



Digital Identifier Inclusion

Version: 1.0 Draft 8

Document Date: 2024-05-08

Editors: Tom Jones

Contributors: Justin Byrd, Isha Chhatwal, Bev Corwin, Salvatore D'Agostino, Jorge Flores, Jim Kragh, Tom Sullivan, Noreen Whysel, Tom Jones

Produced by: Resilient Identifiers for Underserved Populations Work Group

Status:

This document is a Work Group Draft Report produced by the Resilient Identifiers for Underserved Populations (RIUP) Work Group.

Abstract:

This document is based on the idea that all humans with rights or privileges that are accessible by digital identifiers will have the means to access those rights or privileges. The problems with exclusion from access to digital resources are briefly described and then some broad solutions are proposed. Where rights are granted to citizens, government regulations are needed to assure that no eligible person can be denied access to any of their rights and privileges using any smart device that holds government-issued credentials. These credentials must be as current as is required for the stated purpose.

This document is not a Kantara recommendation or specification but is a report distributed for trial implementations. Recipients of this draft are invited to submit, with their comments, notification of any relevant patent rights with supporting documentation for the benefit of the wider community and the ecosystem at large.

IPR Option:

This document is subject to the Kantara IPR Policy option Non-Assertion Covenant

Digital Identifier Inclusion

Feedback: It is expected that a new version of this report will be forthcoming. If you have feedback for the work group, please create an issue at [Issues · KantaraInitiative/Inclusion \(github.com\)](https://github.com/KantaraInitiative/Inclusion)

Suggested Citation:

Digital Identifier Inclusion 1.0. Kantara Initiative Work Group: Resilient Identifiers for Underserved Populations. 2024-05-08. Kantara Initiative Report . **HREF** TK when published

NOTICE



Copyright: The content of this document is copyright of Kantara Initiative, Inc.
© 2024 Kantara Initiative, Inc.

DEAR READER

Digital Identifier Inclusion

Thank you for downloading this publication prepared by the international community of experts that comprise the Kantara Initiative. Kantara is a global non-profit 'commons' dedicated to improving the trustworthy use of digital identity and personal data through innovation, standardization, and good practice.

Kantara is known around the world for incubating innovative concepts, operating Trust Frameworks to assure digital identity & privacy service providers, and developing community-led best practices and specifications. Its efforts are acknowledged by OECD ITAC, UNCITRAL, ISO SC27, other consortia and governments around the world. 'Nurture, Develop, Operate' captures the rhythm of Kantara in consolidating an inclusive, equitable digital economy offering value and benefit to all.

Every publication, in every domain, is capable of improvement. Kantara welcomes and values your contribution through [membership](#), [sponsorship](#), and active participation in the [working group](#) that produced this and participation in all our endeavors so that Kantara can reflect its value back to you and your organization.

Digital Identifier Inclusion

Contents

1. INTRODUCTION	4
1.1. GOALS	4
1.2. ASSUMPTIONS	5
2. OVERVIEW OF THE PROBLEM	6
2.1. EXAMPLES OF EXCLUSION	6
2.2. SECURITY VERSUS INCLUSION	7
3. TERMS AND DEFINITIONS	8
3.1. TAXONOMY	8
3.2. SMART MOBILE DEVICE	10
3.3. TRUSTWORTHY DIGITAL ECOSYSTEM	10
3.4. GUARDIANSHIP	10
3.5. ACCESSIBILITY AND INCLUSION	11
3.6. CONSENT, NOTICE AND AUDIT	11
4. DIGITAL PUBLIC INFRASTRUCTURE	12
5. USE CASES	14
5.1. SCENARIOS	14
5.2. DATA FLOWS	15
5.3. GUARDIANSHIP PROBLEMS	15
5.4. PERSONAS	16
6. REFERENCES	21

Digital Identifier Inclusion

1. INTRODUCTION

This concept of **Digital Identifier Inclusion** is described here along with several use cases. No person creates their own identity in a single place. A person's identity is formed in the places where they work and play, learn and advocate. So, it is unlikely that anyone's identity can ever be completely encompassed by an authenticated identifier in one single Credential. What people need to carry with them is a verified collection of digital claims about themselves tied to an identifier that they can call upon as needed in their online interchanges to protect access to and distribution of their personal information.

