial underpinning role that identification plays in delivering upon government objectives, upholding the rights of individuals, and supporting social dynamics across society.¹⁸ Specifically, Legal Identity forms a basis on which the state recognizes individuals and, based on their Legal Status (see Box 1), provides services that meet fundamental needs.¹⁹ Civil Registration laws and processes provide the foundation upon which this Legal Identity rests. Given the promise of so many positive societal and human outcomes and the importance of legal recognition for ensuring human rights, the UN has set a Sustainable Development Goal (SDG) target that by the year 2030, all people will have access to Legal Identification ([SDG 16.9](#)). According to the World Bank, today's gap is at least 0.8 to 1 billion people,²⁰ although this figure may overlook registered but under-documented populations.

Box 1: Legal Status

Governments confer Legal Status (e.g., as a Citizen at Birth Registration, as an Asylum Seeker or Refugee following due process). The legal code ascribes rights, obligations, etc. as a result of that status.

For the purpose of this paper, the term "Legal Status" is an umbrella covering Civil Status, Nationality Status, Refugee, Stateless Person, and others that governments may confer.


This promise of positive societal and human outcomes has spurred the launch of numerous government-led initiatives around the world, with many looking to **Digital Identity** technologies, solutions, and systems. Yet, as pointed out in a 2021 article by Legal Identity scholar Dr. Bronwen Manby, not all initiatives have the same goals or approach.²¹ Government objectives range from security to stability and resilience to growth. Sovereign governments and their distinct agencies may pursue any number of objectives; so too may the non-profits and private vendors advising them.²² [Table 1](#) provides examples of government-led research and initiatives that propose Digital Identity technologies to achieve various outcomes.

Table 1: Perceived Benefits of Government Identity Initiatives

	Government Motivation	Research and Initiatives
Access to Opportunity	<p>Economic Engagement and Productivity Counterparty trust enables economic activity, supports inclusion, and reduces costs (e.g. fraud).</p>	<p>McKinsey estimates that access to identification (including digital identification) can unlock 3-13% of GDP.</p>
	<p>Financial Stability Digital Identity supports global money movement and counters illicit flows: e.g. drugs, arms, and human trafficking.</p>	<p>The Financial Action Task Force (FATF) argues that reliable and independent identity systems underpin efforts to promote inclusion and stop illicit financial flows.</p>
Access Government Resources	<p>Government Services Ensuring access to government systems benefits to which they are entitled. Reducing fraud ensuring efficient provisioning.</p>	<p>Many culturally-relevant approaches around the world (see Part 2).</p>
	<p>Benefits and Aid Supporting citizens, refugees, asylum seekers, and effectively stateless individuals in times of crisis.</p>	<p>Bill and Melinda Gates Foundation reports that women are more likely to receive their cash benefits under Pakistan’s Biometrically enabled NADRA program.</p>
National Security	<p>Cybersecurity Robust identity and access management underpins cybersecurity within government systems, supply chains, and the core infrastructures that power nations.</p>	<p>The EU Cybersecurity Act and The Biden Administration’s National Cybersecurity Strategy cite Digital Identity as a key enabler.</p>
	<p>Physical Security Recognizing citizens, non-citizens, and bad actors enables governments to provide physical security.</p>	<p>US Department of Homeland Security cites mobile driving licenses (mDL) as an initiative for safer air travel.</p>
	<p>Political Stability Fraud and misinformation have destabilizing effects on democratic processes.</p>	<p>>50% of Estonian voters voted digitally in 2023. Many African nations (e.g. Nigeria, Ghana) leverage biometric authentication to secure elections.</p>

See Endnotes 23 24 25 26 27 28 29

As highlighted above, the wide-ranging motivations in [Table 1](#), coupled with the objective to provide Legal Identity for all (UN SDG 16.9),³⁰ create a context within which many governments now seek to leverage recent technological advances to develop Digital Identity Credentials, Systems, and Ecosystems (see [Key Terms](#)).



Technology is neither good nor bad;
nor is it neutral.
-Melvin Kranzberg

All technologies have positive and negative possible outcomes. In the case of Digital Identity, technology has the power to enhance any negative human impacts already present within a given nation's approach (legal, procedural, and technical) to Legal Identity.³¹ Furthermore, all technologies are necessarily built with an embedded set of values that affect outcomes, whether those values are explicit, implicit, or even unconscious.³²

Many of the initiatives in [Table 1](#) face criticisms and carry serious risks that practitioners must grapple with. For example, as Digital Identity Systems become more extensive and embedded in society, the impact of cybersecurity incidents may include large-scale cross-sector outages and the loss of vast amounts of personal data to bad actors. This level of cybersecurity incident happened to India's Aadhaar system in 2018, resulting in the third-largest cybersecurity breach in history.³³ Other known incidents of Identity System breaches have occurred across the world and in countries with different architectures (e.g., Argentina,³⁴ Nigeria,³⁵ South Korea,³⁶ Estonia,³⁷ and Austria³⁸). Of course, as the capture, storage, and use of biometric technologies grows, so does the possible impact of an insecure or otherwise weak solution: individuals can more easily replace a string of numbers than they can replace their iris, facial template, or fingerprint.³⁹ With Digital Identity Systems acting as "gatekeepers" to a wealth of personal data, such breaches may

result in widespread harm to individuals and, with data loss and fraud at scale, to society as a whole.

Governments and their partners may cause further harm as a result of how they process Digital Identity data themselves. At scale, unscrupulous processing affects society and can unintentionally undermine human rights.⁴⁰ Unscrupulous processing might include biased algorithmic decisions that affect people's lives (e.g., protected characteristics influencing insurance, employment, tenancy, or other critical decisions) or other forms of social manipulation.⁴¹

History offers many examples of intentional human rights violations enabled by Legal Identity Systems. These examples include the misuse of identity data to spy on citizens, disenfranchise them, displace them, de-nationalize them, or commit genocide. Examples from modern history include the use of identity cards to displace and de-nationalize the Rohingya population of Myanmar,⁴² the targeted constraints on access to identification that have disenfranchised black and indigenous voters in the United States,⁴³ the stripping of citizenship for over a million individuals in the province of Assam, India,⁴⁴ and the effects of profligate data collection by Germany's Third Reich and German Democratic Republic regimes.⁴⁵ Whether these harms arise as a result of intentional policy, regime change, or inadequate internal controls, designers must take them into account. Since the likelihood and impact of all of these risks can be heightened by technology, Human Rights organizations continue to raise concerns about the potential misuse of well-intended Digital Identity Solutions promoted by organizations like the UN and World Bank.⁴⁶

Just as no single model of government applies universally, no one Identity System will work everywhere: nations and their people have unique histories, social complexes, expectations of government, and cultures that influence the appropriate solution.⁴⁷ However, this paper builds on a multidisciplinary body of literature to argue that Identity Systems that are steeped in history and designed and built to meet the needs of real people—with their relationships and social contexts in mind—stand to be more sustainable and deliver greater benefits to society.

Why This Paper

Driven by the promise of tangible societal benefits and aided by myriad technological advances, governments now embark upon ambitious projects to shape or re-shape Digital Identity Systems. However, that simple sentence encompasses a great deal of complexity. The term “government” belies the many layers, functions, and agencies that have a stake in Identity Systems: this paper speaks to all of them.

The broad scope is necessary because actions taken by discrete entities may have unintended consequences for the ecosystem.⁴⁸ As established, each public sector actor (whether that’s an individual civil servant, a functional unit and its partners, or an entire organization) at any layer of government (supra-national, national, regional, or local) has their own perspective on identity: their own approach for issuing Legal Identity (and the associated proofs) or Credentials, conferring or defining Legal Status (if relevant), managing Attributes, Authentication, and any activities that authorize access and actions. Their systems often need the capacity to communicate, i.e., to establish trust between parties and validate that an individual has a given set of rights. Many public and private sector entities have a legitimate stake in this ecosystem. Each small component or protocol is shaped by a myriad of technological, policy, and governance decisions. As noted above, each decision in this complex web upholds or brings forth a value system.

Without a holistic government strategy that includes a coherent approach to identifying and recognizing people online, market-led solutions emerge that often support limited functional objectives. Analyzing such trends in recent US history, the Better Identity Coalition (BIC), an industry advocacy group, articulates how the unmet need for verifiable information has led to often unchecked market-led solutions that have had privacy and data security weaknesses, such as attractive data pools, levers for social engineering attacks, and various tracking methods (see Figure 2).⁴⁹ Given the diversity of weaknesses, societal needs, and responsibility dispersion, the challenge to individual civil servants is understandable. Yet, as Windley (2023) argued, “Phishing attacks, fraud, complexity, and friction are the results of not considering how humans participate in an identity solution.”⁵⁰

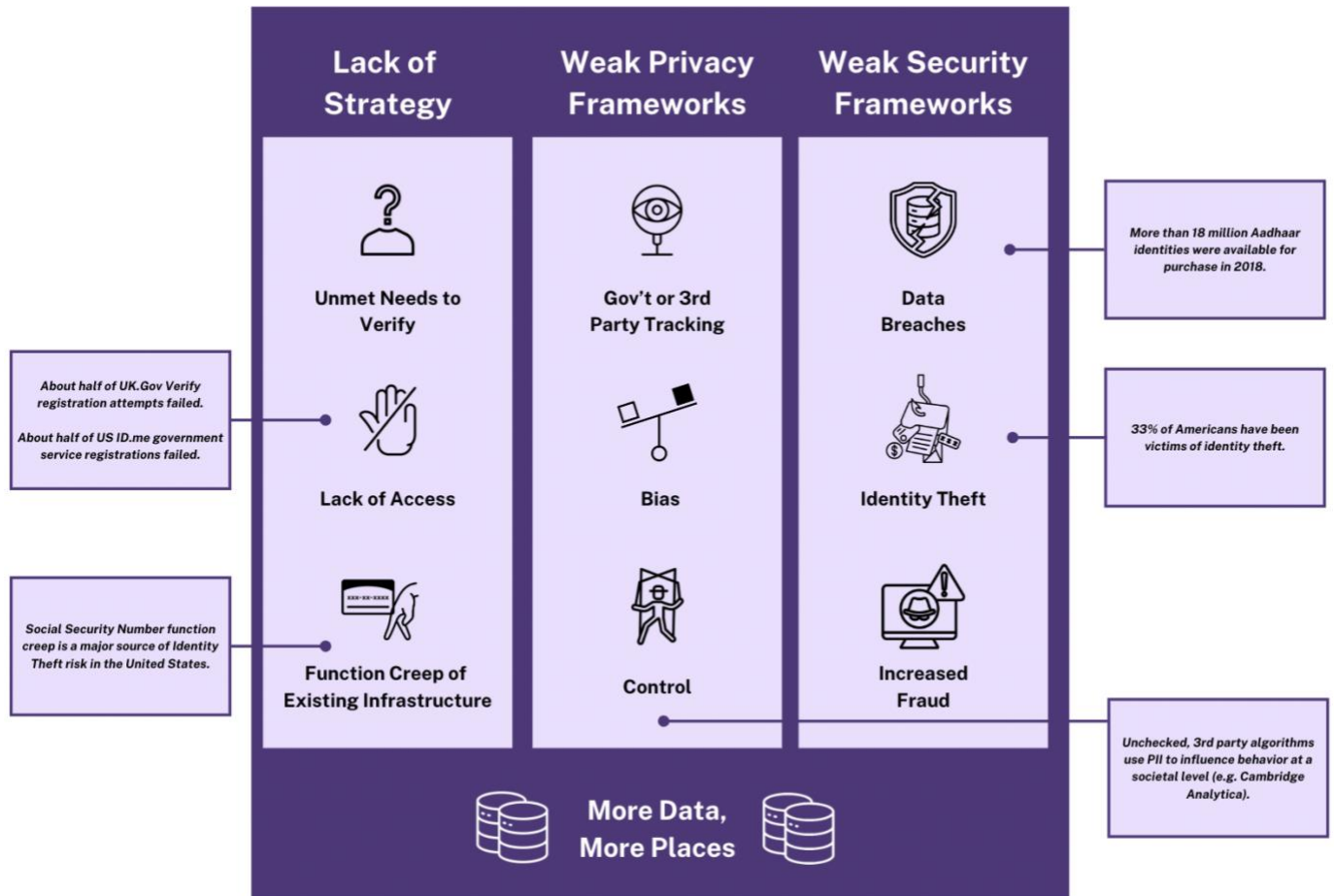


Figure 2: Unintended Consequences of a Weak Digital Identity Strategy

See Endnotes ^{51 52 53 54 55 56 57}

An immature legal, regulatory, or other governance framework is often at the heart of many examples of alleged harm from a weak digital identity strategy.⁵⁸ The data points in Figure 2 show that, in some cases, the strategic gaps are not just technical in nature; instead, they are enabled or exacerbated by the institutional context and may result in various forms of harm. Such harms may include lack of access to state resources,⁵⁹ breaches of government-held private information,⁶⁰ and breaches of private databases leading to identity theft,⁶¹ election interference,⁶² and government surveillance.⁶³ Not only does the absence of legal frameworks create conditions under which harms may develop,

but privacy and security legal scholars argue that laws drafted with simple organization-focused outcomes in mind, such as breach-focused security laws,⁶⁴ incentivize organizational behaviors with negative systemic consequences.⁶⁵ These lessons are crucial for any Digital Identity System, perhaps especially those that will involve private-sector participants and enable them to access data held in government systems.

In designing Digital Identity Systems, government officials are navigating high-stakes, complex terrain. This paper, built upon an extensive review of existing multidisciplinary bodies of related literature, provides a resource for officials in that situation. Its global scope does not imply a “one-size-fits-all” approach; the assumption is that many legitimate approaches will co-exist. Instead, the global scope implies that many of the challenges are common and require collaboration within and across borders. [Part 2](#) explores these challenges in the context of the Digital Identity paradigms in government systems today. [Part 3](#) unifies existing principles-based literature, deepening a discussion about how governments can approach building Human Rights-affirming Digital Identity Systems that are, at once, domestically appropriate and interoperable across borders. To develop these insights, the authors interviewed representatives from government and non-government entities in North America, Europe, Asia, the UK, and Africa.

What do Digital Identity Systems Mean for People?

This paper may be for government officials, but to deliver rights-affirming Digital Identity Systems requires orienting around people and society. The term “Identity” itself is polysemantic and has different meanings as it crosses context. A social scientist may use the term to convey a set of ideas that differ from those that matter to a computer scientist or systems administrator. In some cases, “Identity” is concrete and takes the form of property, as in “my identity was stolen.” In other cases, especially in the digital realm, it is fluid and ever-changing, dependent on dynamic relationships.⁶⁶ All of these interdependent constructs of “Identity” serve legitimate purposes. For the purposes of this paper, “Identity” refers to all the ways that a person conveys who they are to others; they may legitimately choose to assert different—sometimes even competing or contradictory—facets of their identities to any number of counterparties. However, because “Identity” emerges in relation to another party, there is an interdependent meaning: it is also how any one party recognizes another.⁶⁷

Legal Identity, in particular, enables individuals to be recognized by governments and other parties: it forms a foundation for rights, privileges, access, and accountability. The law describes the rights and privileges a person can claim according to their Legal Status. Recognition as a citizen, for example, offers protection, proffers rights (such as voting and welfare), and empowers them to move about their world, access resources, and engage in the economy.⁶⁸ Without access to a persistent Legal Identity, people may struggle to claim Legal Status and increasingly find themselves excluded from education, healthcare, financial services, or many other aspects of daily life.⁶⁹

Whether they are Digital or not, Identity Systems do not work equally well for all people. As articulated above, the shift to Digital technologies may heighten disparities or Human Rights issues in existing analog systems. Individuals have different accessibility needs or preferences that affect their ability (or willingness) to engage with Digital Identity Systems, e.g., a mobile phone constitutes a barrier for some even as it creates broader opportunities for inclusion. Mandating its use may exclude those with visual impairments, learning differences, those who do not have a phone, etc. Others, such as the “Privacy Defender” segment outlined in Ernst & Young’s Connected Citizen Report, simply do not trust the government with their data.⁷⁰

In addition to such individual differences, Digital Identity System design must also consider important variations in context that may emerge in any lifetime. Failures to do so may result in considerable harm to marginalized or vulnerable populations. For example, UK healthcare notification systems linked to identity and authorization management have inadvertently enabled domestic abusers to track their former partners and children.⁷¹



Figure 3: High-Stakes Stakeholders for Identity and Digital Identity Systems

See Endnotes ⁷²

In the next section, [Part 2: Today's Digital Identity Paradigms, the paper](#) explores the types of Digital Identity Systems existing today. In reviewing these ecosystems, It is worth considering how implementations may support or undermine different social groups and

contexts, such as those identified above. Although the paper offers some analysis, this should not replace a more detailed review of stakeholders and at-risk communities internationally or within a given jurisdiction.

Part 2: Today's Digital Identity Paradigms

Driven by differences in culture, infrastructure, institutional readiness, political structure, economic incentives, and much more, a variety of Digital Identity Systems have emerged around the world. Among other cultural factors, each nation's history with Civil Registration and Legal Identity underlies its current context and the appropriate ways a digital solution may complement it.⁷³

In 2016, Consult Hyperion published an in-depth analysis of Digital Identity system archetypes.⁷⁴ This section draws heavily upon that work and adds information and nuance as to where the market topography has changed in intervening years. In particular, this updated diagram reflects that the market has evolved at the poles, where biometrics and wallet-based models have seen significant advances. The following sections will explore the nature of these models alongside a brief discussion of exemplar implementations.