This report is designed to work with mobile devices that are carried with the user and have the capability to be network-attached, such as a smartphone. This Digital Identifier Inclusion is a structured document that describes the application and mobile device that protects authentication secrets. The report outlines solutions that are designed to enable all people access to the benefits provided by the evolving digital identifier ecosystem.

All the terms used in this document are included in the [Terms and Definitions Section](#) below.

This report is part of a series of evolving Kantara reports on distributed identifiers that will all be available [at the work group draft recommendations page](#).

1.1.GOALS

The goal of this report is a digital ecosystem where every eligible person can enjoy the benefits of digital identifiers in a secure and privacy-preserving process.

Any person that has any right or privilege under law must be able to acquire digital credentials when they are needed to access those rights and privileges.

The identifier ecosystem must provide a means for recovery of lost credentials that give a person access to their rights and privileges.

The Holder's Wallet holds the protected authentication secrets needed to authorize consent and to intentionally choose to share protected data among verifiers that have communicated a need to acquire, verify, and protect that data.

The Verifiers can clearly identify themselves and their purpose in requesting subject information in a manner that is acceptable to all eligible subjects or their delegate.

The subject may have more than one identifier (persona) to enable compartmentalizing the rights and privileges that each identifier can access.

Digital Identifier Inclusion

1.2.ASSUMPTIONS

The following assumptions on the existence of a trustworthy ecosystem are further described in [section 2](#). The ecosystem itself is not the subject of this report.

The holder has acquired a smart mobile device (such as a smartphone) that can protect the user credentials needed for authentication.

The holder can install a Wallet on that device with a list of Trust Anchors.

- The user is given full control of the Trust Anchors that are used in any transaction.
- Trust Anchors all start with a set of terms and conditions or a Code of Conduct that defines their concept of a trustworthy ecosystem for certificates that are based on the anchor.
- There is a Code of Conduct and a collection of service providers which are registered as compliant and conformant with the code. It is intended that it applies to other digital ecosystems as well.

Other solutions are possible, such as cloud-based wallets that the user can access using biometrics. These are not further elaborated in the document. (Drummond Reed 2023)

The user should have some Identity Assurance Level (IAL), but that is not part of this report.

Issuers of credentials that contain a subject's sensitive personal information will expect the subject to provide a high level of authentication assurance to access that information.

The user will be able to access the identifier and protection levels of any verifier before the user is requested to supply any personal information.

Digital Identifier Inclusion

2. OVERVIEW OF THE PROBLEM

The rapid advance of technology brings with it a promise that technology can improve our lives. Several efforts at creating a “Human-Centric Digital Identity”, including Elizabeth Garber have made a point of saying how the new identity technology “creates broader opportunities for inclusion.” (Garber 2023) The reality is that technological change brings insecurity and confusion to those who are not part of the change process. Poor and marginalized communities do not have the resources or capabilities to purchase the new technology and so are increasingly excluded from the rapidly evolving community that the comparatively well-off creators of these changes call home. And so, they are increasingly falling further behind.

1.1. EXAMPLES OF EXCLUSION

- Women in Identity collected use cases where people were excluded for arbitrary bureaucratic reasons in Kenya and the UK with suggestions on how to overcome these blockers. (Women in Identity, 2022)
- An Indigenous man from the Heiltsuk Nation and his granddaughter were wrongly handcuffed outside a Bank of Montreal branch in Vancouver. Phone transcripts revealed a Bank of Montreal branch manager called emergency services because she thought Johnson and his granddaughter were presenting fake ID cards. (Sterritt, 2022)

“One of the things I keep seeing is my granddaughter standing on that street, crying while she's being handcuffed. I don't think any parent or grandparent should ever see that in their lifetime.”

– Heiltsuk Nation Grandfather

These cases started with problems in existing ID card systems but are further exacerbated by the bureaucracy of getting digital IDs. Where do people go if they cannot get the digital technology to accept their identifier? While the United Nations has declared (United Nations 1948) put “the right to “recognition as a person before the law,” the mechanisms to assure this right are not described. By removing any human element from the identification process, technology has exacerbated the problem of marginalized populations accessing this declared right.

Digital Identifier Inclusion

Technology innovation thrives on creating fast solutions for the 80% of the population that is already technology savvy. This comes from the Pareto Principle that 80% of results can be achieved by addressing 20% of the causes. (Olivia Guy-Evans 2023). That means that a new product can go to market by solving 20% of the causes that prevent the use of the products. This approach is unsatisfactory for a process that requires “recognition as a person before the law” for all people on this planet.

Susan Morrow further describes the difficulty of getting her identity verified in the Think Digital Partners article, “[I had to get my identity verified, and it was a pain](#)” (Stanley, 2023).

1.2.SECURITY VERSUS INCLUSION

Current and proposed legislation requires that the security of the user’s private data as well as access to eligible resources needs to be as well guarded as possible and practical. However, those with special needs as described below may not be able to acquire a device with the most current security hardware and operating system. The following are some of the cases that must be accommodated for a solution to be fully inclusive.

1. The Holder has an older version of a smartphone, perhaps even a second-hand device, and may still have security vulnerabilities that have been fixed in more recent devices.
2. We already know that “Americans with disabilities [are] less likely than those without to own some digital devices” (Perrin 2021) and have the issues mentioned above. Accommodation of these devices may be less secure, but nonetheless important in serving the underserved.
3. The Holder has needs that require a special device that does not meet current standards.
4. Many underserved Holders will not be able to provide high-assurance identifiers.
5. The Holder should be able to access their rights in situations where online security checks are not available when most needed. This is especially true in disasters.
6. The device must support the expected Holder’s languages and abilities where needed. Solutions include initial training and any help screens available to the Holder. While it is not a good plan to rely on the Holder for the security of the device, it is always the case that the Holder can make choices that damage security.

Digital Identifier Inclusion

3. TERMS AND DEFINITIONS

This report uses terminology and definitions from OpenID Connection and other specifications for JSON Web Token (JWT), JSON Web Encryption (JWE), JSON Web Signature (JWS), and JSON Web Keys (JWK). In addition, OAuth [RFC 6749] and other specifications listed in the normative references at the end of this report have defined terms. In all cases, the taxonomy is here simply to clarify the use of the terms in this report.

2.2. TAXONOMY

Assurance = some message that conveys trust in one of the devices or mechanisms that are used in support of digital Identifiers.

Authenticator = some device or process that can be used to prove the subject's ID based on something you have, something you know, or something you are.

Credential = signed data packet from the Issuer, containing verified claims about the Subject.

Credentialed Caregiver = a human or role that is authorized to help any subject that is in their care that needs help using the technology described here.

Delegate = a human or role that is assigned some set of capabilities by the subject.

Digital Public Infrastructure (DPI) is made up of secure and interoperable digital systems that enable the delivery of public services. [DPI represents a potentially transformative force](#) that can shape societies worldwide, making them safe, stronger and more inclusive. (UN 2024)

Eligible Resources = any right, location, privilege, educational materials, job training programs, housing assistance, or services that the Subject could show they have a legal or customary right to access.

Guardian = [a human or role that has statutory capability to control access](#) to the subject's credentials and other data. (See below)

Holder = the person who has control of the phone and of access to the wallet and credentials on the wallet..

Identification Ecosystem = the entirety of the issuers, wallets, holders, subjects, and verifiers that must work together to enable the use of identifiers on mobile devices. See the definition of a [Trustworthy Digital Ecosystem](#).

Digital Identifier Inclusion

Identifier = one of many possible attributes of a subject that is used to link the subject to their rights and privileges.

Indigenous = Separated communities of individuals that were historically resident and typically speak a language that has no legal recognition.

Information = data about any human, attributes, behaviors, interests, tracking, etc.

Issuer = entity that is trusted to issue credentials containing claims and licenses of the subject.

Liveness = assurance that the identified user is present and continues to be present as the transaction evolves.

Local Connection = Interaction modes other than the Internet, like BLE (Bluetooth Low Energy), NFC (Near field Communication), and QR-codes.

Persona = a collection of attributes with distinct identifiers that a person can assume to allow that person to assume different, distinct roles depending on the context of an interchange, for example, to separate work-from-home roles.

Phone = network-connectable, [smart mobile computing device](#) that might not be able to communicate with the network at the time a credential is needed.

Policy

Presentation = the data from one or more credentials that is communicated to the Verifier.

Proof of Presence = typically some biometric evidence that you are the person identified in the data transaction and not someone else. Note that this can be a live image, fingerprint, or other biometric scan and can be provided to the verifier by the Wallet, or the verifier can perform proof of presence directly.

Receipt = signed data packet from the Verifier with the purpose and list of the Subject's credentials and related data that is needed or desired by the Verifier to authorize access.