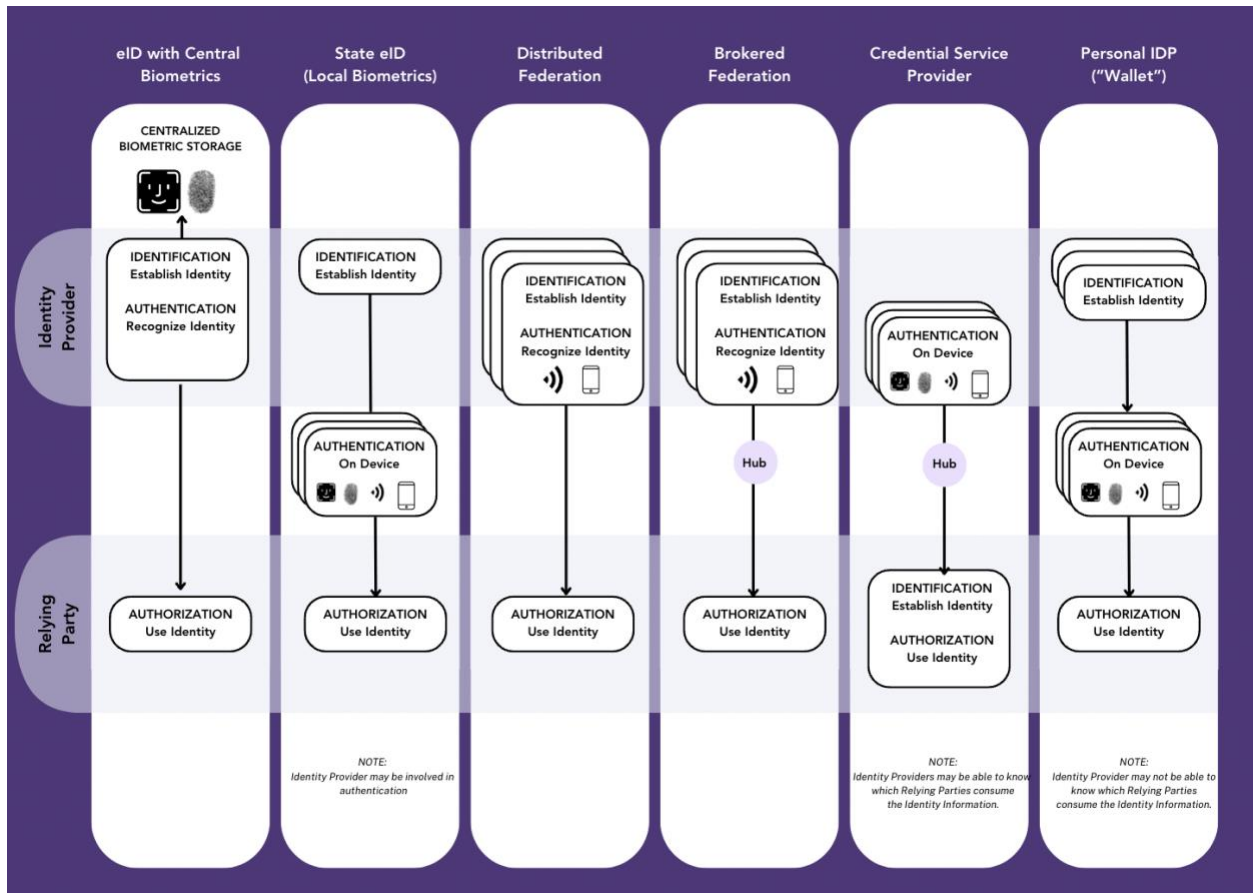


Figure 4: Digital Identity Architectural Models

Figure 4 is adapted from Consult Hyperion’s Digital Identity Issue Analysis (explanation below).⁷⁵

While the definition of “Digital Identity System” at the forefront of this paper allows for various interpretations, it is important to recognize that the term “Digital Identity” means something different across these paradigms. The most important distinction is that, in some paradigms, Digital Identity is issued and recognized by the government. In others, Digital Identity is created by a private entity, following the validation of Legal Identity information contained in a Credential issued by the government. “Digital Identity System,” for the purposes of this paper, encompasses these variations in which people digitally assert information related to (but not always the same as) their Legal Identity.

There are many technical nuances contained within Figure 4. The critical technological differences relate to the nature of the identity provider, the use of biometrics—especially in Authentication—the presence of a central hub, and the presence of a **Personal IDP**, often called a “wallet.” Digital Identity Systems often rely upon a government-issued identity Credential as an anchor. This anchor can be an electronic element contained within a smart card or chip embedded in a piece of physical evidence, like a passport. In some countries, such as India and Uganda,⁷⁶ the government leverages centrally stored biometric data to support Authentication and reduce the likelihood that one individual can present multiple identities linked to government services (**eID with central biometrics**). In other systems, biometric information remains local to the user, held in a smart card or mobile device (the **State eID** and **Personal IDP** models).

Still others, such as Norway⁷⁷ and Canada,⁷⁸ have thriving Digital Identity Systems based on privately-issued Credentials derived from a thorough vetting of the individual and their government-issued documents (**Distributed Federation**). These systems have a broader distribution of federated “Identity Providers” with various Authentication methods. The Identity Providers make decisions about collecting, storing, and using biometric data in these contexts and within the bounds of any legal, regulatory, or other controls established within a Trust Framework. Similarly, some have sought to create a brokered marketplace where users work with a central stateless hub (**Brokered Federation**) or marketplace to select from a variety of secure identity or Authentication providers (**Credential Service Providers**). Finally, as decentralized identity standards mature, governments have developed plans to build **Personal IDP** or wallet-based ecosystems, in which state agencies and any number of Credential Issuers issue eIDs to interoperable wallets that users can leverage to prove their identities anywhere.⁷⁹ Theoretically, those wallets may hold multiple government or privately-issued Credentials, thus differentiating them from the eID archetype above.

Note that [Figure 4](#) intentionally does not lay out these architectural models in terms of a “Centralized” to “Decentralized” scale because it is reductive to do so. Each model contains large stores of Identity Information living within databases at both the Credential Issuer and any Relying Party (or Verifier) who needs to store that data (e.g., for audit purposes). Within each model, there remain multiple technical choices about where data will live and where Authentication will take place, as well as governance choices about which parties can see, amend, or otherwise control that data. For example, in the wallet-based paradigm,

policy decisions will determine the extent to which wallet providers (e.g., a device manufacturer) can see, store, revoke, or otherwise control Credentials. The technical decisions will then need to uphold those policies. The reverse is also true: governance and policy must be developed in response to the possibilities and risks afforded by the available architectural choices.

The Consult Hyperion report analyzes the models in [Figure 4](#) in terms of their vulnerabilities, threats, and viable mitigation strategies, noting that all models have the potential to be implemented poorly or misused.⁸⁰ [Table 2](#) builds upon this work, offering additional risks and mitigants and describing how some variations in architecture share common vulnerabilities, differently weighted in trade-off decisions.

Table 2 – Architectural Models & Associated Risk/Mitigation Strategies

	Key Threats	Mitigation
eID with Central Biometrics	<ul style="list-style-type: none"> • Breach of biometric data leading to irrevocable ID theft • Government surveillance, enabled by excessive data collection • Enables user tracking by third party data recipients • Private Information passed to malicious Relying Parties 	<ul style="list-style-type: none"> • Security standards include biometric protections (e.g. bihashing) • Data minimization and privacy protections in a strong legal framework • Unique identifiers passed to third parties • Set RP rules, controls, and audits/enforcement practices
eID with Local Biometrics	<ul style="list-style-type: none"> • Government surveillance enabled by excessive data collection • Data breach • Enables user tracking by third party data recipients • Private information passed to malicious Relying Parties 	<ul style="list-style-type: none"> • Data minimization and privacy protections in a strong legal framework • Strong minimum security standards built into governance framework • Unique identifiers passed to third parties • Set RP rules, controls, and audits/enforcement practices
Distributed Federation	<ul style="list-style-type: none"> • Private Information passed to malicious relying parties • Poor privacy practices by Identity Provider • Data breach at Identity Provider • Consumer choice without clarity around IDP privacy & security 	<ul style="list-style-type: none"> • Set RP rules, controls, and audits/enforcement practice • Data protection standards (incl tech), enforcement, and contracts • Strong minimum security standards in governance framework • Transparency coupled with strong minimum standards & governance
Brokered Federation	<ul style="list-style-type: none"> • Hub architecture creates risk of tracking (by the hub) • Private Information passed to malicious Relying Parties • Poor privacy practices by Identity Providers • Data breach at Identity Provider or Hub • Consumer choice without clarity around IDP privacy & security 	<ul style="list-style-type: none"> • Hub must be stateless, store no data • Set RP rules, controls, and audits/enforcement practice • Data protection standards (incl tech), enforcement, and contracts • Strong minimum security standards in governance framework • Transparency coupled with strong minimum standards & governance
Credential Service Providers	<ul style="list-style-type: none"> • Hub architecture creates risk of tracking (by the hub) • Authentication only does not facilitate identity proofing • Issuers and verifiers may not trust each other in a triple blind model • Inclusion limited to type of providers in the system 	<ul style="list-style-type: none"> • Hub must not store data about where credentials are used • Minimum standards for identity proofing elsewhere in the ecosystem • Strong governance framework and enforcement model in place • Ensure a variety of providers to promote inclusion (i.e. not just banks)
Personal IDP ("Wallet")	<ul style="list-style-type: none"> • Difficult to establish trust between all parties in the ecosystem, which includes issuers, holders, wallets, verifiers, relying parties • Reliance on end user to understand privacy and safety practices • Reliance on end user to remember/maintain private keys 	<ul style="list-style-type: none"> • Develop a scalable model for establishing, maintaining, and revoking trust between parties • Strong minimum privacy & security standards underpinned by law • Provide secure recovery options and alternatives

Adapted from Consult Hyperion’s Digital Identity Issue Analysis⁸¹

This work’s risk mitigation strategies assume objectives promoting privacy and human rights protections. They also demand that the institutional frameworks that define, govern, and enforce protections mature at a similar rate to the technological implementation. Therefore, understanding the global archetypes requires analysis of architectural models alongside governance typologies.

The Monetary Authority of Singapore articulates four Governance Typologies ([Figure 5](#)), ranging from fully **Private Governance** to fully **Public Governance**.⁸² In between these models exist varying degrees of collaboration, including private consortia, **Government-Enabled Governance**, and **Public-Private Governance** models.

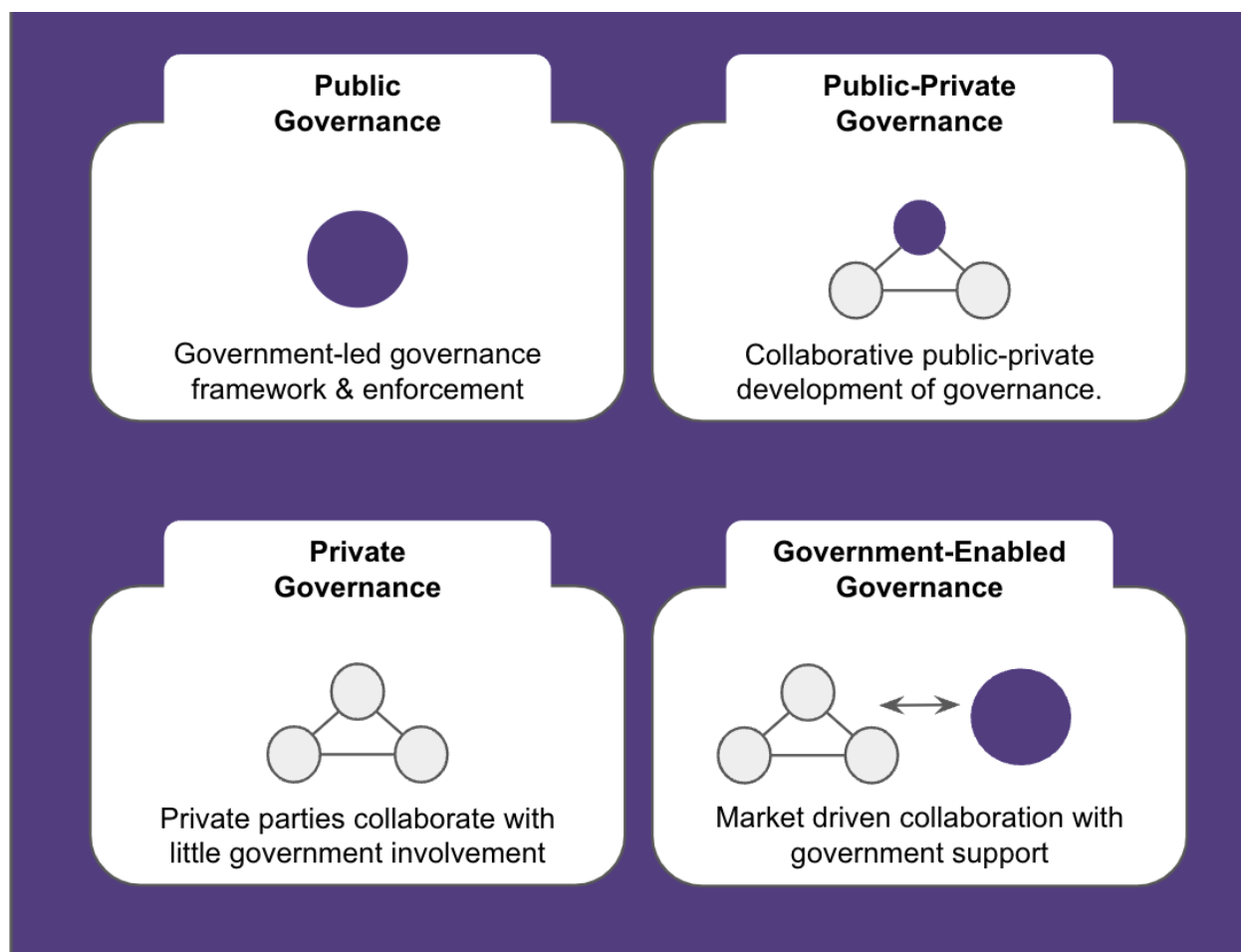


Figure 5: Governance Typologies

For a more rigorous and detailed comparison of Trust Frameworks, see [OIX – A Guide to Trust Frameworks for Smart Digital ID](#)⁸³

Note that while the earlier technological architecture models (Figure 4) describe self-contained digital identity systems, the typology of governance models above (Figure 5) can be applied on multiple levels, from a single system to a network with multiple Ecosystems

interacting. With that said, when overlaying governance with technology, an interesting set of paradigms emerges.

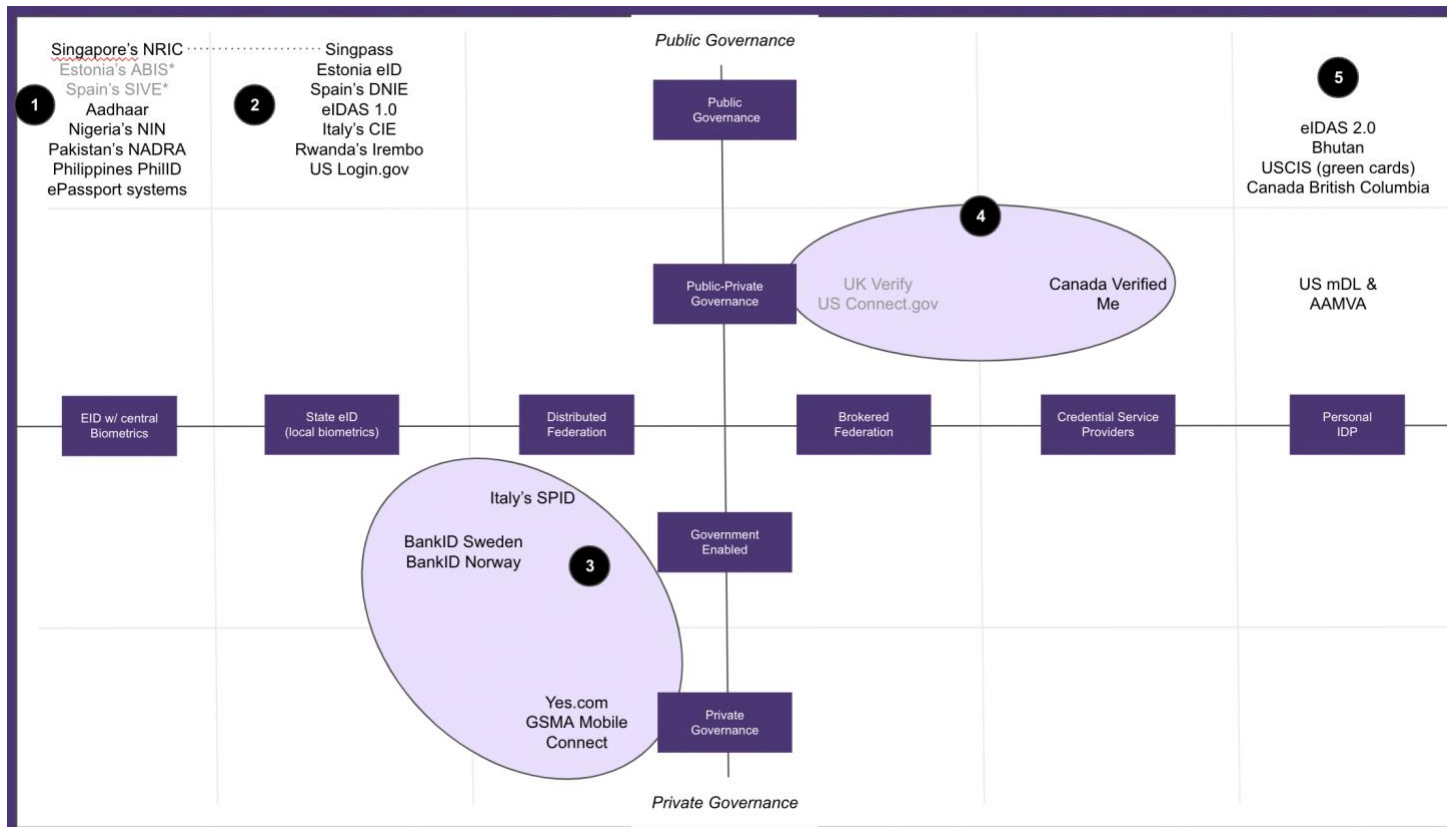


Figure 6: Digital Identity Paradigms – Technology vs. Governance

The following sections explore the five paradigms articulated in this diagram.

Paradigms 1 and 2: Government-Issued eID

Most government-recognized schemes fall under an eID archetype, supported by fully public governance. However, the treatment of biometric data represents a notable technical difference between many schemes. Paradigm 1, typified by India's Aadhaar and the models in many emerging development programs led by the World Bank, involves the collection and remote storage ("centralized" for the purposes of this paper) of biometric information. This storage of biometrics enables the government to ensure that each individual has only one ID and that resources (e.g., benefits) are flowing to the right people.

It also enables individuals to recover any identity documents that have been lost or stolen because they can be looked up in a database. In this context, the government's central biometric database may be called to act as an authenticator, meaning that the government has visibility into where those Attributes were used. This architecture, therefore, demands heightened privacy rules and data security practices to prevent the impacts of data loss and potential surveillance.

Meanwhile, the architecture of Singapore's Singpass,⁸⁴ Estonia's eID,⁸⁵ and others represented by Paradigm 2 usually involve *local* biometric storage: biometric information stored on a device or machine-readable card controlled by the user. In this latter context, while the government may play the role of "Identity Provider" in a transaction, Authentication (proof that the user is the unique person associated with that identity) happens on a local device. In these contexts, some limits are placed on the extent to which governments can see where individuals are using their identities.

Importantly, [Figure 6](#) shows that many governments whose Digital Identity Systems rely upon more privacy-preserving local (device or smart-card) biometrics also maintain identity systems that store biometric data on citizens and/or non-citizens. This list includes Singapore's NRIC, Estonia's ABIS, and Spain's SIVE systems. Implemented strategically and effectively, these boundaries between systems and the digital identifiers used by individuals in daily life can preserve the confidentiality and integrity of identity data.

However, the boundaries between systems—especially emerging systems—are not always clear-cut or codified into law. In some countries where the legal underpinnings and/or Trust Framework development has lagged behind the Digital ID technical implementation (e.g., India,⁸⁶ Nigeria,⁸⁷ Uganda⁸⁸), privacy advocates have identified significant harms. This disparity is not unlike the United States roll-out of Social Security Numbers without sufficient legislative limits on their use, leading to identity theft.⁸⁹ Without maturing these institutional frameworks, people are at risk of surveillance and other harms. For more on legal and other institutional frameworks, see section 3.2.

IN India's Aadhaar⁹⁰

Description	Aadhaar is the world's largest Digital Identity System and sits beneath a multilayer stack that powers many aspects of the Indian economy ⁹¹
Relationship to Legal Identity	Aadhaar proves uniqueness and residency in India. It is not a guarantee of rights associated with a given Legal Status.
Governance	Unique Identification Authority of India (UIDAI) 2018 Supreme Court Ruling on the use of Aadhaar ⁹²
Year / Maturity	2009 – Highly mature technology; high adoption by citizens and agencies; wide application across the private sector. Implemented with immature institutional frameworks. UIDAI still acts as its own regulator. ⁹³
Volumes	1.2 billion
Biometrics	Yes – centrally stored fingerprints, facial template, iris scan
Services Offered	Universally used across government services Within the bounds of the 2018 Supreme Court ruling, private sector entities can use APIs built on Aadhaar to: <ul style="list-style-type: none"> - Offer financial services products - Obtain and confirm e-signatures - Verify mobile account holders - Conduct KYC - Authenticate employees
Standards and Protocols	XML API ⁹⁴ (much of the Aadhaar protocols were developed in-house)
Highlights	Over 99% of adults enrolled Rs 2trillion (USD\$24billion) state savings over nine years ⁹⁵
Lowlights	<ul style="list-style-type: none"> ● Data breaches of historic scale⁹⁶ ● Reports of government surveillance⁹⁷ ● Reports of Fake ID production⁹⁸

ng Nigeria's National Identification Number (NIN)⁹⁹

Description	The National Identity Management Commission (NIMC), established by the NIMC Act No. 23 of 2007, operates the National Identity Database in Nigeria, registers persons covered by the Act, assigns Unique National Identification Numbers (NIN), and issues General Multi-Purpose Cards (GMPC).
Relationship to Legal Identity	The NIN is required and establishes uniqueness and residency. NIMC refers to tying all information about an individual and using it for "establishing and verifying individual identity." As such, it may also be used to record Legal Status.
Governance	NIMC operates and governs the NIN system Data Privacy Law was signed in July 2023 ¹⁰⁰
Year / Maturity	2007 – less technical information available than Aadhaar but with a similar institutional context (legislative and governance)
Volumes (Individual Identities)	Required for all citizens 16 and over 92.6M NINs issued as of Dec 2022
Biometrics	Yes – fingerprints and facial recognition. Reported proposal to link to national DNA database ¹⁰¹
Services Offered	Integrated across a variety of public, financial, and private services. Required for access to various transactions, including hospitality, health, travel, insurance, financial products, internet access, employment, academia, professional bodies, welfare, property, etc. ¹⁰²
Standards and Protocols	RESTful APIs conformant to OSIA specifications ^{103 104}
Highlights	Improved accuracy of voter rolls
Lowlights	Low early (voluntary) adoption linked to privacy concerns ¹⁰⁵ Government-mandated registration of NIN to SIM cards led to a rise in coronavirus cases ¹⁰⁶

sg Singapore's NRIC and Singpass¹⁰⁷

Description	"Singpass is your trusted digital identity for all the secure transaction needs in your everyday life."
Relationship to Legal Identity	Singpass is a national Digital Identity derived from Legal Identity and accepted by all agencies "except when physical documents are required under legislation." ¹⁰⁸
Governance	Government Technology Agency of Singapore
Year / Maturity	2003 – Singpass launched 2017 – NRIC 2018 – Singpass App linked to NRIC Highly mature technology, usage, and governance
Volumes	4.5m registered users ¹⁰⁹
Biometrics	Yes ¹¹⁰ <ul style="list-style-type: none"> • NRIC requires biometric registration (face, fingerprint, iris) • Singpass registration requires Facial Verification or MFA. • While many Singpass services rely on local, device-based Authentication, public and private entities with a lawful purpose can use the Identiface API Service that matches the database.
Services Offered	2000 services / 700 organizations. The private sector can integrate with the following Singpass APIs: <ul style="list-style-type: none"> • Login • Verification • Signing • Biometric-as-a-service
Standards and Protocols	OAuth2 and DPoP, PKCE, QR (out of band)
Highlights	<ul style="list-style-type: none"> • 97% adoption¹¹¹ • 80% decrease in application time using "MyInfo" service¹¹² • more than 1,400 digital services and empowers over 340 government agencies and private organizations
Lowlights	Some privacy criticism ¹¹³

Italy's Carta di Identità Elettronica (CIE)¹¹⁴ and Sistema Pubblico di Identità Digitale (SPID)¹¹⁵

Description	CIE – electronic identity card SPID is a public Digital Identity System connecting public and private services through a network of private ID providers who vet foundational documents
Relationship to Legal Identity	The CIE conveys Legal Identity and Legal Status and is used in lieu of a passport. The SPID is derived from another form of Legal Identity.
Governance	Regulated by Italian Agency for Digital Identity (AGID) Underpinned by GDPR and NIS2 Security Directive
Year / Maturity	2016 – Mature technology with 50% SPID take-up by individuals and private sector organizations. Mature governance, underpinned by Europe's GDPR, eIDAS, and a framework maintained by AGID.
Volumes (Individual Identities)	30 million / 50% of all adults ¹¹⁶
Biometrics	Local biometrics, when used within local device, are permitted
Services Offered	Relying Party for verified identities Qualified Attributes
Standards and Protocols	SAML2 – for current instance OAuth2 and OpenID Connect – in staging, ready to roll out in 2023
Highlights	Nine IDPs Incentive schemes were used to drive adoption
Lowlights	No negative stories have been identified as yet

Paradigms 3 and 4: Government-Enabled Marketplaces

In some jurisdictions—sometimes in addition to government-issued Digital Identity Credentials—governments have sought to enable (or procure) thriving, privately operated Digital Identity Systems. For example, Bank-based Digital Identity Systems in Nordic countries like Norway, Sweden, and Finland leverage bank Know-Your-Customer (KYC) processes to verify identities and issue a widely adopted, widely used BankID Credential. The government enables these systems by accepting them for various government use cases, and financial regulators oversee their use.

Like the Nordic BankID model, Canada's Interac system (formerly SecureKey) relies upon bank-grade customer identification. With that said, its 'triple blind' technical architecture means that no personal data passes through a central hub to a Relying Party. Instead, it can be used to authenticate an identity already established and proofed securely. The Canadian model further differentiates itself from BankID in that the Digital ID and Authentication Council of Canada (DIACC) receives funding through public and private-sector memberships and works across private industry to develop and maintain a "Pan Canadian Trust Framework" that clarifies technology-agnostic principles and key governance recommendations for Digital Identity Systems in Canada.¹¹⁷

Other government-supported initiatives, e.g., UK Verify,¹¹⁸ sought to create federated or brokered marketplaces for Digital ID. However, several implementations like this one have failed to reach targets (especially adoption) and have undergone a period of re-imagining.

noNorway's BankID¹¹⁹

Description	BankID is used by all the banks in Norway and can be used by organizations and enterprises that are looking for secure and simple identification online
Relationship Digital Identity	Banks verify Legal Identity. Does not confer or convey Legal Status.
Governance	Private governance (BankID Board of Directors) in the context of a strong financial regulator and country-wide legislation covering: <ul style="list-style-type: none"> - Europe's General Data Protection Regulation (GDPR¹²⁰) - Electronic signatures and Trust Services¹²¹
Year / Maturity	2004 - Very Mature technology with a high adoption rate among end users. Mature governance underpinned by strong legislation and enforcement authorities.
Volumes (Individual Identities)	4.3 million
Biometrics	Device-bound biometrics with passkey support are being rolled out ¹²²
Services Offered	IDP is delivered by a private entity that is shared by Banks. RPs are Banks, Government departments, and private businesses
Standards and Protocols	OAuth2 and OpenID Connect
Highlights	Very high acceptance among the population Fraud reduction from 1% to 0.00042%
Lowlights	<ul style="list-style-type: none"> • Not available for services outside Norway and cannot be used to cross borders. • Some concerns about its ubiquity leading to bank Credential sharing (driver for rolling out device biometric support)¹²³

ca Canada's Interac System (formerly SecureKey)

Description	Interac offers a "triple-blind" Sign-In Service (Credential Service Provider) and a Verification Service in which a stateless central hub enables users to login or verify with their bank.
Relationship to Legal Identity	Banks verify Legal Identity. Does not confer or convey Legal Status.
Governance	Pan Canadian Trust Framework ¹²⁴ Underpinned by the Personal Information Protection and Electronic Documents Act (PIPEDA) ¹²⁵
Year / Maturity	SecureKey Technologies was founded in 2008 and matured enough to serve the majority of Canadians banked with all of the largest banks in Canada. It was later licensed by Interac and acquired by Avast (now Gen Digital).
Volumes	200M individual transactions per year, supporting the majority of adult Canadians.
Biometrics	Leverages Bank authentication protocols
Services Offered	Credential Service Provider for Authentication Identity Verification Can be used across government services and verified private entities
Standards and Protocols	The verification service combines mature BankID federation and decentralized technology, ¹²⁶ including Hyperledger Fabric ¹²⁷
Highlights	Very high adoption by banks, users, and government Privacy-preserving technology
Lowlights	No negative stories have been identified as yet

Paradigm 5: The Emerging Wallet-Based Paradigm

While Europe's initial eIDAS legislation fit squarely into Paradigm 2, its emergent evolution represents the final paradigm worth highlighting. Born out of an objective to ensure interoperability and digital accessibility to citizens across the European Union, this new regulation mandates that all Member States issue citizens with a "European Digital Identity Wallet" ("EUDI Wallet"), which can hold both government-issued and other Credentials: a "personal IDP" architecture. Regulators intend to mandate that private entities of sufficient size—including banks and other service providers—must accept these Credentials.¹²⁸ Note that specific privately-led "wallet" offerings, such as those emerging from large technology firms in the US and China, may best fit with Paradigm 5 and have the potential to influence the standards that take hold globally.

While this is the largest scale example, supported by EU-wide legislation, there are multiple efforts around the world. The Kingdom of Bhutan has launched its wallet-based National Digital ID System (NDI)¹²⁹ and there are multiple efforts underway in North America to build wallet-based ecosystems. These efforts include the government of British Columbia issuing wallets and verifiable "Person Credentials" to their citizens,¹³⁰ Green Card issuance by the United States Citizen and Immigration Services (USCIS),¹³¹ and the efforts to standardize and govern Mobile Drivers Licenses (mDL) by the ISO and the American Association of Motor Vehicle Administrators (AAMVA).¹³²

While these are all "wallet-based" ecosystems, it is important to note that they are not the same. There are many emerging standards and technologies in this space. These nascent programs are working to mature variants with significant differences, including trust establishment, communications protocols, and the sharing and storage of data. Furthermore, like all systems, they exist in relation to any given nation's legal foundations for conferring Legal Identity and protections, like Privacy and Data Security.

eu Europe's eIDAS 2.0

Description	To provide EU citizens and residents with a harmonized digital identity and wallet." ¹³³
Relationship to Legal Identity	eIDAS is built on the Legal Identity Systems conferring and conveying Legal Status across the member states.
Governance	eIDAS 1→2 Underpinned by GDPR and NIS2 Security Directive The eIDAS 2.0 legislation is evolving alongside the technical frameworks and pilots.
Year / Maturity	<ul style="list-style-type: none"> • Not yet in force / Large Scale Pilots underway / National initiatives to design or select digital wallets • Moderately mature, grounded in GDPR and NIS2. Still developing scalable models for counterparty trust establishment, maintenance, and revocation.
Volumes	Nascent – four Large-Scale pilots initiated that will touch millions of EU residents
Biometrics	Biometrics may be used for 1:1 matching
Services Offered	Various delivery components and opportunities to rely upon credentials provided
Standards and Protocols See the EU's Architectural Reference Framework for more detail ¹³⁴	W3C VC Data Model ¹³⁵ OpenID for Verifiable Credentials Issuance ¹³⁶ OpenID for Verifiable Presentations ¹³⁷ Self-Issued OpenID Provider v2 ¹³⁸ ISO 18013-5 (mDL) ¹³⁹ SD-JWT ¹⁴⁰ JSON-LD with LD Proofs (optional) ¹⁴¹
Highlights	Visionary approach to end-user control and privacy Broad engagement with industry and standards organizations
Lowlights	Not delivered yet; many details still under review

us United States USCIS Digital Permanent Resident Cards¹⁴²

Description	USCIS administers the United States' lawful immigration system. They are piloting and planning implementation as Verifiable Credentials.
Relationship to Legal Identity	Legal form of Identity pertaining to one type of Legal Status (once obtained). Not yet widely used and accepted.
Governance	USCIS issues green cards and issues these digital green cards under the same existing authority. No national privacy legislation or Identity Trust Framework directly governs this program.
Year / Maturity	2023
Volumes (Individual Identities)	12.9 million people in the United States hold physical Green Cards; ¹⁴³ the digital card program is not yet live.
Biometrics	A photograph is also contained in the digital version of the green card. When people apply for green cards, their photo and fingerprints are taken and stored in the government's system.
Services Offered	Digital Green cards are issued and will be accepted at the border. Those cards can be used for other identity uses by the holders.
Standards and Protocols	National Institute of Standards and Technology (NIST) guidelines W3C VC Data Model ¹⁴⁴ and W3C DID Core ¹⁴⁵ VC-API to connect to existing government systems Credential Handler API to transmit and receive Credentials
Highlights	<p>Department of Homeland Security Science and Technology Directorate helped fund the development of the core DID and VC Data Model Standards. Now supporting Conformance Testing amongst vendors.</p> <p>Support for Individual Privacy</p> <ul style="list-style-type: none"> • Architecture prevents government tracking where the ID is used • Enabling selective Attribute disclosure • Enabling individual awareness of Verifier use of issued credentials <p>Support for a Competitive Ecosystem and Individual Choice</p> <ul style="list-style-type: none"> • Choice of identifiers for individuals • Choice of wallets for individuals
Lowlights	Not delivered yet; many details still under review

usca North American Mobile Driving License (mDL)








as led by the American Association of Motor Vehicle Administrators

Description	While neither the US nor Canada has a single national identity system, they collaborate on the standards for administering driver's licenses, including efforts to put mobile driver's licenses into a device wallet.
Relationship to Legal Identity	Driver's licenses are widely accepted forms of government-issued identification but do not convey Legal Identity or Status.
Governance	AAMVA
Year / Maturity	The National Institute of Standards and Technology has been running mDL pilots since 2016 ¹⁴⁶ (ISO) standard for the mobile driving license (ISO 18013-5) was approved on 18 August 2021 and published on 30 September 2021 The States with conformant mDL credentials accepted by TSA are Arizona, California, Colorado, Georgia, Iowa, Maryland, and Utah (as of September 2023).
Volumes (Individual Identities)	Data not available
Biometrics	Driver's picture is shared with agent or officer checking license
Services Offered	Intended for use as an entitlement to drive and ID card primarily for law enforcement and airline travel contexts.
Standards and Protocols	ISO 18013-5 NIST guidelines
Highlights	Mobile driver's licenses enhance user experience, especially when presented in digital and app-2-app channels. However, it raises privacy and vendor lock-in concerns that must be addressed. ¹⁴⁷
Lowlights	ISO18013-5 mDL standard covers in-person presentation. Standards for online presentation, such as ISO 18013-7—which profiles OpenID for Verifiable Presentations—and related work on the Browser API, are immature and require incubation. Meanwhile, some wallets are creating their own presentation models, leading to concerns about <ul style="list-style-type: none"> • vendor lock-in • how the governance model will prevent wallet providers from accessing, storing, or tracking PII • data correlation by browsers and third-party verifiers online

Key Considerations

Digital Identity Systems, like all technologies, carry the potential for misuse, abuse, and poor implementation. As pointed out in Part One, they are also infused with a set of values that determine their outcomes (intentionally or unintentionally). Governments need to strategically explore the risks, mitigations, and trade-offs of any project with respect to its goals (which this paper argues should be centered around sustaining and promoting Human Rights). Thinking systemically, this includes designing for different use cases and, in particular, the higher-stakes contexts within which individuals and legal entities rely (or may come to rely) upon the exchange of Digital Identity data. In order to protect people and prevent harm, it is critically important to consider how foundational Legal Identity Systems, functional government-issued Digital Identity Systems (e.g., mobile driver's licenses), and Digital Identity Systems derived from government-issued ID (e.g., BankID) should interact to support those use cases and contexts.

Table 3: Indicative Trade-offs by Stakeholder Type (not a comprehensive list)

Stakeholder	Salient Needs	Trade-Off
 <p>General Public</p>	<ul style="list-style-type: none"> • Access rights and services associated with my Identity, including, but not limited to, Legal Status • Prove trustworthiness • Prevent fraud identity theft • Transparency and auditability • Control over personal data • Broad protections over how data is collected and used to affect human behavior 	<p>Ease of use vs. security and privacy</p> <p>Data minimization vs. data collection (e.g., to combat fraud)</p> <p>Data destruction vs. data retention (e.g., for audit purposes)</p>
 <p>Children</p>	<ul style="list-style-type: none"> • As Above • Parent/ Guardian association, delegation, and revocation • Prevent additional harms, e.g., through age assurance online 	<p>Data minimization vs. data protection</p>
 <p>Undocumented & Stateless</p>	<ul style="list-style-type: none"> • Legally recognizable ID • Recoverable ID 	<p>Inclusion vs. controlled access</p> <p>Inclusion vs. privacy and data minimization</p>
 <p>Family Migration</p>	<ul style="list-style-type: none"> • Interoperable ID and cross-border recognition of Legal Status • Irrevocable family relationships 	<p>Interoperability vs. privacy and data minimization</p> <p>Irrevocability vs. flexibility</p>
 <p>Under Threat (various contexts)</p>	<ul style="list-style-type: none"> • Process to determine Legal Status, including as a Refugee • Private sensitive data • Private day-to-day activities • Identity replacement 	<p>Privacy vs. access</p>
 <p>Disability & Carers</p>	<ul style="list-style-type: none"> • Accessibility and support • Delegation and revocation 	<p>Privacy, access, counter-fraud all may exist in tension</p>
 <p>Legal Entities</p>	<ul style="list-style-type: none"> • Combat fraud • Receive data to verify users • Protect data • Comply with regulation 	<p>Data collection and retention (especially for counter-fraud) vs. Data minimization and destruction</p>

Recognizing the different needs of users in the system demands values-based trade-off decisions, as well as defining design, roll-out, and operational strategies that will mitigate the risks of any given trade-off. These decisions must consider the institutional rules accompanying the technical design choices and how they will be controlled and enforced. For example, codifying legal boundaries that limit who can see and store identifiers enables network participants, technologists, and standards architects to understand the boundaries within which they must operate technically and procedurally. To mitigate risks requires that legal, enforcement, and governance frameworks keep pace with technology (in addition to evolving socio-cultural norms).