Registry = trusted list of trusted issuers, wallets, and verifiers needed for the Identifier Ecosystem to function. See the section on [Trustworthy Digital Ecosystem](#).

Subject = the identified person (or persona) that the credential is issued to, maybe the Holder or another User as well.

Trust Anchor = the root of authority for a signing chain used as the source of trust for identifiers.

Digital Identifier Inclusion

User = In this report, the user can be any of the Holder, verifier agent, Subject, or other person in authorized possession of the Phone to complete the consent process.

Verifier = the entity that receives and determines if the subject attribute data is sufficient

Wallet = code running on the phone that will protect PII or authentication secrets and can collect consent and register accesses.

2.3. SMART MOBILE DEVICE

The minimal requirement for a smart mobile device is that it can always be carried on (or within) the person and communicate with issuers and verifiers as needed. It is the source of mobile human digital identifiers and existing digital credentials. There are two categories of smart mobile devices considered here based on existing technologies. Clearly, this list could grow over time.

1. The smart card attached to the device allows for protected storage of user secret identification information. It requires some sort of trusted chip reader and the means to assure that user consent is honored.
2. The smartphone allows protected storage together with a wireless connection that is normally active and a user experience that permits local authentication of the user's presence and consent to share personal data.

2.4. TRUSTWORTHY DIGITAL ECOSYSTEM

It helps to understand how Mobile Assurance fits into the broader picture of a Trustworthy Digital Ecosystem by starting from the top of the trust chain (the root) and working down through any intermediaries to the device or mechanism used in support of mobile identifiers. Each node in the trust chain will create a signed certificate as evidence of their authority to provide a trusted statement.

The simplest form of a digital ecosystem starts with a single **Trust Anchor**, which could be viewed as the one node to “rule them all.” This is the single source of trust from which all other entities in the ecosystem can trace the provenance of their trust.

2.5. GUARDIANSHIP

The terms “[guardian](#)” or “[subject's delegate](#)” are defined elsewhere. A delegation statement is required when one user requests to view or alter information about another user. The purpose of this in an identifier ecosystem is to enable access to digital rights and privileges by those people who do not have the ability to operate digital devices on their own behalf.

Digital Identifier Inclusion

2.6.ACCESSIBILITY AND INCLUSION

The term accessibility comes with pre-existing legal ramifications. It should be noted that in the US all that is required by the Americans with Disabilities Act (ADA) regulation is “Reasonable Accommodation.” The definition of Inclusion in this case is far beyond just “Reasonable Accommodation.” While employers must provide “Reasonable Accommodations” for workers, they are not required to do so if it would impose an undue hardship on the operation of their business.

This document goes well beyond accessibility to insist that all persons who have the right to request a credential must be able to benefit fully from any credential that may be issued digitally that confers that right or privilege. No identifier ecosystem can be considered complete that does not provide access to all eligible people.

2.7.CONSENT, NOTICE, AND AUDIT

The recommended way to ensure that the subject privacy is preserved to their satisfaction is to:

1. Notify the user of the purpose and disposition of any requested user private information.
2. Specifically request (opt-in) any information above and beyond that covered by the purpose.
3. Display the request to the user and ask for informed consent.
4. Preserve all such requests and the consent granted for user inspection.
5. Enable audit of the verifiers’ requests so that compliance can be assured.
6. Notify the user of any changes, including unauthorized access as soon as possible.
7. Disable any right or privilege granted to compromised accounts or tokens.

Notification is not defined here as there may be no channel back to a user, so local regulations apply. The reader is directed to the Kantara ANCR document (Kantara 2018) for detailed information.

Digital Identifier Inclusion

4. DIGITAL PUBLIC INFRASTRUCTURE

This section tracks the (UN 2024) Interim Report on Leveraging DPI for Safe and Inclusive Societies

Key Priorities of Digital Cooperation Achieving Universal Connectivity by 2030

1. Promoting the digital public good creating a more equitable world
2. Ensuring digital inclusion for all, including the most vulnerable
3. Strengthening digital capacity buildout (universal availability)
4. Ensuring the protection of human rights in the digital era
5. Supporting global cooperation on artificial intelligence
6. Promoting trust and security in the digital environment
7. Building a more effective architecture for digital cooperation

Trust and equity are key to how DPI can be leveraged to build a safe and inclusive society. Given the fundamental role DPI can play in delivering public services, it is essential that these services benefit all people in a safe and equitable manner, while ensuring that no rights or privileges are degraded or retrogressive measures adopted. To uphold this, the proper actions needed to build a safe and inclusive society should be embedded across all stages of the DPI life cycle, and integrated into all associated legal and regulatory frameworks and governance mechanisms.

2.8. INCLUSION AS A CATALYST FOR EQUITY

Equity has multiple facets. It implies fair and inclusive access to DPI. The aim is not just to make technology available to everyone; it is about tailoring it to be scalable (up or down) and people-friendly, so that engaging with DPI becomes a seamless experience for all, irrespective of background or resources. Equity underpins all Sustainable Development Goals (SDGs), hence a focus on equity through the DPI life cycle can accelerate achievement of the SDGs. Ultimately, this means ensuring that the disadvantaged and the most vulnerable people can reap the benefits of inclusive and sustainable development. Inclusivity is essential for fostering equity. It can manifest through design choices that solve problems related to identification or biometric failure, for instance. Similarly, inclusivity should be woven into policies that mandate bias assessment in service or product delivery. Inclusivity can also be used to incentivize awareness and digital literacy outreach. For marginalized individuals and communities

Digital Identifier Inclusion

who rely on a government safety net for basic necessities, the consequences of exclusion can be particularly severe and exacerbate existing inequalities.

Digital Identifier Inclusion

5. USE CASES

2.9. SCENARIOS

It is important that scenarios where digital identification is required support every eligible person to which it applies, regardless of their digital capacity and competence. The following long list of potential use cases comes from several sources including the campaign by ID4Africa, which seeks worldwide recognition of the fundamental right and practical necessity of having proof of identity in today's digital age. (ID for Africa 2020) The chosen date of ID Day, September 16, symbolizes UN Sustainable Development Goal 16.9, which aims to provide legal digital identifiers including birth registration to all individuals by 2030. (United Nations 16.9).

1. The bouncer at a bar wants to use their smartphone to check age prior to entry.
2. The unattended door provides access to a protected space.
3. The airport access lines need to know if you have RealID or similar for access.
4. [The holder is blind](#) or cannot read but must be able to understand and exercise her rights and privileges.
5. The Holder does not speak the language of the credential issuer or verifier.
6. The Subject is comatose, and the Emergency Medical Services (EMS) needs some medical history (break the glass).
7. During a disaster the emergency agency wants to deliver services while limiting fraud.
8. During a pandemic, extraordinary actions require extraordinary identification.
9. A Subject who needs emergency care may require a temporary identifier.
10. Law enforcement needs to ensure the holder is eligible to be where they are located.
11. Food or liquor delivery needs proof that the holder is legally able to accept delivery.
12. A homeless teenager with a phone needs to access shelter or social services.
13. A device is assigned to a job, and the user is the person who is taking that shift for that job.
14. Wards of the state that are not competent to demand their own rights have recourse.
15. Holder can take secure control of online assets like financial and health details.
16. Holder is enabled to report incidents without fear of retaliation.
17. Holder can cross the border to trade his produce with ease.
18. Holder can register for school and has a chance to realize her potential.
19. With timely birth registration, Subject will never be invisible.
20. Juan doesn't need to feel helpless but can easily access his disability benefits.
21. Holder can get proper health care based on their medical history.
22. Holder can own a SIM card and stay in touch with loved ones.
23. Subject's vote can count in a free and fair election.
24. Multiple Subjects can be legally employed and gain a proper salary with a family phone.
25. A Subject receives her monthly pension to support her daily needs.
26. Holders can get state-issued privileges, like a new business license.

Digital Identifier Inclusion

27. The holder can register his land ownership and protect his children's inheritance.

Some of these use cases are from the Identity Day website:

<https://www.id-day.org/2023campaign?ref=blog.identity.foundation>

2.10. DATA FLOWS

The following use cases focus on the data passed between the holder and the verifier using a direct wireless connection between their devices, which are imagined as smartphones. The first three provisioning steps are not part of the use cases as they would have occurred earlier. See the following section on user preparation of the device. Note that the holder is the owner of the device, it is possible for the Holder to allow another user on the device. If the verifier needs assurance of the holder, they can ask for proof of presence.

1. Holder gets a personal computing device like a smartphone.
2. A holder may need to load the wallet and may create a biometric proofing scheme for access.
3. Holder requests a subject credential to be securely stored in the wallet.
4. Verifier requests Holder supply information giving notice, authority, and purpose.
5. The Wallet interprets the request and displays a consent screen to the holder.
6. Holder agrees to the request and sends back a packet containing the data they consented to release.
7. Receipts are generated to serve two purposes: the holder has a record; the auditor has a trail.