Of course, “trade-off” should not imply a binary choice. Instead, designers need to decide where to place emphasis, and today’s emerging standards and technologies enhance implementers’ flexibility and range of motion available within each scale. As new tools emerge, however, so do the threats: for example, technologies that improve biometric capture and increased storage capacity heighten the risk of biometric identity theft and the unprecedented impacts that this could have on people. Appendix A shows other examples of how advances in some areas created new technical challenges elsewhere in the stack. Implementers must continuously assess their threat models and incorporate best-available countermeasures. Today’s simplest technological and architectural risk-mitigation strategies include things like:

- Encrypt as much as possible at rest and in motion, especially information that could be used to identify a unique individual
- Biohashing or other encryption processing to protect biometric data (if stored)
- Adherence to modern FIDO 2 (and evolving) standards
- Unique identifiers per Relying Party or Third-Party Verifiers help to avoid correlation of data
- If a central hub for Authentication exists, it should be stateless and never store personal information at rest

The next section explores and consolidates the literature that seeks to guide governments on how to make values-based or principles-based trade-off decisions in the implementation of rights-affirming Digital Identity Systems.

Part 3: Recommendations for Digital Identity Systems

A Unified Set of Principles

The body of literature around government-issued ID and government-led ecosystems coalesces around several key themes that align with the findings of this paper (see [Appendix B – Aligning Digital ID Principles](#)). This literature grounds itself in human rights and democratic ideals; in so doing, it suggests that governments should take a strategic, human-centric approach that carefully weighs the risks and trade-offs inherent in any system.

In particular, this paper endorses the 2023 OECD Recommendation of the Council on the Governance of Digital Identity,¹⁴⁸ which unifies much of that literature (see also [Appendix C – OECD Digital Identity Recommendations as a Checklist](#)). This chapter builds upon the pillars of the OECD’s comprehensive work, as well as inputs from prior influential works, including ID2020,¹⁴⁹ the World Bank’s ID4D,¹⁵⁰ the World Economic Forum,¹⁵¹ OIX Guide to Trust Frameworks for Smart Digital ID,¹⁵² and mature Trust Frameworks, such as that of DIACC.¹⁵³ Rather than develop a new framework, this paper makes specific recommendations for deeper engagement on crucial themes around which these principles-based models converge ([Figure 7](#)).



Figure 7: Recommendations by Theme and Aligned to OECD Pillars

The following recommendations bring the latest literature together in order to deepen the discussion of ‘How’ a government can deliver on these principles. A final summary is presented in [Table 5](#).

Pillar 1: Human-Centricity

Design is everywhere, design is power, and design is political.¹⁵⁴

To promote Human Rights and human thriving through Digital Identity Systems, governments need to recognize, as suggested by the definitions offered in [Part 1](#), that “Identity” is a context-dependent idea. In some cases, especially to organizations, it may be helpful to consider it relatively discrete and static (i.e., any individual has one recognizable identity to manage access). In other contexts, where people relate to countless individuals and entities over time, “Identity” is dynamic and relational. Part 1 argued that prevailing organization-centric technology and legal frameworks have led to (or failed to prevent) real harms to people and communities. Since the Augmented Social Network called for user-centric Digital Identity Systems in 2003, many more have advanced similar ideals.¹⁵⁵ Information systems, social science, and development scholars have called for a global approach that addresses data justice.¹⁵⁶ The November 2022 report by the Digital ID and Authentication Council of Canada (DIACC) and Human Technology Foundation (HTF)¹⁵⁷ refers to the process by which governments design identity solutions and includes a set of Human-Centric principles, many of which align with those promoted by other advocacy groups, such as ID2020,¹⁵⁸ ID4D,¹⁵⁹ Women in Identity,¹⁶⁰ the World Economic Forum,¹⁶¹ and organizations such as Trust over IP Foundation¹⁶² and MyData Global.¹⁶³ Most recently, the OECD recommendations place the needs of real humans and society, including the businesses and other services reliant upon identity technology, at the forefront.¹⁶⁴ Building upon the Human Rights foundations recommended in Part 1, this paper recommends an inclusive, value-sensitive approach to Human-Centered Design underpinned by standards.

A Human Rights Foundation

[Part 1](#) argued that, given the high stakes, governments should design Identity Systems (including Digital Identity Systems) and Ecosystems with an expressed purpose of sustaining and promoting Human Rights, whether or not other benefits present a meaningful driving force as well. To do so requires analyzing the risks and opportunities in relation to established Human Rights Frameworks. As such, any exploration of Digital Identity Systems must be considered within the context of their relationship (or potential relationship) to Legal Identity, Legal Status, and Civil Registration.¹⁶⁵ All of these concepts are naturally bound and yet must not be conflated.

The concepts are bound because any such analysis must include Article 6 of the Universal Declaration of Human Rights (right to legal recognition)¹⁶⁶ and Sustainable Development Goal 16.9 (Legal Identity for all), both of which focus on Legal Identity. Furthermore, such an analysis should also consider how Identity Systems (including Digital Identity Systems) can support any and all obligations in the Covenants and Treaties that comprise the international Human Rights frameworks that exist, now and in the future. These legal frameworks include, for example, the Convention Relating to the Status of Refugees,¹⁶⁷ treaties on Statelessness,¹⁶⁸ witnesses,¹⁶⁹ and the Declaration of the Rights of the Child.¹⁷⁰ The analysis should begin with the bodies of work available at the United Nations, including those cited above, and particularly with their Guidelines on the Legislative Framework for Civil Registration, Vital Statistics, and Identity Management Systems.¹⁷¹

Human-Centered Design

In order to achieve governments' rights-affirming goals, the people who will use the system (as well as other societal stakeholders, such as legal entities) need to play a central role in an open, iterative, and trustworthy Digital Identity System design process.¹⁷² Ultimately, this helps to ensure that it is fit for purpose, since such systems may fail to achieve the level of adoption that warrants investment. For example, the UK Parliament recently shut down the GBP 154M Gov.UK Verify program, citing one-sixth of the expected take-up and a 38-50% successful sign-up rate.¹⁷³

Human-Centered Design (HCD) is "a discipline of developing solutions in the service of people."¹⁷⁴ This paper has adopted "Human-Centered" as opposed to "User-Centered" or "Person-Centered" because it conveys a breadth in scope that the others may not (although, as with many terms used in this paper, it may depend on how they are defined in context). Rather than a sole focus on a user interface (and rather than a sole focus on the target user), for example, an HCD process aims to achieve positive outcomes systemically and across many stakeholder communities.¹⁷⁵ In a 2004 article, HCD scholar Klaus Krippendorf argues that HCD is concerned with "enabling many individual or cultural conceptions to unfold into uninterrupted interfaces with technology."¹⁷⁶

The process itself, which may be deployed with the support of many methods and tools not described in this paper, demands broad inclusion and deep engagement to build empathy for those who will rely upon the system. Prototype development and iterative design-test

sprints bolster and extend that understanding. This process informs not just the user experience design but also the set of choices offered (“one size does not fit all”¹⁷⁷), risk analysis, risk mitigation, and trade-off decisions. It enables implementers to challenge assumptions and gather real insights about what will drive adoption and use. For example, UK researchers found that 70% of supermarket shoppers preferred to prove age via an anonymous facial scan over a Reusable Digital ID.¹⁷⁸ Furthermore, HCD considers scenarios in which things go wrong—the “unhappy paths,” like redress mechanisms for fraud and identity theft.

Inclusive

While Digital Identity Systems promise to simplify processes and enhance benefits, they must be designed to include communities with different needs—throughout their lives and accounting for change. As pointed out by McKinsey, inclusive access to Digital Identity Systems may create tremendous opportunities for people.¹⁷⁹ Persona development, such as those cited in Ernst and Young’s *Connected Citizen Report*, can help.¹⁸⁰ However, as pointed out in [Table 3](#), there are many for whom the wrong solution could deepen disparities, increase exclusion, or create tools of oppression.

The OECD includes consideration for vulnerable populations, including those that cannot or choose not to use the options proffered by government.¹⁸¹ The Secure Identity Alliance, in a 2021 report, highlighted several noteworthy examples of broad engagement leading to inclusive practices, including innovative identity solutions designed for careers in France, people unwilling or unable to adopt government-recommended technologies in Azerbaijan, and wallets for domestic violence survivors in Australia.¹⁸² “The Human Impact of Identity Exclusion” points out that many such populations often face seemingly insurmountable challenges when replacing documents or accessing well-intended Identity Systems. These problems lead to economic exclusion and lack of access more broadly.¹⁸³ To truly represent the rights of all, implementers must design for the full range of human experience, accounting for—even beginning with—marginalized communities and “edge-case” scenarios. These populations must be identified and engaged early in an HCD process.

Box 2: Champion Use Case Examples

The global community has many opportunities to leverage Digital Identity technologies to provide access and inclusion at scale. This paper recommends including some of the most complicated “champion” use cases and defining how such technologies can bolster Human Rights in those contexts – and where the Legal Identity and institutional frameworks would need to evolve.

Family Relationships

The bond between family members, e.g., a parent’s relationship with their child, and/or caregivers is universally applicable - and universally complicated (known as “Delegation”). In the physical world the emotional parent-child “bond” is well understood. However, mechanisms to assert that bond are broken, inadequately served by current standards and frameworks. Countries struggle to deploy their own child-protecting policies.¹ This issue is fraught: fraud, abuse, consent, and control risks abound. As a result, there remain barriers to a parent or caregiver’s ability to enroll in and access services. Collaborating to solve this issue as a “champion” use case could unite organizations in serving families and address long-standing problems.

Between Borders

Much Identity literature focuses on how Digital Identity Systems support citizens and established residents. This, arguably, assumes good intentions towards vulnerable populations within its citizenry: however, millions of stateless and effectively stateless populations (those whose governments oppress them, seek to assimilate them, or abdicate responsibility for their human rights) do exist. Given the UN Declaration on Human Rights applies to all,¹ this paper would be remiss if it did not recommend that governments cooperate internationally to develop accessible and interoperable identification systems for such people. Critically, such an effort must enable these individuals to obtain a recognized Legal Status and participate in the global economy.

Value-Sensitive Design

As implied by the definition of HCD above, ease-of-use and adoption are important but insufficient goals for the system:¹⁸⁴ such a narrowly focused process may lead to the adoption of systems that undermine the interests of people,¹⁸⁵ as seen in algorithms that promote “sticky” misinformation¹⁸⁶ or third-party applications screen scraping bank account data.¹⁸⁷ Instead, the ecosystem must also protect people and communities, bolstering their rights in the face of harms they may not recognize or control. For these reasons, it is also essential that this HCD process surfaces values, guides trade-off decisions, and aims to strengthen governance (in addition to deploying usable, useful

technologies). Embedding Value-Sensitive Design research and practice, therefore, offers a helpful complement and ensures the HCD process will surface the correct information.¹⁸⁸

Embedding values into an ecosystem's design and delivery is not a simple task.¹⁸⁹ With that said, scholars are modifying VSD tools to support the needs of emerging technologies, like Artificial Intelligence.¹⁹⁰ [Table 4](#) outlines some considerations.

Table 4: Value-Sensitive Implications on the HCD Process

Phases of Human-Centered Design	Implications of Value-Sensitive Design
<p>Who are we reaching? Stakeholder Mapping Setting HCD Objectives for Communities Developing Personas</p>	<p>Broad, cross-societal stakeholder groups</p> <p>Multi-disciplinary researchers</p>
<p>What do we need to know? Gathering Existing & New Insights Journey Mapping</p>	<p>Qualitative research methods designed to surface values and tensions</p>
<p>Identifying Barriers and Opportunities Rapid Inquiry Synthesizing Information</p>	<p>Identify areas where value tensions need to be negotiated and managed technically, procedurally, legally, or otherwise</p>
<p>Ideas and Prototyping Generating Ideas Building Prototypes</p>	<p>Embed values into requirements</p> <p>Document negotiation strategy</p>
<p>Measurement & Improvement Piloting & Iterating</p>	<p>Research methods to assess (and address) the “embodied” values of a delivered pilot or program</p>

See Endnote ¹⁹¹

This process aims to ensure that the Digital Identity System underpins a balanced set of values that ensures the technologies enhance the capabilities of real people to engage in their world.¹⁹² Notably, it goes beyond naming a broad set of values and towards identifying requirements and using values to negotiate inevitable trade-off decisions.

Human-Centric Standards

Open and robustly developed standards have the power to mature technologies and institutions such that they meet the needs – and underpin the values – of society. However, they will reflect the values of the working groups that develop them. The non-profit organizations and working groups leading the standardization of Identity Systems must be globally diverse and inclusive in order to develop robust and equitable standards that reflect all of society. Such bodies need to recognize and convey this ambition.

Governments can help by engaging directly: they should support standards bodies in their mission, collaborate, and make their needs known so that working groups can meet them. For example, to deliver on a “champion” use case (e.g., the “digital bond” between parent and child cited above), standards bodies need to understand requirements from not just the most active participants (often large, private entities in the global north), but also from government stakeholders and multi-lateral institutions, especially in the global south. In the sections that follow, specific attention will be paid to organizations, working groups, and families of standards that promote critical aspects of Identity Ecosystems grounded in Human-Centric values: security, privacy, interoperability, and strong governance.

There are two global efforts emanating from the identity industry that are specifically working towards the development of guidelines for Identity Systems seeking to include marginalized populations: Women in Identity is developing an international Code of Conduct for Identity Inclusion,¹⁹³ and ID2020 is focused on promoting the rights of migrants, stateless people, and those whose rights are under threat.

Recommendations for Delivering Human-Centric Identity Systems

1. Develop and maintain a Human Rights Analysis of identity systems, including the role that Digital Technologies play in addressing gaps and promoting rights.
2. Broad, inclusive engagement of Identity Ecosystem stakeholder groups.
3. Follow a Values-Sensitive HCD process that reflects the risks and benefits to stakeholder groups and begin with a core value set.
4. Define values-based trade-off decisions and risk mitigation strategies
5. Work with standards bodies to mature standards that achieve these values-based priorities
6. Engage, specifically, with the Women in Identity Code of Conduct and ID2020 to ensure that identity systems are designed with vulnerable and marginalized populations in mind
7. Collaborate on "champion" use cases that will sharpen user requirements at scale, and enable global collaboration on interoperable digital identity infrastructure (e.g. the "digital bond" between parent and child, stateless people, etc.)

Pillar 2: Strategic Design and Governance

“Systemic problems, if addressed structurally, can be ameliorated far more readily than countless scattered problems.”¹⁹⁴

While there are many approaches to Digital Identity technical architecture and governance that can work, [Part 2](#) establishes important trade-off decisions that must be made and mitigated to avoid the unintended consequences articulated in [Figure 2](#). Given the complex nature of government and Identity Systems’ role in society, the OECD recommends a coordinated and strategic approach to designing Digital Identity Solutions. The Human-Centric design process recommended above will surface the values that inform the Ecosystem goals and strategy. From there, governments need to craft layers of institutional support that guide the technology, roll-out, and ongoing operations of Digital Identity

Systems (see [Figure 8](#)). These, of course, are built on the foundation of Human Rights Frameworks and those laws governing Legal Identity and Legal Status.



Figure 8: Layers of Institutional Frameworks to Strengthen Governance

These layers include bolstering (or designing) the legal foundations, defining a Trust Framework, and ensuring strong ongoing governance.

Legal Foundations

One limitation of the OECD recommendations is that they pre-suppose conditions under which Legal Identity, data security, data protection, and privacy laws exist and are fit for purpose; this assumption does not always hold true. Yet, as articulated in [Part 2](#), these legal underpinnings are critical in mitigating the risks inherent in any Digital Identity Ecosystem – and preventing the harms or Human Rights Issues arising from flawed Legal Identity institutions and infrastructure.¹⁹⁵ These foundations, therefore, must keep pace with technology as it emerges. This includes applying existing standards in new contexts as well as creating new ones.

With respect to data security¹⁹⁶ and privacy laws in particular,¹⁹⁷ scholars have called for human-centric approaches to designing governance systems and institutional protections. Many argue that the legal foundations underpinning emerging technologies, including Digital Identity Systems, fail to adequately protect individuals and adopt a reading of human rights fit for the current age. In her cutting-edge book, “Beyond Data,” Elizabeth Renieris argues that even the most advanced privacy legislation in the world, arguably Europe’s General Data Protection Regulation (GDPR), places too much of a burden on individuals to exercise control over their data when the repercussions of mass anonymized/pseudonymized data ingestion into emerging technologies creates unforeseeable—at least to the average person—implications for society as a whole. In order to protect against harms like algorithmic bias or mass manipulation,¹⁹⁸ society would benefit from a modern reading of human rights law in relation to emerging technology.¹⁹⁹

With that said, there are things that legislators can achieve alongside and in parallel with international efforts to redefine human rights for the post-digital age. Scholars Solove and Hartzog argue that modern security legislation emphasizes post-breach investigation and culpability to the detriment of incentivizing systemic prevention.²⁰⁰ They assert that the law can better protect people with a holistic approach that makes privacy-by-design and security-by-design essential business practices. Such foundations would minimize the unintended consequences of quick fixes and point solutions.

Drawing upon the works referenced below (especially Renieris, Solove, and Hartzog), this paper makes two recommendations in terms of the legal foundations of Identity Ecosystems:

1. Building upon Recommendation 1 (see above), governments must take steps to define how legal frameworks must adapt in order to underpin the human rights agenda with respect to emerging technology in collaboration with international governance, human rights organizations, civil society, academia, and the private sector.
2. Evolve national privacy and security legislation to assure these rights and establish flexible guidelines that demand organizational data stewardship and adoption of the most appropriate privacy and security measures available to them.

Trust Framework

While privacy and security law are critical underpinning components of strategic Digital Identity Systems, they alone are not sufficient in upholding the intended set of values. Since treaties and laws rightfully take longer to change, it is likely correct that they avoid overly prescriptive requirements. However, given the potential risks and benefits across sectors and all of society, nations are increasingly recognizing Digital Identity Systems as critical state infrastructure requiring dedicated guidelines and independent oversight.²⁰¹ This is why the OECD principles specifically recommend the development of a robust Trust Framework informed by the human-centered requirements defined by their stakeholders. As defined by the Open Identity Exchange in their *Guide to Trust Frameworks*, this is where ecosystem-specific principles, roles, rules, and obligations are defined to feed into an ongoing governance and enforcement model (see [Figure 9](#)).²⁰² Such frameworks should be detailed but flexible: they are designed to complement the legal and regulatory foundations upon which they are built. Furthermore, they provide crucial inputs to the contracts and technology requirements that will underpin operations.

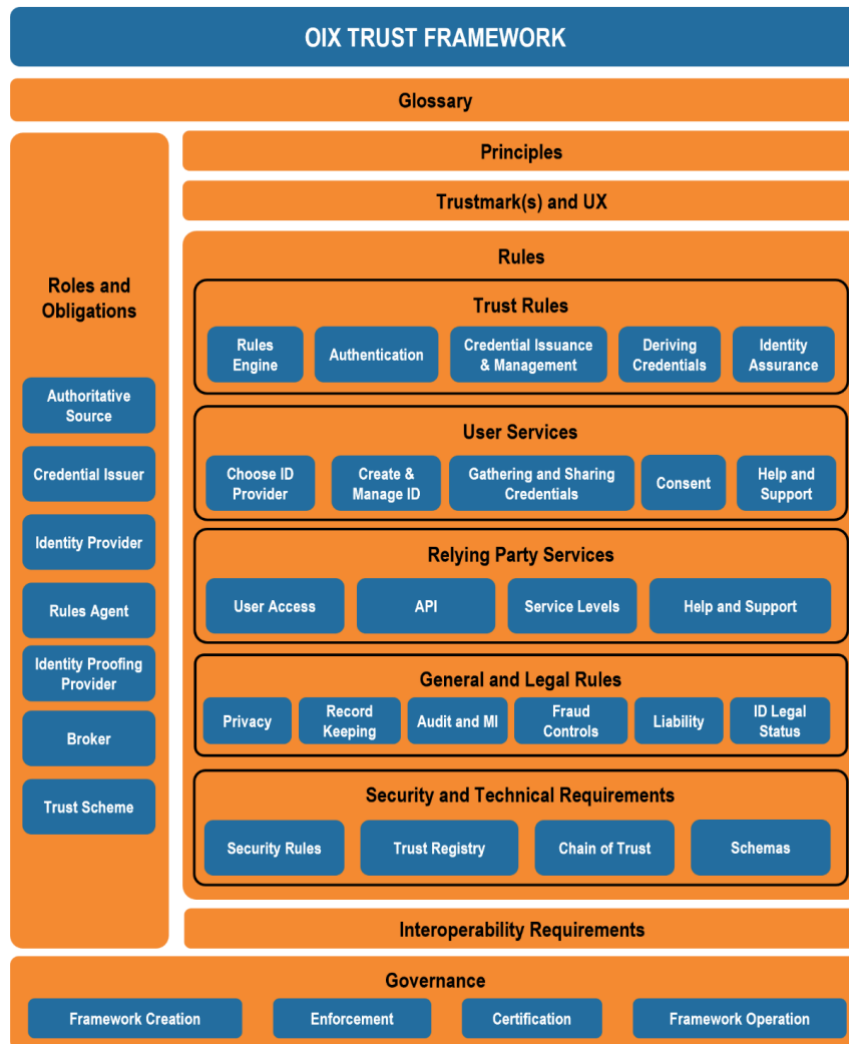


Figure 9: OIX Guide to Digital Trust Frameworks (Source: OIX²⁰³)

Increasingly, nations are developing Digital Identity Trust Frameworks as a public-private collaboration, citing the need to build strong Identity Ecosystems that empower citizens and support a thriving private sector.²⁰⁴ For example, Canada’s Pan-Canadian Trust Framework (PCTF) is a body of work developed in partnership with private entities and government officials alike: it provides guidelines for many different types of Digital Identity Systems and architectures. Despite having very different architectures, for example, operators of the wallet-based British Columbian ID ecosystem and the bank-based Verified.me Ecosystem operated by Interac both participate in DIACC and drive the PCTF.

While this effort requires commitment and investment, the effort can spawn multiple Identity Ecosystems that innovate within the bounds of an agreed set of values.

It is important to note that these agreed values should permeate all aspects of the Trust Framework, including how the system is rolled out and managed/evaluated over time. Well-intended Systems have had negative consequences for individuals in roll-outs that were, arguably, misaligned to intended values. For example, there have been reports of Ugandan citizens losing access to medical care or age-related benefits as a result of National ID mandates that preceded full roll-out and failed to adequately deal with previously undocumented people.²⁰⁵ Further examples of unintended harms can be found in “Paving a Digital Road to Hell” by the Center for Human Rights and Global Justice.²⁰⁶ This is why the Centre for Internet and Society recommends rights-based, rules-based, and risks-based checks in evaluating the comprehensiveness of the Trust Framework.²⁰⁷ Finally, ongoing analysis of the costs and benefits accrued to citizens and all stakeholders post-implementation should be carefully designed (according to the Values elicited in the HCD process) and carried out to ensure that the Ecosystem continues to perform as intended.²⁰⁸

Recommendations for Strategic Design and Strong Governance

1. Collaborate internationally to interpret the UN's Human Rights covenants for the post-digital era and, in turn, evaluate how well existing legal frameworks address this interpretation
2. Build or evolve national and regional privacy and security legislation to assure these rights and requires organizational data stewardship via privacy-by-design and security-by-design best practices
3. Treat Digital Identity as Critical Infrastructure that requires a national, supra-national, and sub-national strategies (and associated investment) as appropriate
4. Invest time and resources into public-private collaboration on a Digital Identity Trust Framework, supported by OIX, that transforms prioritized Human Centered Values into Ecosystem guidelines
5. Include aspects of Ecosystem Design, Implementation, Management, and Evaluation into the Trust Framework

Pillar 3: Secure and Privacy-Protecting Identity Systems

Pillars 3 and 4 reflect that all of the principles-based literature on Digital Identity Systems place high value on Security, Privacy, and Interoperability. This section briefly articulates further resources in relation to Security and Privacy, which are complex topics and the subject of many other dedicated papers, textbooks, etc.

Data Security underpins all of the intended benefits of Digital Identity Systems. This includes benefits to individuals, groups and communities, private entities, and government actors: anyone with an identity or the need to verify one. Given this dependence on identity integrity—particularly viewed alongside the vast public and private interdependencies inherent in any supply chain—security is now a fundamental component of Corporate

Social Responsibility (CSR).²⁰⁹ Government officials must take great care to ensure that institutional frameworks, in the form of legislation and Trust Frameworks that will guide Digital Identity Systems, create privacy and security incentives for all actors in the ecosystem.²¹⁰ Europe's NIS2 Directive²¹¹ may yet serve as a template for legislation, and the United States NIST draft SP800-63-4 provides a comprehensive framework for securing identity systems.²¹² Readers interested in this topic are advised to begin there.

While security is inherently linked to privacy, the two are not the same: security is how an organization's assets, including data, are protected, while privacy concerns the collection, processing, and storage of data in the first place.²¹³ The two can be in conflict. For example, combating fraud and cybercrime requires the identification of actors and, sometimes, the holding or sharing of data regarding suspicious activity. These tensions must be balanced at multiple levels, including (but not limited to) the legislative and Trust Framework levels (indeed, NIST draft SP800-63-4 seeks to do this) and mitigated through policies, procedures, technical controls, etc., wherever necessary.

The OECD has developed a set of Privacy Principles²¹⁴ as a best-practice starting point in balancing these needs. They cover eight topics, which are aligned to those set out in Article V of Europe's General Data Protection Regulation (GDPR)²¹⁵ as well as the 2018 Council of Europe Convention 108 for the Protection of Individuals with Regards to the Processing of Personal Data, which any country can ratify:²¹⁶

1. Collection Limitation
2. Data Quality
3. Purpose Specification
4. Use Limitation
5. Security Safeguards
6. Openness
7. Individual Participation
8. Accountability

[Appendices D-E](#) include Bodies and Working Groups developing secure, privacy-enhancing Digital Identity standards to support implementations around the world. For readers interested in a deep dive into the privacy considerations of emerging Digital Identity Systems, we recommend reading the sister paper to this one, "Government-Issued Digital

Identity Credentials and the Privacy Landscape,” which explores these specific issues in terms of global laws, implementations, gaps, trade-offs, and clear recommendations to close or remediate known issues.

Recommendations for Security and Privacy

1. Further the notion that data security is a fundamental part of Corporate Social Responsibility and must factor into all processes (e.g., development and procurement processes).
2. Refer to existing best practice documentation, including (currently):
 - a. Legislation: Europe’s NIS2 and GDPR
 - b. Trust Framework: NIST SP800-63-4
 - c. Privacy: OECD Privacy Principles, GDPR, and the Council of Europe’s Convention 108
3. Read “Government-Issued Digital Identity Credentials and the Privacy Landscape” to review risk and approaches not yet addressed by current laws and best practice.
4. Ensure that security protocols selected have been tested using formal security analysis methods and any weaknesses have been addressed.
5. Ensure that ecosystem participants have clear, empirically measurable, and mandatory certification and conformance processes to ensure the desired outcomes are achieved in practice.

For further reading on recommendations 4 and 5, see the University of Stuttgart’s Web Infrastructure Model²¹⁷ and NIST’s overview of Conformance Testing.²¹⁸

Pillar 4: Delivering International Interoperability

Given that Digital Identity Systems underpin relationships within and across ecosystems and governments, principles-based Digital Identity literature aligns with promoting cross-sector, cross-border interoperability. This means defining not only how a person relates to a given government but also how—and the boundaries within which—government systems enable trusted relationship lifecycles (establishment, maintenance, termination, and revocation) in other domains.²¹⁹

Standards for Interoperable Ecosystems

To deliver on these goals requires both technical and semantic interoperability (in addition to legal and organizational interoperability)²²⁰ in areas such as:

- Mutual trust establishment between ecosystem entities
- Identification of individuals, entities, and devices (although the latter two are not the primary focus of this paper, they require identification and interaction with – or on behalf of – human identities)
- Standardized interfaces at the protocol level
- Aligned existing national and supra-national identity assurance standards and policies
- Harmonized data and meta-data (information content and format)²²¹
security practices and configurations

In pursuit of interoperability, organizations have begun to come together in order to align efforts through the stack. The Trust Over IP Foundation is seeking to create common standards for internet trust using decentralized technologies.²²² The non-profit MyData Global has worked with entities on a “journey of interoperability” with personal data since 2019.²²³ Further, the non-profits guiding the Global Assured Identity Network are collaborating to bridge existing trust ecosystems, establish strong methods of assuring counter-party trust, and semantically harmonize trust and policy frameworks.²²⁴ Additional efforts are listed in [Appendices E-F](#).

Governments have a critical role in catalyzing the development of Open Standards and mandating certification to enable interoperability across these layers. For example, the European Union’s Architectural Reference Framework²²⁵ is actively supporting the maturation of emerging families of standards, such as OpenID for Verifiable Credentials,

that meet the values-based priorities required by their strategy, and they are contemplating the path to conformance and certification to underpin their goals. Similarly, the Silicon Valley Innovation Program (within DHS Science and Technology) has played a powerful role in shaping the W3C Credentials Community Group roadmap. Specifically, it has led to continuing development and increasing maturation of Citizenship and Traceability Vocabularies, JSON-LD, and LD Signatures for Verifiable Credentials. Direct collaboration (i.e., unmediated by vendors) promises to reduce costs to government, minimize vendor lock-in, heighten security, and encourage swift progression towards safer, more effective (i.e., mature) systems that underpin the values and goals unearthed in a Value-Sensitive HCD process.

An important point to emphasize is the role of certification and conformance: all the best standards and policies become irrelevant if participants in the Ecosystem are not mandated to conform to them. Such an Ecosystem is vulnerable to the security, privacy, and interoperability risks that the standards and policies are designed to mitigate. While conformance testing alone is not a panacea, it is an essential tool.

Like the examples above, and as recommended by the OECD, this paper urges governments to develop these as **Open** Standards. This transparent approach ensures long-term Ecosystem stability and sustainability.²²⁶ In short, governments will deliver more benefits more quickly through ongoing direct engagement with and support for Open Standards communities developing identity solutions (see Appendix [Appendices D-E](#)).

Recommendations for Interoperability

1. Promote the development of aligned policy frameworks and technical standards.
2. Share priorities and engage directly with Open Standards communities in order to mature the standards that address those priorities.
3. Participate in Open Standards in order to heighten public-private collaboration, increase transparency and trust, and speed the process to maturity.
4. Introduce mandatory certification and conformance testing to key ecosystem standards and policies.

Conclusion and Summary

The opportunities afforded to societies and their governments by Digital Identity Systems are vast; the complexities and the risks match them in scale. It is through human-centered collaboration—embedding core values within every layer of technical and institutional design—that governments will deliver Digital Identity Ecosystems that sustain and promote human rights.

Table 5: Summary of Recommendations

Pillar 1: Human-Centric Identity Systems
Develop and maintain a Human Rights Analysis of identity systems, including the role that Digital Technologies play in addressing gaps and promoting rights.
Broad, inclusive engagement of Identity Ecosystem stakeholder groups
Follow a Values-Sensitive HCD process that reflects the risks and benefits to stakeholder groups and begin with a core value set.
Define values-based trade-off decisions and risk mitigation strategies
Work with Standards Bodies to mature standards that achieve value-based priorities
Engage, specifically, with the Women in Identity Code of Conduct and ID2020 to ensure that Identity Systems are designed with Vulnerable and marginalized populations in mind
Collaborate on “Champion” use cases that will sharpen user requirements at scale and enable global collaboration on interoperable Digital Identity infrastructure (e.g., the “digital bond” between parent and child, stateless people, or others)
Pillar 2: Strategic Design and Governance
Collaborate internationally to interpret the UN’s Human Rights covenants for the post-digital era and, in turn, evaluate how well existing legal frameworks address this interpretation
Build or evolve national and regional privacy and security legislation to assure these rights and require organizational data stewardship via privacy and security by design best practices
Treat Digital Identity as Critical Infrastructure that requires national, supra-national, and

sub-national strategies as appropriate
Invest time and resources into public-private collaboration on a Digital Identity Trust Framework, supported by the OIX guide, that transforms prioritized Human Centered Values into guidelines across the Ecosystem
Include aspects of Design, Implementation, Management, and Evaluation into the Trust Framework
Pillar 3: Secure and Privacy-Protecting Identity Systems
Further, the notion that data security is part of Corporate Social Responsibility and must factor into all processes (e.g., development and procurement processes).
Refer to existing best practice documentation, including (currently): <ul style="list-style-type: none"> • Legislation: Europe’s NIS2 and GDPR • Trust Framework: NIST SP800-63-4 • Privacy: OECD Privacy Principles, GDPR, and the Council of Europe’s Convention 108
Read “Government-Issued Digital Identity Credentials and the Privacy Landscape” to review risks and approaches not yet addressed by current laws and best practices.
Ensure that security protocols selected have been tested using formal security analysis methods and that any weaknesses have been addressed.
Ensure that ecosystem participants have clear, empirically measurable, and mandatory certification and conformance processes to ensure the desired outcomes are achieved in practice.
Pillar 4: Delivering International Interoperability
Promote the development of aligned policy frameworks and technical standards
Share priorities and engage directly with Open Standards communities in order to mature the standards that address those priorities
Participate in Open Standards in order to heighten public-private collaboration, increase transparency and trust, and speed the process to maturity
Introduce mandatory certification and conformance testing to key standards and policies

Appendix A – Evolving Threat Models

– As technologies emerge and mature, the shift towards Identity Ecosystems designed for human-centric relationships becomes ever more possible. More than half of the people on the planet have access to connected mobile devices;²²⁷ those devices have increasingly sensitive camera lenses, sensors, and other biometric capabilities that can recognize their user-owner(s). To store that data at all would have once presented an insurmountable challenge, but today, organizations can store and secure it, even in the cloud.

To do this safely requires emerging cryptographic tools and techniques, like biohashing. Similarly, advances in cryptography, cloud computing, and secure messaging protocols enable data to travel with reduced risk confidentiality breaches. This Table conveys how many of the advances in Digital Identity technologies shift the threat model.