2.11. GUARDIANSHIP PROBLEMS

All subject's privacy must be accommodated which means that guardians and credentialed caregivers must take responsibility for the duty of care.

In creating resilient and inclusive digital identifier ecosystems, particular attention must be paid to the privacy and duty of care for all subjects, especially those under the guardianship or care of others. This section addresses the challenges and outlines responsibilities to ensure that the privacy and rights of every subject are respected and protected in the digital space.

Responsibilities of Guardians and Credentialed Caregivers

1. **Privacy Protection:** Guardians and caregivers must uphold the highest standards of privacy protection, especially for sensitive Personal Identifiable Information (PII). This includes compliance with relevant data protection regulations and ethical guidelines.
2. **Informed Management of Digital Identifiers:** Guardians and caregivers are tasked with managing the digital identifiers and data entered for those under their care. This

Digital Identifier Inclusion

management should be informed, responsible, and always in the best interest of the subject.

3. **Accessibility and Inclusivity:** [Digital identifier systems must be accessible to all, regardless of their digital literacy or physical abilities](#). Guardians and caregivers should facilitate access and understand the unique needs of those they support.
4. **Ethical and Legal Compliance:** Adherence to ethical principles and legal requirements is absolute. This includes understanding and respecting the rights and privileges of the subject, particularly in contexts where they cannot advocate for themselves.
5. **Feedback and Continuous Improvement:** Encourage and incorporate feedback from guardians, caregivers, and the subjects they represent to continuously improve identifier systems. Feedback is crucial for addressing emerging challenges and adapting to changing needs.
6. **Training and Awareness:** Provide comprehensive training and resources to guardians and caregivers to equip them with the necessary skills and knowledge for managing digital identifiers effectively and ethically.

Ensuring Equitable Access

- **Addressing technological barriers:** Ensure that those with older or less sophisticated devices that are still supported by the manufacturer can still access all rights and privileges.
- **Special Considerations:** Acknowledge and provide for the needs of those requiring specialized devices or accommodations.

Dependencies

1. Verifiers must be trusted before any user information is released.
2. Trust federations can be used to help users make informed decisions.
3. User consent and trust must begin with no user information transferred.
4. Standards exist to collect needed attributes wherever they may be.

2.12. PERSONAS

The following 4 personas were selected as representing the edges of the user space which includes two people that are fully functional in a digital world and two that are not.

1. Abbey, the soccer mom balancing a work life with a family at home and a single smartphone. Abbey's household consists of herself, a spouse and one child.
2. Ichiro, the computer professional

Ichiro works for a large multinational as a contractor at home. He has a laptop issued by the company and his personal phone that he also uses for business purposes. He wants to keep

Digital Identifier Inclusion

his business and personal access separate. His wife has dementia and cannot be relied on to handle her phone by herself.

3. Juan, the severely disabled adult dependent on a support system

Juan's caregiver has a phone that is assigned to Juan as it contains his medical history as well as a care plan that must be followed to ensure his continued health. Juan's phone travels with him whenever he needs to go to the hospital for treatment, which is frequent. The caregivers at all of these locations can access and update data for Juan on his smartphone.

4. Maya, the teenager who is alone on the streets

Maya, a teenager with a malfunctioning kidney, left a home environment that was extremely hostile and lives on the streets where she has a constant struggle to stay safe on cold nights and deal with her continuing kidney disease. She depends on her smartphone for access to social services.

5. Luis, an Indigenous, migrant farmworker

Luis is 34 years old, and lives with a working spouse and an 8-year-old child, they have one smartphone between them, all are on state-sponsored health plans, and both work and have taxes taken from their income, which is not sufficient, by itself, to sustain them. This covers the case of 2 adults and a child using the same phone.

6. Sara – living in a refugee camp.

Sara is a native of Syria age 33 living in a refugee camp in Turkey, trying to get access to the EU, has a smartphone, but cannot always afford the money to keep cell service, can use it at one point in the camp where Wi-Fi is enabled, has no steady income, rudimentary health care provided in camp which has given her an ID card

2.13. RESULTS

Failed Paths:

- Subject has no tolerance for technology and ignores or misunderstands the instructions or the purpose of the exercise.