Technological Advances	Maturity	Identity Challenges They Support	Challenges They Create
JOSE	Established	Communication of identity data in a standard signed or encrypted fashion	Handling and processing these objects
X509 Certificates	Established	Asserting specific information	Static nature
SAML2	Established	Secure single-sign on, esp. for web cases in enterprise	XML-based payload and web browser-focused interactions Third-party tracking
OAuth2 Suite	Established	Secure information exchange	Third-party tracking Consent hacking
OpenID Connect Suite	Established	Secure ID information exchange	Third-party tracking Consent hacking
Mobile Devices	Established	Local Authentication Access to digital, portable identifiers	Device dependency Cross-device flows
Biometric Capture	Growth	Authentication Deduplication	Secure data storage Privacy

Cloud Computing	Established	Secure Storage at Scale	Access controls
Secure Biometric Storage E.g., Biohashing	Emergent	Securing Biometrics	Privacy / Rules of Use
FIDO 2	Growth	Secure phishing-resistant Authentication	Linking users to Legal Identities
Passkeys	Emergent	Portable user Authentication	Provenance, assertions and Securing cloud-based User experience, adoption
Shared Signals Framework	Emergent	Communicating important events between entities in a Digital Identity Ecosystem	Agreements to share data are needed
Verifiable Credentials	Emergent	Data Model for expressing information about an entity that is digitally signed for integrity	Relying Party consumption
Decentralized Identifiers	Emergent	A data model that supports decentralized PKI providing public key material and endpoints	
Trust Registries	Emergent	These support governance authorities recording entities that conform to the governance framework being listed	Horizontal and vertical scaling Discovery by actors in the Ecosystem
Selective Disclosure	Emergent	End-user privacy controls	Relying Party consumption

Appendix B – Aligning Digital ID Principles

Theme	ID2020 ²²⁸	ID4D ²²⁹	WEF ²³⁰	DIACC & HTF ²³¹	OECD ²³²
Human Centric					
Designed for Human-Centric Outcomes	x	x		X	x
Designed for Users (incl. children, vulnerable, and guardianship)	x	x	x	X	x
Designed for Service Providers	x			X	x
Caters for Pseudonymous Identity	x			X	x
User Choice and Control	x	x	x	x	x
Inclusion					
Universal Access / Remove Barriers	x	x		x	x
Voluntary / Not Mandatory	x	x		x	x
Unique to You / Persistent Identifiers	x	x			x
Portable / Resilient (Always Accessible)	x			x	x
Strategic Governance and Design					
Critical / Strategic National Infrastructure					x
Independent Oversight		x			x
Transparent Policies	x			x	x
Clear Accountability	x	x	x	x	x
Public / Private Collaboration					x
Public Engagement / Dialogue				x	x
Accessible Onboarding and Regulatory Sandboxes					x
Long Term Sustainability		x	x	x	x
Environmental Impact					x
Secure and Privacy-Protecting					
Data Minimization / Selective Disclosure	x	x	x	x	x
Prevent Aggregation / Correlation	x				x
Privacy-by-Design	x	x	x	x	x
Security Minimum Standards	x	x	x	x	x
Enforce Privacy and Security Laws, Regulations, Guidelines					x
Internationally Interoperable					
Responsive	x	x			

Theme	ID2020 ²²⁸	ID4D ²²⁹	WEF ²³⁰	DIACC & HTF ²³¹	OECD ²³²
Human Centric					
Designed for Human-Centric Outcomes	x	x		X	x
Designed for Users (incl. children, vulnerable, and guardianship)	x	x	x	X	x
Designed for Service Providers	x			X	x
Caters for Pseudonymous Identity	x			X	x
User Choice and Control	x	x	x	x	x
Inclusion					
Universal Access / Remove Barriers	x	x		x	x
Voluntary / Not Mandatory	x	x		x	x
Unique to You / Persistent Identifiers	x	x			x
Portable / Resilient (Always Accessible)	x			x	x
Strategic Governance and Design					
Critical / Strategic National Infrastructure					x
Independent Oversight		x			x
Transparent Policies	x			x	x
Clear Accountability	x	x	x	x	x
Public / Private Collaboration					x
Public Engagement / Dialogue				x	x
Accessible Onboarding and Regulatory Sandboxes					x
Long Term Sustainability		x	x	x	x
Environmental Impact					x
Secure and Privacy-Protecting					
Conform to Standards	x	x			x
Prevent Vendor Lock-In	x	x			x
Cross-Sector Interoperability	x			x	x
Technical Interoperability (cross border)	x	x	x	x	x
Legal Interoperability (cross border)	x				x

Appendix C: OECD Principles As a Checklist

Developing User-Centred and Inclusive Digital Identity

II.RECOMMENDS that Adherents **design and implement digital identity systems that respond to the needs of users and service providers**. To this effect, Adherents should:

- Take into account the domestic context, including digital maturity and existing digital identity developments, when considering the design, implementation or iteration of a digital identity system;
- Use service design methodologies to ensure that digital identity systems respond to the needs of users and achieve accessible, ethical, and equitable outcomes, particularly by:
 - identifying the needs of users, service providers, and other affected parties;
 - considering the end-to-end user experience of the digital identity lifecycle;
 - measuring operational performance in order to iterate the digital identity system and solutions, as appropriate.
- Encourage the development of digital identity solutions that are portable for users in terms of:
 - location, including in-person, remotely, at all levels of government, and across borders;
 - technology, including availability through the most convenient device, mobile form factors or communication medium and without being constrained by the speed or quality of internet connection;
 - sector, to allow access to public services as well as the wider economy as appropriate.
- Encourage the development of privacy-preserving and consent-based digital identity solutions that give users greater ownership over their attributes and credentials, and the ability to more easily and securely control what attributes and credentials they share, when, and with whom.

III.RECOMMENDS that Adherents **prioritise inclusion and minimise barriers to access to and the use of digital identity**. To this effect, Adherents should:

- Promote accessibility, affordability, usability, and equity across the digital identity lifecycle in order to increase access to a secure and trusted digital identity solution, including by vulnerable groups and minorities in accordance with their needs;
- Take steps to ensure that access to essential services, including those in the public and private sector is not restricted or denied to natural persons who do not want to, or cannot access or use a digital identity solution;
- Facilitate inclusive and collaborative stakeholder engagement throughout the design, development, and implementation of digital identity systems, to promote transparency, accountability, and alignment with user needs and expectations;
- Raise awareness of the benefits and secure uses of digital identity and the way in which the digital identity system protects users while acknowledging risks and demonstrating the mitigation of potential harms;
- Take steps to ensure that support is provided through appropriate channel(s), for those who face challenges in accessing and using digital identity solutions, and identify opportunities to build the skills and capabilities of users;
- Monitor, evaluate and publicly report on the effectiveness of the digital identity system, with a focus on inclusiveness and minimising the barriers to the access and use of digital identity.

Strengthening the Governance of Digital Identity

IV.RECOMMENDS that Adherents **take a strategic approach to digital identity and define roles and responsibilities across the digital identity ecosystem**. To this effect, Adherents should:

- Set out a long-term vision for realising the benefits and mitigating the risks of digital identity for the public sector and wider economy either in a dedicated strategy or as part of a broader strategy;
- Secure national strategic leadership and delivery oversight and define and communicate domestic roles and responsibilities within the digital identity ecosystem;
- Encourage co-operation and co-ordination between government agencies and competent authorities at all levels of government, as relevant and applicable;
- Take steps to ensure that government agencies, and competent authorities at all levels of government, as well as other relevant actors, as applicable, take responsibility for stewarding, monitoring, and protecting the digital identity ecosystem, including by safeguarding the rights of users, and prioritising inclusion;
- Promote collaboration between the public and private sectors by supporting the development of a healthy market for digital identity solutions, as appropriate, that encourages innovation and competition and explores the potential value of alternative models and technologies;
- Establish a national or regional trust framework, or where applicable, align with relevant regional trust frameworks, to set out common requirements, including cybersecurity requirements, against different Levels of Assurance (LoA) for digital identity solutions that digital identity solution providers can follow to facilitate trust within the digital identity ecosystem;
- Establish clear responsibilities for the regulation and oversight of digital identity systems, such that the rights of users and affected parties are protected and that adequate and effective mechanisms for dispute resolution, redress and recovery are in place;
- Promote a sustainable and resilient digital identity system by taking into account the environmental impact of technology choices, and the need for

ongoing investment to reflect the costs for all relevant actors throughout the digital identity lifecycle;

Oversee the digital identity system to adapt to new needs, threats, risks and opportunities.

V.RECOMMENDS that Adherents **protect privacy and prioritise security to ensure trust in digital identity systems**. To this effect, Adherents should:

Recognise security as foundational to the design of trusted digital identity systems and ensure that digital identity solution providers and solutions comply with all relevant requirements, in a manner that is consistent with defined Levels of Assurance (LoA) and/or is consistent with a risk-based approach, to protect users, service providers, and societies, including from possible identity theft or alteration;

Treat user control, privacy and data protection as fundamental tenets of digital identity systems, and encourage the adoption of privacy-by-design and privacy-by-default approaches that include informed consent, integrity, confidentiality, selective disclosure, purpose specification, as well as collection and use limitations regarding personal data, including by considering the need for specific standards and mechanisms to protect against the misuse of special categories of personal data, including biometric data;

Prevent the aggregation of datasets between services or the retention of unnecessary personal data trails being left when users use digital identity solutions to access different services;

Enforce accountability obligations under existing data protection and privacy laws;

Introduce robust arrangements to ensure that any attributes and credentials shared through a digital identity solution are accurate, complete, kept up-to-date, and relevant;

- Identify the specific needs concerning how to safely accommodate and protect children and vulnerable groups and minorities in the design and use of digital identity systems;
- Consider taking steps to establish legally recognised mechanisms, as deemed necessary, by which users can use digital identity solutions to mandate someone, or delegate representation rights, to act on their behalf in a manner that is visible to, manageable for, and traceable by, the user;
- Promote the use of open standards and open-source software in the design of the digital identity system and other relevant actions to mitigate the risks to users, service providers and societies associated with dependency on any single hardware or software vendor.

VI.RECOMMENDS that Adherents **align their legal and regulatory frameworks and provide resources to enable interoperability**. To this effect, Adherents should:

- Ensure that, as appropriate, domestic policies, laws, rules and guidelines for the digital identity system cover issues such as governance, liability, privacy, resilience and security, to encourage and facilitate interoperability and portability in terms of location, technology and sector;
- Ensure that digital identity solutions are technology and vendor neutral as long as they comply with all relevant security requirements, and promote the use of internationally recognised technical standards and certification;
- Provide access to a catalogue of resources intended to support service providers onboard with the digital identity system such as common technical components, documentation or relevant technical support as appropriate;
- Support the creation of mechanisms, such as regulatory sandboxes, to provide a secure and controlled environment in which to explore the risks and opportunities of emerging technologies, and/or updates to digital identity systems that might affect interoperability;

Monitor and report on compliance with existing domestic rules and internationally recognised technical standards across the digital identity ecosystem, as appropriate.

Enabling Cross-Border Use of Digital Identity

VII.RECOMMENDS that Adherents **identify the evolving needs of users and service providers in different cross-border scenarios**. To this effect, Adherents should:

Identify the priority use cases for cross-border interoperability of digital identity systems according to their context and the experience of their users by identifying the activities that require the sharing of attributes and/or credentials in a different jurisdiction;

Co-operate internationally to identify the needs of service providers in other jurisdictions for recognising, integrating and trusting a digital identity solution;

Identify the risks associated with the cross-border interoperability of digital identity systems and associated use cases, and adopt mitigation measures as necessary.

VIII.RECOMMENDS that Adherents **co-operate internationally to establish the basis for trust in other countries' digital identity systems and issued digital identities**. To this effect, Adherents should:

Designate a national point of contact to engage as appropriate and applicable with international counterparts and activities in support of cross-border digital identity;

Engage in international regulatory co-operation to enable cross-border interoperability of digital identity systems, such as by assessing and/or mapping the coherence, compatibility or equivalence of existing legal requirements, trust frameworks and technical standards, exploring collaboration through free trade agreements, and identifying opportunities for cross-border regulatory experimentation;

- Engage in bilateral and multilateral co-operation in collaboration with relevant stakeholders from across the digital identity ecosystem by participating in international technical standards work, exchanging experiences and best practices, and aligning innovation programmes;
- Ensure that the cross-border interoperability of digital identity is not used to unduly discriminate against foreign users in their access to essential services or commercial transactions;
- Work towards clarifying the basis for liability related to the use of digital identity in cross-border transactions;
- For cross-border public services, enable, as appropriate, the matching of identity attributes stored in a particular public sector body abroad with the attributes or information shared about the user through the digital identification process, to ensure matching between the identity and digital identity of the user trying to access the service;
- Produce a roadmap scoping out steps that would be needed to enable:
 - domestically recognised digital identity solutions and associated attributes and credentials to be used internationally;
 - digital identity solutions and associated attributes and credentials from other countries to be recognised domestically.

Appendix D: Non-Profits with a Role in Human-Centric Digital Identity

This is a 'Living Appendix' that we maintain and update. Reviewers may suggest organizations aligned with the messages in this paper that should be included.

Body	Mission & Website
Decentralized Identity Foundation	Together we're building a new identity ecosystem Join us in developing the foundational components of an open, standards-based, decentralized identity ecosystem for people, organizations, apps, and devices.
DIACC	The DIACC believes it is critical to protect and promote Canadian values and perspectives in the digital economy. The DIACC uses the following principles as guidance to support our mission and vision.
EBSI - European Blockchain Services Infrastructure	The European Blockchain Services Infrastructure (EBSI) aims to leverage the power of blockchain for the public good. EBSI is an initiative of the European Commission and the European Blockchain Partnership.
FIDO Alliance	The FIDO Alliance is an open industry association with a focused mission: authentication standards to help reduce the world's over-reliance on passwords. The FIDO Alliance promotes the development of, use of, and compliance with standards for authentication and device attestation.
Global Assured Identity Network - Technical POC (OIDF) - Policy Working Group (OIX)	More than 150 co-authors released the 2021 GAIN Digital Trust whitepaper, which called for the creation of a globally interoperable network for high-trust identity assurance. When the OpenID Foundation's Chairman, Nat Sakimura, announced this international collaboration at the European Identity Conference, he described the authors' shared vision as "An internet where people can trust one another."
Global Legal Entity Identifier Foundation (GLEIF)	We enable smarter, less costly and more reliable decisions about who to do business with
ID2020 (Ethical Identity)	Through its partners, ID2020 is driving multi-stakeholder collaboration to set the future course of digital ID. As an Alliance, we work to ensure that safety, security, interoperability, and individual control are built into digital ID systems by-design.
IETF Internet Engineering Task Force	The overall goal of the IETF is to make the Internet work better.

	<p>Its mission is to produce high quality, relevant technical and engineering documents that influence the way people design, use, and manage the Internet in such a way as to make the Internet work better. These documents include protocol standards, best current practices, and informational documents of various kinds.</p> <p>Several groups at the IETF work on protocols leveraged for user-centric identity</p>
ISO International Organization for Standardization	<p>ISO (International Organization for Standardization) is an independent, non-governmental international organization with a membership of 168 national standards bodies.</p> <p>Through its members, it brings together experts to share knowledge and develop voluntary, consensus-based, market relevant International Standards that support innovation and provide solutions to global challenges.</p> <p>This paper draws heavily on ISO 18013-5, Mobile Driving Licence</p>
Kantara Initiative	<p>We are a global community focused on improving the trustworthy use of identity and personal data. Our working groups explore innovation, standardization and develop good practice around the collection, storage and use of personal information and identity.</p>
MyData Global	<p>MyData Global's purpose is to empower individuals by improving their right to self-determination regarding their personal data. MyData Global facilitates a global community of personal data professionals and organisations, who share a vision of, and advance the state-of-the-art for a human-centric paradigm towards personal data.</p>
NIST National Institutes of Standards and Technology	<p>To promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve our quality of life.</p> <p>NIST SP800-63-4 is the latest Digital Identity Guidelines</p>
OASIS	<p>IDTrust cluster of groups has been engaged in standards related to user-centric ID.</p>
Open Identity Exchange (OIX)	<p>OIX is a community for all those involved in the ID sector to connect and collaborate, developing the guidance needed for inter-operable, trusted identities Through our definition of, and education on Trust Frameworks, we create the rules, tools and confidence that will allow every individual a trusted, universally accepted, identity.</p>

OpenID Foundation	<p>The Foundation's vision is to help people assert their identity wherever they choose, and help people assert their identity wherever they choose, and its mission is to lead the global community in creating identity standards that are secure, interoperable, and privacy preserving.</p>
Open Wallet Foundation	<p>The OWF is a consortium of companies and non-profit organisations collaborating to drive global adoption of open, secure and interoperable digital wallet solutions as well as providing access to expertise and advice through our Government Advisory Council.</p> <p>The OWF 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.</p>
Secure Identity Alliance	<p>Unlock the full power of identity to enable people, economy and society to thrive.</p>
Trust Over IP Foundation	<p>Developing a complete architecture for Internet Digital Trust.</p> <p>And a better Internet for everyone.</p>
UNDP - Regi-Trust	<p>Digital TRUST Infrastructure for Discovery and Validation (Regi-TRUST) is an infrastructure project sponsored and hosted at the United Nations Development Programme (UNDP). The project is intended to develop and provide a suite of tools to enable discovery and validation of trusted services by leveraging existing Internet infrastructures of the Domain Name System (DNS) and its security extensions.</p>
W3C Credentials Community Group	<p>This group is under the W3C IPR umbrella but operates entirely by volunteers with minimal W3C staff support. It writes specifications that are not "official" W3C recommendations. Many specifications move from CCG into work in official W3C Working groups or other Standards development organizations.</p>
W3C Official Working Groups	<p>W3C is leading the Web to its full potential by developing protocols and guidelines that ensure the long-term growth of the Web.</p> <p>Decentralized Identifier (DID), JSON-LD, and Verifiable Credentials (VC)</p>
Women In Identity	<p>Women in Identity drives the digital identity industry to build solutions with diverse teams to promote universal access which enables civic, social and economic empowerment around the world.</p>

Appendix E: Privacy and Security Best Practices

This will be a 'Living Appendix' that we maintain and update. Reviewers may suggest organizations aligned to the messages in this paper that should be included.

FIDO Alliance	FIDO2	Best practice guidelines to shift towards phishing resistant authentication
GDPR	European Data Protection Law	Rules around the protection, processing, and movement of personal data
NIS 2	European Directive	Legislation establishing a common level of cybersecurity across the EU
NIST	SP800-63-4	Digital Identity Guidelines
	Cybersecurity Framework	The Framework focuses on using business drivers to guide cybersecurity activities and considering cybersecurity risks as part of the organization's risk management processes.
OECD Privacy Principles	Legal Instrument 0188	Recommendations concerning the protection of privacy and transborder flows of personal data
OpenID Foundation	OpenID Connect Core	PAs above provides end user approval in the journey and transaction specific signed assertions
	OIDC FAPI Profile	The FAPI profile provides a proven set of security configuration for OIDC implementers and ecosystems to use mitigating clearly defined threats
	OIDF ASC	As an early stage spec with the intent is to enable better privacy through better data minimisation in OpenID Connect
	OpenID4VC	As an emerging set of specs this work will standardize and secure interchange of signed digital credentials like verifiable credentials and mDLs
	OpenID SSF	The Shared Signals Framework is an emerging spec that enables quick and efficient notification of events that may be acted upon after the authentication and authorisation stages of the journey, such as when fraud is suspected

	OIDC4IDA	OpenID Connect for Identity Assurance allows a standardised and detailed description of the identity assurance process that was performed on a given end user, enabling a richer understanding by the relying party
--	----------	---

-
- ¹ Image sourced from United Nations. *Universal Declaration of Human Rights*, 2015. e-book. 14-15.
- ² See, for example, United Nations Office of the High Commissioner of Human Rights. "[Fact Sheet No.2 \(Rev.1\) The International Bill of Human Rights](#)." Accessed September 1, 2023.
- ³ United Nations Development Program. "[The SDGs in Action](#)." UNDP (Accessed June 26, 2023.)
- ⁴ White, O., Madgavkar, A., Manyika, J., Mahajan, D., Bughin, J., Mccarthy, M., and Sperling, O. "[Digital Identification: A Key to Inclusive Growth](#)," McKinsey Global Institute (2019)
- ⁵ Bill and Melinda Gates Foundation. "[Digitization for Improved Governance: Financial Services for the Poor](#)" (August, 2021)
- ⁶ O'Halloran, D., George, M., Duda, C. Leong, C., Johnson, J., and Keeling, J. "[Digital Identity Ecosystems: Unlocking New Value](#)." World Economic Forum (2019)
- ⁷ World Bank Group. "[Principles on Identification for Sustainable Development: Toward the Digital Age \(English\)](#)" Washington, D.C.: World Bank Group (2022)
- ⁸ See, for example Center for Human Rights and Global Justice. "[Paving a Digital Road to Hell](#)." Center for Human Rights and Global Justice: New York University School of Law (2022).
- ⁹ United Nations. "[Guidelines on the Legislative Framework for Civil Registration, Vital Statistics and Identity Management](#)." New York (2022)
- ¹⁰ United Nations High Commissioner for Refugees. "[Text of the 1954 Convention relating to the Status of Stateless Persons](#)." New York (1954)
- ¹¹ United Nations High Commissioner for Refugees. "[Convention and Protocol Relating to the Status of Refugees](#)." New York (1967)
- ¹² United Nations High Commissioner for Refugees. "[Convention on the Reduction of Statelessness](#)." (1967)
- ¹³ OECD. "[Recommendation of the Council on the Governance of Digital Identity](#)" Legal Instruments 049 (1967)
- ¹⁴ United Nations. *Universal Declaration of Human Rights*, 2015. e-book. 14-15
- ¹⁵ World Bank. "[ID4D Global Dataset – volume 21: Global ID Coverage Estimates](#)." (2023)
- ¹⁶ UNICEF. "[The State of the World's Children: Children in a Digital World](#)" (2017)
- ¹⁷ PwC, "[Global Economic Crime and Fraud Survey 2022: Protecting the Perimeter](#)." (2022)
- ¹⁸ Szreter, S. "[The Right of Registration: Development, Identity Registration, and Social Security – a Historical Perspective](#)." *World Development*, 35, no. 1 (2007), <https://doi.org/10.1016/j.worlddev.2006.09.004> as cited in Manby, B. "The Sustainable Development Goals and 'Legal Identity for All': 'First Do No Harm' *World Development*, 139 (2021)
- ¹⁹ See, for example Wenz, K. M., Palacios, R.J. and Lantei, S. "[Incentives for Improving Birth Registration Coverage: A Review of the Literature](#)." *Identification for Development*. Washington D.C.: World Bank Group. (2017)
- ²⁰ Clark, J., Diofasi, A., and Casher, C "[850 million people globally don't have ID - why this matters and what we can do about it](#)" *World Bank Blogs* (Feb 6, 2023)
- ²¹ Manby, B. "The Sustainable Development Goals and 'Legal Identity for All': 'First Do No Harm' *World Development*, 139 (2021)
- ²² United Nations. *Universal Declaration of Human Rights*, 2015. e-book. 14-15.

-
- ³⁰ United Nations Development Program "[The SDGs in Action](#)." UNDP (Accessed June 26, 2023)
- ³¹ Manby, Bronwen. 'The Sustainable Development Goals and "Legal Identity for All": "First, Do No Harm"'. *World Development* 139 (2021). <https://doi.org/10.1016/j.worlddev.2020.105343>.
- ³² Brey, Philip. 2010. 'Values in Technology and Disclosive Computer Ethics'. In *The Cambridge Handbook of Information and Computer Ethics*, edited by Luciano Floridi, 41–58. Cambridge: Cambridge University Press. <https://doi.org/10.1017/CBO9780511845239.004>.
- ³³ Nair, P. "[Aadhaar breach report: Reactions on freedom and privacy](#)" CSO Online (Jan 11, 2018)
- ³⁴ Cimpanu, C. "[Hacker steals government ID database for Argentina's entire population](#)" *The Record* (October 17, 2021)
- ³⁵ Sahara Reporters "[EXCLUSIVE: Hacker breaks into NIMC Server, Steals Over Three Million National Identity Numbers of Nigerians](#)" Sahara Reporters: New York (January 10, 2022)
- ³⁶ Thomson, I. "[South Korea faces \\$1bn bill after hackers raid national ID database](#)" *The Register* (October 14, 2014)
- ³⁷ Jennings, R. "[Estonian Hacker Steals 300,000 Government ID Photos](#)" *Security Boulevard*" (July 30, 2021)
- ³⁸ Reuters, "[Dutch hacker obtained virtually all Austrians' personal data, police say](#)" Reuters (January 25, 2023)
- ³⁹ Weinert, A. "[Biometrics, Keep Your Fingers Close](#)" Microsoft (May 26, 2020)
- ⁴⁰ Renieris, E.M. *Beyond Data*. MIT Press: New York (2022)
- ⁴¹ O'Neil, C. *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy*, New York: Penguin (2017) and Rainie, L. and Anderson, J. "[Code-Dependent: Pros and Cons of the Algorithm Age](#)" Pew Research Center (February 8, 2017)
- ⁴² Holzl, V. "[Identity and belonging in a card: how tattered Rohingya IDs trace a trail toward statelessness](#)" *The New Humanitarian* (March 1, 2018)
- ⁴³ Shah, P. and Smith, R. S. "[Legacies of Segregation and Disenfranchisement: The Road from Plessy to Frank and Voter ID Laws in the United States](#)" *RSF: The Russell Sage Foundation Journal of the Social Sciences* Vol 7, No 1 (February 2021) pp. 134-146
- ⁴⁴ Masiero, S. "[A new layer of exclusion? Assam, Aadhaar and the NRC](#)" *London School of Economics Blogs* (September 12, 2019)
- ⁴⁵ Martin, M. "[Germany's new e-ID cards raise hackles over privacy](#)" Reuters (November 10, 2010)
- ⁴⁶ Center for Human Rights and Global Justice "[Paving a Digital Road to Hell](#)" Center for Human Rights and Global Justice: New York University School of Law (June 2022)
- ⁴⁷ Abouharb, M. Rodwan and Daveed Gartenstein-Ross. "The Civicness of Nations: Measuring Expectations of Government." *International Studies Quarterly*, vol. 55, no. 4, 2011, pp. 1099–1120.
- ⁴⁸ Sheldrake, P. "[Human Identity: the Number One Challenge in Computer Science](#)" (2022) Accessed on August 23, 2023
- ⁴⁹ Better Identity Coalition "[Better Identity in America: A Blueprint for State Policymakers](#)" Better Identity Coalition (2022), p. 5-6
- ⁵⁰ Windley, P. J. *Learning Digital Identity: Design, Deploy, and Manage Identity Architectures* O'Reilly Media, Inc (January, 2023), p. 37

-
- ⁵¹ Khaira, R. "[Rs 500, 10 minutes, and you have access to billion Aadhaar details](#)" The Tribune (January 3, 2018)
- ⁵² Donnan, S. and Bass, D. "[How Did ID.me Get Between You and Your Identity](#)" *Bloomberg Businessweek* (January 20, 2022)
- ⁵³ UK Public Accounts Parliamentary Committee "[Accessing public services through the government's Verify digital system](#)" (May 8, 2019)
- ⁵⁴ Wilson, C. "[No, You Can't Have My Social Security Number: why using SSNs for identification is risky and stupid](#)" *Slate.com* (July 14, 2009)
- ⁵⁵ FirstPost "[Aadhaar security breaches: Here are the major untoward incidents that have happened with Aadhaar and what was actually affected](#)" Firstpost (January 16, 2018)
- ⁵⁶ Maiero, S. "[Digital identity as platform-mediated surveillance](#)" *Big Data and Society*, 10(1) (January 3, 2023)
- ⁵⁷ Confessore, N. "[Cambridge Analytica and Facebook: The Scandal and the Fallout So Far](#)" New York Times: London (April 4, 2018)
- ⁵⁸ Burt, C. "[Nigeria ID4D head calls for stronger legal framework to support digital ID consistency](#)" *Biometric Update.com* (November 30, 2022)
- ⁵⁹ See, for example UK Public Accounts Parliamentary Committee "[Accessing public services through the government's Verify digital system](#)" (May 8, 2019) and Donnan, S. and Bass, D. "[How Did ID.me Get Between You and Your Identity](#)" *Bloomberg Businessweek* (January 20, 2022)
- ⁶⁰ Khaira, R. "[Rs 500, 10 minutes, and you have access to billion Aadhaar details](#)" The Tribune (January 3, 2018)
- ⁶¹ Consumer Financial Protection Bureau "[Equifax data breach settlement](#)" Accessed on September 1, 2023
- ⁶² Confessore, N. "[Cambridge Analytica and Facebook: The Scandal and the Fallout So Far](#)" New York Times: London (April 4, 2018)
- ⁶⁴ Solove, D. J. and Hartzog, W. *Breached! Why Data Security Law Fails and How to Improve It* Oxford University Press (March 1, 2022)
- ⁶⁵ Renieris, E.M. *Beyond Data* MIT Press: New York (2022)
- ⁶⁶ See, for example, Sheldrake, P. "[Human Identity: the Number One Challenge in Computer Science](#)" (2022) Accessed on August 23, 2023
- ⁶⁷ Andrieu, J. "[A Primer on Functional Identity](#)" Web Of Trust (November 18, 2019)
- ⁶⁸ United Nations "[Human Rights Instruments](#)" United Nations (Accessed on Jun 25, 2023)
- ⁶⁹ Woman in Identity "[Code of Conduct: the Human Impact of Identity Exclusion](#)" Women in Identity (Accessed on June 25, 2023)
- ⁷⁰ Bertrand, A. and McQueen, J. "[How can digital government connect citizens without leaving the disconnected behind?](#)" Ernst and Young (February, 24, 2021)
- ⁷¹ Oppenheim, M. "[How NHS is inadvertently telling domestic abusers where they can track down their victims](#)" The Independent (February 16, 2022)
- ⁷² Figure 3 references include:
World Bank. "[ID4D Global Dataset – volume 21: Global ID Coverage Estimates.](#)" (2023)
United Nations Refugee Agency "[Statelessness around the world](#)" Accessed on September 5, 2023
United Nations Refugee Agency "[1 percent of humanity displaced: UNHCR Global Trends Report](#)" (June 18, 2020)
AARP "1 in 5 Americans Now Provide Unpaid Family Care" (July 15, 2022)

-
- Freedom House "[Freedom in the World 2023](#)" (March, 2023)
- United Nations Office on Drugs and Crime "[Victim Assistance and Witness Protection](#)" Accessed on September 10, 2023
- World Health Organization "[Disability](#)" (March 7, 2023)
- Huecker, M.R., King, K.C., Jordan, G.A., Smock, W. "[Domestic Violence](#)" National Library of Medicine. Last updated April 9, 2023.
- ⁷³ Breckenridge, K. and Szreter, S. "[Registration and Recognition: Documenting the Person in World History](#)" 39:3 (January 2014)
- ⁷⁴ Nyst, C., Pannifer, S., Whitley, E., Makin, P. "[Digital Identity: Issue Analysis](#)" version 1.6. Consult Hyperion (June 8, 2016)
- ⁷⁵ *ibid*
- ⁷⁶ Handforth, C. and Wilson, M. "[Digital Identity Country Profile: Uganda](#)" GSMA: London, UK (2019)
- ⁷⁷ BankID "[About Us](#)" BankID (Accessed on June 15, 2023)
- ⁷⁸ Interac "[Access government services with Interac sign in service](#)" Interac (Accessed on June 25, 2023)
- ⁷⁹ European Commission "[The Common Union Toolbox for a Coordinated Approach Towards a European Digital Identity Framework](#)" v1.0.0
- ⁸⁰ Nyst, C., Pannifer, S., Whitley, E., Makin, P. "[Digital Identity: Issue Analysis](#)" version 1.6. Consult Hyperion (June 8, 2016) 161-175
- ⁸¹ Nyst, C., Pannifer, S., Whitley, E., Makin, P. "[Digital Identity: Issue Analysis](#)" version 1.6. Consult Hyperion (June 8, 2016)
- ⁸² Monetary Authority of Singapore "[Foundational Digital Infrastructures for Inclusive Digital Economies](#)" Singapore (April 2021)
- ⁸³ Open Identity Exchange (OIX) "[Trust Frameworks for Smart Digital ID](#)" (June 2022)
- ⁸⁴ Singpass "[Your improved digital ID to make life easy](#)" Singapore: Singpass (Accessed June 26, 2023)
- ⁸⁵ e-estonia "[e-Identity](#)" (Accessed on July 3, 2023)
- ⁸⁶ Supreme Court of India "Writ Petition (Civil) No. 494 of 2012" New Delhi: Supreme Court of India (September 26, 2018) *See Also:* Varadhan, S. and Mohanty, S. "[Supreme Court imposes curbs on use of Aadhaar](#)" Reuters Technology News (September 26, 2018)
- ⁸⁷ Iruoma, K. "Got your number: [Privacy concerns hobble Nigeria's digital ID push](#)" Reuters (August 5, 2021)
- ⁸⁸ Center for Human Rights and Global Justice, Initiative for Social and Economic Rights, and Unwanted Witness "[Chased Away and Left to Die](#)" (June 8, 2021)
- ⁸⁹ Puckett, C. "[The Story of the Social Security Number](#)" *Social Security Bulletin* 69 (2) U.S. Social Security Administration (2009)
- ⁹⁰ Unique Identification Authority of India "[Usage of Aadhaar](#)" (Accessed on July 3, 2023)
- ⁹¹ Bill and Melinda Gates Foundation, "[Digitization for Improved Governance: Financial Services for the Poor](#)," (2021) p.12-13
- ⁹² Supreme Court of India "Writ Petition (Civil) No. 494 of 2012" New Delhi: Supreme Court of India (September 26, 2018) *See Also:* Varadhan, S. and Mohanty, S. "[Supreme Court imposes curbs on use of Aadhaar](#)" Reuters Technology News (September 26, 2018)
- ⁹³ Young, K. "[Key Differences Between the U.S. Social Security System and India's Aadhaar System](#)" New America (August 5, 2019)
- ⁹⁴ Unique Identification Authority of India "[Aadhaar e-KYC API Specification](#) - Version 2.0" (May 2016)

-
- ⁹⁵ Business Standard "[Aadhaar a 'bedrock' for govt welfare schemes, saved over RS 2trn](#)" Business Standard (June 01, 2022)
- ⁹⁶ Nar, P. "[Aadhaar breach report: Reactions on freedom and privacy](#)" CSO (Jan 11, 2018) ↓
- ⁹⁷ Henne, Kathryn. "Surveillance in the Name of Governance: Aadhaar as a Fix for Leaking Systems in India." *Information, Technology and Control in a Changing World*, June 22, 2019, 223–45.
- ⁹⁸ Kumar, A. (ed) "[How fraudsters are using loopholes in Aadhaar system to create Fake IDs](#)" [India.com](#) (March 18, 2023)
- ⁹⁹ National Identity Management Commission "[National Identity Management Commission: providing assured identity](#)" NIMC (Accessed on June 26, 2023)
- ¹⁰⁰ Nigeria Data Protection Commission "[Nigeria Data Protection Bill, 2022](#)" NDPC (Accessed June 26, 2023)
- ¹⁰¹ Biometric Update "[Nigeria's national biometric ID proposed to go digital, add DNA](#)" Biometric Update (August 16, 2020)
- ¹⁰² Federal Republic of Nigeria Official Gazette "[Mandatory Use of the National Identification Number Regulations, 2017](#)" Lagos: Federal Republic of Nigeria Official Gazette, 104: 121 (November 13, 2017)
- ¹⁰³ National Identity Management Commission "[Enhanced NIMC Verification System v1.0](#)" [NIMC.gov](#) (Accessed June 26, 2023)
- ¹⁰⁴ OSIA "[Unlocking the ID Ecosystem with OSIA: a universal interoperability framework for innovation, competition, and sustainability](#)" Accessed on September 21, 2023
- ¹⁰⁵ Iruoma, K. "Got your number: [Privacy concerns hobble Nigeria's digital ID push](#)" Reuters (August 5, 2021)
- ¹⁰⁶ McSweeney, E. "[As Covid-19 cases rise in Nigeria, a government policy is creating crowds and chaos](#)" CNN (February 10, 2021)
- ¹⁰⁷ Singpass "[Your improved digital ID to make life easy](#)" Singapore: Singpass (Accessed June 26, 2023)
- ¹⁰⁸ GovTech Singapore "[All Government Agencies to Accept Singpass Digital IC from 1 November 2021](#)" (October 28, 2021)
- ¹⁰⁹ Post, V. "[The evolution of Singpass: How Singapore's national digital identity came about](#)" KrAsia (April 27, 2023)
- ¹¹⁰ Macellino, A. "[Singpass introduces biometric face verification, Kofax integrates digital signatures](#)" Biometric Update (December 17, 2020)
- ¹¹¹ Cooper, A., Marskell, J., and Chan, C.H. "[National Digital Identity and Government Data Sharing in Singapore](#)" The World Bank ID4D and Govtech Singapore (2022) pp xiv
- ¹¹² Ibid, pp 46
- ¹¹³ En, T.J. "[Singapore's flawed data privacy regime](#)" New Naratif (June 11, 2018)
- ¹¹⁴ Ministero dell'Interno "[Electronic Identity Card \(CIE\)](#)" Carta Identita Interno (Accessed on June 26, 2023)
- ¹¹⁵ Agenzia per l'Italia Digitale "[SPID Public Digital Identity System](#)" (Accessed on June 26, 2023)
- ¹¹⁶ Mascellino, A. "[Italian national digital ID scheme reaches 30 million users milestone](#)" Biometric Update (May 9, 2022)
- ¹¹⁷ DIACC "[Pan-Canadian Trust Framework](#)" DIACC (Accessed June 26, 2023)
- ¹¹⁸ UK Parliament "[Accessing public services through the Government's Verify digital system](#)" London: UK Parliament (May 8, 2019)