Post Condition:

Digital Identifier Inclusion

- If validation is accepted by the verifier, the Holder has a phone that can be used for access to any participating resource.

Tracked Results:

- The phone will hold receipts of consent interactions that can be reviewed by the Holder.

2.14. USER PREPARATION OF THE DEVICE FOR SECURE USE

In some cases, the issuer or the verifier will require the holder's device to produce an assurance message along with the other data transmitted from the user. An example is described in [the Kantara Mobile Assurance Statement](#). The following example applies in that case.

Registration Ceremony

The user needs to have installed an app on their Phone before completing this step. The instructions from the Verifier should help the user acquire an app to hold the necessary credential. After the Phone app is running the user will choose to create an identifier and add a binding of that identifier to an appropriate authentication credential. For authentication assurance (AAL2) they will need to establish that their identifier is bound to a private key held in the Trusted Execution Environment on the Holder's device. Any User Agent needs to have its own certificate informing the supplier and verifier that the app can be trusted to reliably report this information as well as user consent to proceed. The application MUST provide information to the device Policy to prevent use of the application by anyone other than the subject or guardian. The following is an example of one implementation of the user experience in providing proof that they are entitled to access their personal data on the site of any data controller.

2.15. CONCLUSIONS AND DESIRED RESULTS

One semantic problem needs to be clear; the nouns "person" and "subject" do not always reference human beings. Sometimes the term "natural person" is used to represent a human. In large part the problems with the evolving ecosystems, the standards that define them and the laws that govern them are not designed to accommodate all of the actual living humans. In fact, some of the existing standards, like the Decentralized Identifiers defined by the W3C are specifically designed to avoid this distinction as they assert (without providing evidence) that this improves the "herd privacy" of actual humans.

Digital Identifier Inclusion

If the standards and laws do not recognize the unique needs of representing all humans in digital ecosystems, it is certain that they will not accommodate all humans into that digital ecosystem. This paper deals with the rights and privileges of all humans and how the evolving digital ecosystem must accommodate all humans.

The statements made in this document are designed to make the case that whatever rights and privileges might be expressed in digital formats, all people who are eligible for those rights and privileges must be accommodated in those digital formats if they are to be considered as viable replacements for the pre-digital systems deployed today.

We have given a few examples above, but the real work needs to be done on the standards and applications now in development. In the following we will list a few specific cases now in development and point out their deficiencies with regard to inclusion. It isn't that these examples are any worse than others now in development, but just so that there can be some concrete examples of the work yet to be done.

1. EU Digital Wallet does not appear to provide any consideration for people that are not fully digitally literate with a working smartphone. There appears to be no protection if that device is not available and working on a network at the time of a request by the verifier. Note that the eID card is available and does cover most use cases that do not require delegation. One possibility is that the eID card will be accommodated somehow in a wallet. Designs are still in development.
2. Pan-Canadian Trust Framework™ Trust Registries as defined in the [Trust Framework | Digital ID & Authentication Council of Canada \(diacc.ca\)](#) is entirely about stakeholders except for the following: “Canadian citizens and consumers, i.e. end users, are the beneficiaries of trust that will be achieved through service standardization and accountability to the PCTF.” There is no statement about how eligible humans will be accommodated, only about how they can be excluded if they do not meet the requirements of the stakeholders. The impact is that “eligible citizens and consumers” cannot expect that any of their rights or privileges will be in any way protected by the Trust Registries. The implication seems to be that either you have a smartphone on which you know how to keep the credentials safe or that any of the stakeholders can exclude you and you have no recourse to their decision.
3. [Swiss Federal Identifier](#) does require affirmative actions similar to that in the US ADA, but not any extraordinary efforts to include all eligible people regardless of their

Digital Identifier Inclusion

ability. It is still better than the existing efforts in the EU or Canada.

4. The US (NIST 2022) SP 800-63-4, Digital Identity Guidelines now in draft form “specifically mandates that agencies account for impacts to individuals and communities in addition to impacts to the organization”. The draft also mandates that federal agencies “support enterprise risk management efforts and encourage informed, inclusive, and human-centric service delivery. ... including challenges to providing services to all people who are eligible for and entitled to them.” The last comments were accepted on 2023-04-14 and an update is expected in 1Q 2024 and will adopt the issuer-holder-verifier model used in ISO. (NIST 2023) It is likely that the mandate to be inclusive has proven to be harder than was expected.

The following quote is from that draft: “Equity as defined in Executive Order 13985, Advancing Racial Equity and Support for Underserved Communities Through the Federal Government [EO13985], refers to the consistent and systematic fair, just, and impartial treatment of all individuals, including individuals who belong to underserved communities that have been denied such treatment, such as Black, Latino, and Indigenous and Native American persons, Asian Americans and Pacific Islanders, and other persons of color; members of religious minorities; lesbian, gay, bisexual, transgender, and queer (LGBTQ+) persons; persons with disabilities; persons who live in rural areas; and persons otherwise adversely affected by persistent poverty or inequality.”

Digital Identifier Inclusion

6. REFERENCES

- Elizabeth Garber, M. H. (2023). *Human-Centric Digital Identity*: Open ID Foundation et al.
Retrieved from
https://openid.net/wp-content/uploads/2023/09/Human-Centric_Digital_Identity_Final.pdf?ref=blog.identity.foundation
- GSMA (2019) The Digital Lives of Refugees: how displaced populations use mobile phones and what gets in the way
<https://www.gsma.com/solutions-and-impact/connectivity-for-good/mobile-for-development/blog/the-digital-lives-of-refugees-how-displaced-populations-use-mobile-phones-and-what-gets-in-the-way/>
- Olivia Guy-Evans, *Pareto Principle (The 80-20 Rule): Examples & More* 2023-09-21
<https://www.simplypsychology.org/pareto-principle.html>
- Identity Day. 2023 Social Media Campaign. Retrieved from
<https://www.id-day.org/2023campaign?ref=blog.identity.foundation/> on October 31, 2023.
- IEEE SA User-Centered Approach to Designing a User Interface for Rural Communities Industry Connections Activity Initiation Document (ICAID) (2021-05-11)
https://standards.ieee.org/wp-content/uploads/import/governance/iccom/IC21-004-Designing_a_User_Interface_for_Rural_Communities.pdf
- ID for Africa *Spotlight on Inclusion* 2020-09-16
https://id4africa.com/2021/files/LiveCast_6_Spotlight_on_Inclusion.pdf
- Kantara (2018) Consent Receipt Specification Version 1.1.0
<https://kantarainitiative.org/download/7902/>
- Stanley, Matt. (2023-09-27). I had to get my identity verified, and it was a pain. Web. Think Digital Partners. Retrieved from
<https://www.thinkdigitalpartners.com/guest-blog/2023/09/27/i-had-to-get-my-identity-verified-and-it-was-a-pain/>.)
- NIST (2022) *Digital Identity Guidelines* NIST SP 800-63-4 ipd
<https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-4.ipd.pdf>
- NIST (2023-12-12) A Note on progress...NIST's Digital Identity Guidelines
<https://www.nist.gov/blogs/cybersecurity-insights/note-progressnists-digital-identity-guidelines>

Digital Identifier Inclusion

Andrew Perrin and Sara Aske (2021-09-10, *Americans with disabilities less likely than those without to own some digital devices*

<https://www.pewresearch.org/short-reads/2021/09/10/americans-with-disabilities-less-likely-than-those-without-to-own-some-digital-devices/>

Drummond Reed (2023). *EP001 - Unveiling Bhutan's National Digital Identity Ecosystem*.

(un)Trustables Podcast. Retrieved 12 2023, from

<https://untrustables.simplecast.com/episodes/ep001-bhutan-has-launched-a-national-digital-identity-program>

A. Sterritt (2022). *Heiltsuk man, granddaughter handcuffed outside Vancouver bank settle human rights case against police*. Vancouver: CBC. Retrieved from

<https://www.cbc.ca/news/canada/british-columbia/maxwell-johnson-granddaughter-human-rights-complaint-vancouver-police-1.6598580>

United Nations. (1948) Universal Declaration of Human Rights. Web. Retrieved 2023-11-01

from <https://www.un.org/en/about-us/universal-declaration-of-human-rights>

United Nations 16.9 Promote peaceful and inclusive societies for sustainable development, provide access to justice for all and build effective, accountable and inclusive institutions at all levels

https://sdgs.un.org/goals/goal16#targets_and_indicators

Women in Identity. (2022). *Code of Conduct: The Human Impact of Identity Exclusion*.

Women in Identity. Retrieved from

<https://silkstart.s3.amazonaws.com/f024b533-68d2-4a1c-ad5f-7db12c05f36d.pdf>