-
- ¹¹⁹BankID "[BankID: We ensure safe and secure identification and signing](#)" BankID (Accessed June 26, 2023)
- ¹²⁰Official Journal of the European Union "[Regulation \(EU\) 2016/679 Of the European. Parliament And Of The Council](#)" (April 27, 2016)
- ¹²¹Ministry of Local Government and Districts "Act on the Implementation of the EU Regulation on electronic identification and trust services for electronic transactions in the internal market" (June 15, 2018)
- ¹²²BankID "[BankID with Biometrics](#)" BankID (Accessed on June 27, 2023)
- ¹²³Hersey, F. "[Digital parenting, minimized fraud and a 'just do it' attitude: Future Identity Festival!](#)" Biometric Update (November 17, 2021)
- ¹²⁴DIACC "[Pan-Canadian Trust Framework](#)" DIACC (Accessed June 26, 2023)
- ¹²⁵Office of the Privacy Commissioner of Canada "[The Personal Information Protection and Electronic Documents Act \(PIPEDA\)](#)" (Accessed on July 5, 2023)
- ¹²⁶Avast "[Avast to Acquire SecureKey Technologies](#)" PRNewswire (March 24, 2022)
- ¹²⁷SecureKey Technologies "[Verified Me: Your Identity in Your Control](#)" (December 2019)
- ¹²⁸European Commission "Regulation of the European Parliament and of the Council amending Regulation (EU) No 910/2014 as regards establishing a framework for a European Digital Identity" COM(2021) 281 final. Brussels: European Commission (June 3, 2021)
- ¹²⁹Macdonald, A. "[Bhutan launches self-sovereign biometric digital ID, crown prince first to enroll!](#)" Biometric Update (February 23, 2023)
- ¹³⁰British Columbia "[Digital Credential Services](#)" (Accessed on June 27, 2023)
- ¹³¹John, A. "[US Digital Immigration Credentials Overview](#)" FedID Conference Slides (December, 2022)
- ¹³²International Organization for Standardization "[ISO/IEC 18013-5 Personal identification - ISO-compliant driving licence - Part 5: Mobile driving licence \(mDL\) application](#)" ISO (September 2021)
- ¹³³Council of the EU "[European digital identity \(eID\): Council makes headway towards EU digital wallet, a paradigm shift for digital identity in Europe](#)" Brussels: Press Release (December 6, 2022)
- ¹³⁴European Commission "[The Common Union Toolbox for a Coordinated Approach Towards a European Digital Identity Framework](#)" v1.0.0
- ¹³⁵W3C "[Verifiable Credentials Data Model v1.1](#)" (March 3, 2022)
- ¹³⁶Lodderstedt, T., Yasuda, K., Looker, T. (eds) "[OpenID for Verifiable Credential Issuance](#)" OpenID Foundation (February 3, 2023)
- ¹³⁷Terbu, O., Lodderstedt, T., Yasuda, K., Looker, T. "[OpenID for Verifiable Presentations - draft 18](#)" OpenID Foundation (April 21, 2023)
- ¹³⁸Yasuda, K., Jones, M., and Lodderstedt, T. "[Self-Issued OpenID Provider v2](#)" OpenID Foundation (January 1, 2023)
- ¹³⁹International Organization for Standardization "[ISO/IEC 18013-5 Personal identification - ISO-compliant driving licence - Part 5: Mobile driving licence \(mDL\) application](#)" ISO (September 2021)
- ¹⁴⁰Fett, D., Yasuda, K. and Campbell, B. "[Selective Disclosure JWTs \(SD-JWT\)](#)" IETF Draft
- ¹⁴¹Sporny, M. Longley, D., Kellogg, K., Lanthaler, M., Champin, PA, Lindstrom, N. "[JSON LD 1.1](#)" W3C (July 16, 2020)
- ¹⁴²John, A. "[US Digital Immigration Credentials Overview](#)" FedID Conference Slides (December, 2022)
- ¹⁴³Baker, B., Miller, S. "[Estimates of the Lawful Permanent Resident Population in the United States and the Subpopulation Eligible to Naturalize: 2022](#)" Homeland Security: Office of Immigration Statistics (October 2022)

-
- ¹⁴⁴ W3C "[Verifiable Credentials Data Model v1.1](#)" (March 3, 2022)
- ¹⁴⁵ W3C "[Decentralized Identifiers \(DIDs\) v1.0](#)" (July 19, 2022)
- ¹⁴⁶ Thales "[Gemalto wins U.S. Government Grant for DDL Pilot in Four Jurisdictions](#)" Thales Group (November 14, 2016)
- ¹⁴⁷ Hersey, F. "[Digital ID Credentials come to the Apple Wallet, inform apps, but EU may cause friction](#)" Biometric Update (October 4, 2022)
- ¹⁴⁸ OECD, "[Recommendation of the Council on the Governance of Digital Identity](#)" Legal Instruments 0491 (2023)
- ¹⁴⁹ ID2020 "[ID2020 Technical Requirements](#)" ID2020 Certification (April 28, 2019; Accessed June 26, 2023)
- ¹⁵⁰ World Bank Group "[Principles on Identification for Sustainable Development: Toward the Digital Age \(English\)](#)" Washington, D.C.: World Bank Group (November 3, 2022)
- ¹⁵¹ O'Halloran, D., George, M., Duda, C. Leong, C., Johnson, J., and Keeling, J. "[Digital Identity Ecosystems: Unlocking New Value](#)" World Economic Forum (September 2021)
- ¹⁵² Mothershaw, N. "[Trust Frameworks for Smart Digital ID](#)" The Open Identity Exchange (June 2022)
- ¹⁵³ de Brisis M.M. and Brennan, J. "[Universal Digital Identity Policy Principles to Maximize Benefits for People: A shared European and Canadian Perspective](#)" DIACC and Human Technology Foundation (November 2, 2022)
- ¹⁵⁴ Solove, D. J. and Hartzog, W. *Breached! Why Data Security Law Fails and How to Improve It* Oxford University Press (March 1, 2022), p.176
- ¹⁵⁵ Planetnetwork "[Augmented Social Network](#)" (Accessed on June 27, 2023)
- ¹⁵⁶ See, for example, Masiero, S. and Bailur, S. "[Digital Identity for Development: the quest for justice and a research agenda](#)" *Information Technology for Development*, 27:1, pp.1-12 (2021) Further sources can be found on the [Global Data Justice](#) website
- ¹⁵⁷ de Brisis M.M. and Brennan, J. "[Universal Digital Identity Policy Principles to Maximize Benefits for People: A shared European and Canadian Perspective](#)" DIACC and Human Technology Foundation (November 2, 2022)
- ¹⁵⁸ ID2020 "[Manifesto](#)" (Accessed on June 27, 2023)
- ¹⁵⁹ World Bank Group "[Principles on Identification for Sustainable Development: Toward the Digital Age \(English\)](#)" Washington, D.C.: World Bank Group (November 3, 2022)
- ¹⁶⁰ Woman in Identity "[Code of Conduct: the Human Impact of Identity Exclusion](#)" Women in Identity (Accessed on June 25, 2023)
- ¹⁶¹ O'Halloran, D., George, M., Duda, C. Leong, C., Johnson, J., and Keeling, J. "[Digital Identity Ecosystems: Unlocking New Value](#)" World Economic Forum (September 2021)
- ¹⁶² Trust Over IP Foundation "[Overcoming Human Harm Challenges in Digital Identity Ecosystems](#)" V1.0 Trust Over IP Foundation (November 16, 2022)
- ¹⁶³ <https://www.mydata.org/participate/declaration/> chapter 3
- ¹⁶⁴ OECD, "[Recommendation of the Council on the Governance of Digital Identity](#)" Legal Instruments 0491 (2023)
- ¹⁶⁵ See, for example Manby, Bronwen. 'The Sustainable Development Goals and "Legal Identity for All": "First, Do No Harm"'. *World Development* 139 (2021). <https://doi.org/10.1016/j.worlddev.2020.105343>. [copy attached, since this is not open access]
- ¹⁶⁶ United Nations. *Universal Declaration of Human Rights*, 2015. e-book. 14-15

-
- ¹⁶⁷ United Nations High Commissioner for Refugees. "[Convention and Protocol Relating to the Status of Refugees.](#)" New York (1967)
- ¹⁶⁸ United Nations High Commissioner for Refugees. "[Text of the 1954 Convention relating to the Status of Stateless Persons.](#)" New York (1954)
- ¹⁶⁹ United Nations Office on Drugs and Crime "[Victim Assistance and Witness Protection](#)" Accessed on September 10, 2023
- ¹⁷⁰ United Nations "[Convention on the Rights of the Child](#)" (November, 1989)
- ¹⁷¹ United Nations Department of Economic and Social Affairs "Guidelines on the Legislative Framework for Civil Registration, Vital Statistics, and Identity Management Systems" New York (2023)
- ¹⁷² de Brisis M.M. and Brennan, J. "[Universal Digital Identity Policy Principles to Maximize Benefits for People: A shared European and Canadian Perspective](#)" DIACC and Human Technology Foundation (November 2, 2022)
- ¹⁷³ UK Parliament "[Accessing public services through the Government's Verify digital system](#)" London: UK Parliament (May 8, 2019)
- ¹⁷⁴ Luma Institute "[Innovating for People: Handbook of Human-Centered Design Methods](#)" (February 22, 2021)
- ¹⁷⁵ unicef "[Human Centered Design 4 Health](#)" unicef (Last Accessed June 27, 2023)
- ¹⁷⁶ Krippendorf, Klaus "[Intrinsic motivation and human-centred design](#)" *Theoretical Issues in Ergonomics Science*, 5(1) (2004) 43-72 as cited in Sheldrake, P. "[Once more with meaning – a review of a draft industry paper on human-centric digital identity](#)" (August 14, 2023)
- ¹⁷⁷ de Brisis M.M. and Brennan, J. "[Universal Digital Identity Policy Principles to Maximize Benefits for People: A shared European and Canadian Perspective](#)" DIACC and Human Technology Foundation (November 2, 2022)
- ¹⁷⁸ Morrison, R. "[UK supermarket digital ID trial success could see law changed](#)" Tech Monitor (January 3, 2023)
- ¹⁷⁹ White, O., Madgavkar, A., Manyika, J., Mahajan, D., Bughin, J., McCarthy, M., and Sperling, O., "[Digital Identification: A Key to Inclusive Growth.](#)" McKinsey Global Institute (2019)
- ¹⁸⁰ Bertrand, A. and McQueen, J. "[How can digital government connect citizens without leaving the disconnected behind?](#)" Ernst and Young (February, 24, 2021)
- ¹⁸¹ OECD, "[Recommendation of the Council on the Governance of Digital Identity](#)" Legal Instruments 0491 (2023)
- ¹⁸² Secure Identity Alliance "[Giving Voice to Digital Identities Worldwide: Key Insights and Experiences to Overcome Shared Challenges](#)" Secure Identity Alliance (2021)
- ¹⁸³ Woman in Identity "[Code of Conduct: the Human Impact of Identity Exclusion](#)" Women in Identity (Accessed on June 25, 2023).
- ¹⁸⁴ See, for example Davis, Fred D. "Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology" *MIS Quarterly* 13 (3): 319–40.
- ¹⁸⁵ Ravenscraft, E. "[How to Spot - and Avoid - Dark Patterns on the Web](#)" *Wired* (July 29, 2020).
- ¹⁸⁶ Myers, S.L. "[How Social Media Amplifies Misinformation More than Information](#)" *New York Times* (October 13, 2022).
- ¹⁸⁷ Pimintel, B. "[Banks and fintechs agree: It's time for screen scraping to go. So what's next?](#)" Protocol (October 5, 2021)

-
- ¹⁸⁸ Winkler, T. and Spiekermann, S. "[Twenty years of value sensitive design: a review of methodological practices in VSD projects](#)" *Ethics and Information Technology*, 23, pp. 17-21 (March 2021)
- ¹⁸⁹ Van de Poel, I. "[Embedding Values in Artificial Intelligence \(AI\) Systems.](#)" *Minds and Machines* 30, 385-409 (2020)
- ¹⁹⁰ Umbrello, S. and van de Poel, I. "[Mapping Value Sensitive Design onto AI for Social Good Principles](#)" *AI Ethics* 1(3) 283-296 (2021)
- ¹⁹¹ Winkler, T. and Spiekermann. "[Twenty years of value sensitive design: a review of methodological practices in VSD projects](#)" *Ethics and Information Technology*, 23 (2021)
<https://doi.org/10.1007/s10676-018-9476-2>
- ¹⁹² Marsman, Henk. "[Is the Capabilities Approach Operationalizable to Analyse the Impact of Digital Identity on Human Lives.](#)" *Data & Policy* 4 (2022): e43. doi:10.1017/dap.2022.37.
- ¹⁹³ Woman in Identity "[Code of Conduct: the Human Impact of Identity Exclusion](#)" *Women in Identity* (Accessed on June 25, 2023)
- ¹⁹⁴ Solove, D. J. and Hartzog, W. *Breached! Why Data Security Law Fails and How to Improve It* Oxford University Press (March 1, 2022) p.191
- ¹⁹⁵ See, for example Manby, Bronwen. 'The Sustainable Development Goals and "Legal Identity for All": "First, Do No Harm"'. *World Development* 139 (2021).
<https://doi.org/10.1016/j.worlddev.2020.105343>.
- ¹⁹⁶ Solove, D. J. and Hartzog, W. *Breached! Why Data Security Law Fails and How to Improve It* Oxford University Press (March 1, 2022) page number
- ¹⁹⁷ Renieris, E.M. *Beyond Data* MIT Press: New York (2022) page number
- ¹⁹⁸ Confessore, N. "Cambridge Analytica and Facebook: The Scandal and the Fallout So Far" *New York Times*: London (April 4, 2018) <https://www.nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal-fallout.html>
- ¹⁹⁹ Renieris, E.M. *Beyond Data* MIT Press: New York (2022)
- ²⁰⁰ Solove, D. J. and Hartzog, W. *Breached! Why Data Security Law Fails and How to Improve It* Oxford University Press (March 1, 2022)
- ²⁰¹ Lips, S., Tsap, V., Bharosa, N, Draheim, D., Krimmer, R., and Tammet, T. "[Management of National eID Infrastructure as a State-Critical Asset and Public-Private Partnership: Learning from the Case of Estonia](#)" (May 19, 2022)
- ²⁰² Mothershaw, N. "[Trust Frameworks for Smart Digital ID](#)" *The Open Identity Exchange* (June 2022)
- ²⁰³ Mothershaw, N. "[Trust Frameworks for Smart Digital ID](#)" *The Open Identity Exchange* (June 2022)
- ²⁰⁴ de Brisis M.M. and Brennan, J. "[Universal Digital Identity Policy Principles to Maximize Benefits for People: A Shared European and Canadian Perspective](#)" *DIACC and Human Technology Foundation* (November 2, 2022)
- ²⁰⁵ Center for Human Rights and Global Justice, Initiative for Social and Economic Rights, and Unwanted Witness "[Chased Away and Left to Die](#)" (June 8, 2021)
- ²⁰⁶ Center for Human Rights and Global Justice "[Paving a Digital Road to Hell](#)" *Center for Human Rights and Global Justice: New York University School of Law* (June 2022)
- ²⁰⁷ Bhandari, V., Trikanad, S. and Sinha, A. "[Governing ID: A Framework for Evaluation of Digital Identity](#)" *Centre for Internet and Society, India* (January 22, 2020)
- ²⁰⁸ van der Straaten, J. "Identification for Development It Is Not: Inclusive and Trusted Digital ID Can Unlock Opportunities for the World's Most Vulnerable' - A Review" (November 20, 2020)

-
- ²⁰⁹ Easterly, J. "[Congressional Hearing On Evolving the U.S. Approach to Cybersecurity: Raising the Bar Today to Meet the Threats of Tomorrow](#)" Washington, D.C.: US House of Representatives - Homeland Security Committee (November 3, 2021)
- ²¹⁰ Solove, D. J. and Hartzog, W. *Breached! Why Data Security Law Fails and How to Improve It* Oxford University Press (March 1, 2022)
- ²¹¹ "Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on Measures for a High Common Level of Cybersecurity across the Union, Amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and Repealing Directive (EU) 2016/1148 (NIS 2 Directive)." European Union, December 14, 2020. <http://data.europa.eu/eli/dir/2022/2555/oj>.
- ²¹² NIST "[SP 800-63-4 \(draft\) Digital Identity Guidelines](#)" NIST (December 16, 2022)
- ²¹³ Solove, D. J. and Hartzog, W. *Breached! Why Data Security Law Fails and How to Improve It* Oxford University Press (March 1, 2022)
- ²¹⁴ OECD. "Recommendation of the Council Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data." OECD Legal Instruments, October 7, 2013. <https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0188>.
- ²¹⁵ "[Regulation \(EU\) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC \(General Data Protection Regulation\)](#)." European Union, May 4, 2016.
- ²¹⁶ Council of Europe. "[Convention for the protection of individuals with regard to the processing of personal data](#)." Convention 108+. (June 2018)
- ²¹⁷ University of Stuttgart "The Web Infrastructure Model (WIM)" <https://www.sec.uni-stuttgart.de/research/wim> (Last Accessed September 24, 2023)
- ²¹⁸ <https://www.nist.gov/itl/ssd/information-systems-group/overview-conformance-testing>
- ²¹⁹ Young, K. *The Domains of Identity* Anthem Press (June 25, 2020)
- ²²⁰ European Commission. Directorate General for Informatics. 2017. New European Interoperability Framework: Promoting Seamless Services and Data Flows for European Public Administrations. LU: Publications Office. <https://data.europa.eu/doi/10.2799/78681>
- ²²¹ Open Identity Exchange. "[OIX defines the need for clear, global data standards for identity information](#)." August 29, 2023.
- ²²² Trust Over IP Foundation "[Why Trust Over IP](#)" Trust Over IP Foundation (November 16, 2022)
- ²²³ MyData Operators. <https://mydata.org/operators>. (Last Accessed September 24, 2023)
- ²²⁴ Garber, E., Mothershaw, N., Labriolle, S., and Comparin, D. "[GAIN in 2023](#)" (2023)
- ²²⁵ European Commission "[The Common Union Toolbox for a Coordinated Approach Towards a European Digital Identity Framework](#)" v1.0.0
- ²²⁶ Theodorou, Y. "[Modernising Digital-ID Systems: What Open Standards and Open-Source Software Really Mean](#)" Tony Blair Institute for Global Change (December 15, 2022)
- ²²⁷ "The Mobile Economy - The Mobile Economy." 2022. The Mobile Economy. November 29, 2022. https://www.gsma.com/mobileeconomy/#key_stats.
- ²²⁸ "ID2020 Technical Requirements: v1.0" https://docs.google.com/document/d/1L0RhDq98xj4ieh5CuN-P3XerK6umKRTPWMS8Ckz6_J8/edit (Last Accessed September 24, 2023)
- ²²⁹ World Bank Group et al (2022) Principles on Identification for Sustainable Development <https://www.idprinciples.org/>

²³⁰ World Economic Forum. "[Unlocking Identity Ecosystems: Unlocking New Value.](#)" (September 2021)

²³¹ "Universal Digital Identity Policy Principles to Maximize Benefits for People: A Shared European and Canadian Perspective." 2022. Digital ID & Authentication Council of Canada. November 2, 2022. <https://diacc.ca/2022/11/02/policy-design-principles-to-maximize-people-centered-benefits-of-digital-identity/>.

²³² OECD Privacy Principles, <https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0491>