

Digital Identifier Inclusion

**Version:** 1.0.0

**Date:** 2023-10-31

**Editor:** Tom Jones

**Contributors****:** Bev Corwin, Salvatore D’Agostino, Jim Kragh, Tom Sullivan, Noreen Whysel, Tom Jones

**Produced by:** Kantara Work Group: Resilient Identifiers for Underserved Populations

**Status:** Draft 3

This document is the designed as a Report produced by the Resilient Identifiers for Underserved Populations (RIUP) Work Group (refer to the [Kantara Initiative Operating Procedures](https://kantarainitiative.org/confluence/display/GI/All+Policies?preview=/37750179/104600198/KI%20Operating%20Procedures%20Version%203.0.pdf) for more information on Kantara Reports, Recommendations and Specifications). It is published in this state so that it can be implemented so that implementors can feed back valuable insights that inform a formal Specification. Comments should be directed to: [TK](https://github.com/KantaraInitiative/DistributedAssurance/issues)

**Abstract:** The goal of this report is to describe the minimal features of a smart mobile device that can hold information about any human subject that allows that subject to access all the rights and privileges provided by an evolving digital ecosystem. Government regulations are needed to assure that no eligible person can be denied access to any of their rights and privileges by 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 ecosystem at large.

**Notice:** Copyright (c) 2023 Kantara and the persons identified as the document contributing authors. All rights reserved.

This document is subject to the [Kantara IPR Policy option Non-Assertion Covenant](https://kantarainitiative.org/confluence/display/GI/Option+Non-Assertion+Covenant)

**Suggested Citation:** *Digital Identity Inclusion Draft 0 Kantara Initiative Report from the* Resilient Identifiers for Underserved Populations (RIUP) Work Group .

# Introduction

This concept of **Digital Identifier Inclusion** is described here along with several use cases. No person creates their 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 is a collection of [Verified Claims](https://tcwiki.azurewebsites.net/index.php?title=Verified_Claim) that they can call upon as needed in their online interchanges to protect access to and distribution of their personal information.

This specification is designed to work with devices that are carried with the user and have the capability to be network attached, such as a smartphone.

This specification is a part of a series of evolving Kantara specifications on distributed identifiers that will all be available [at the work group draft recommendations page](https://kantarainitiative.org/confluence/display/WT/Draft+Recommendations).

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 specification.

Wallets come with a list of Trust Anchors that can be amended by the holder of the device.

Trust Anchors all start with a set of terms and conditions or a [Code of Conduct](https://wiki.idesg.org/wiki/index.php/Code_of_Conduct) that define their concept of a trustworthy ecosystem for certificates that are based in the anchor.

* There is a Code of Conduct, a trust anchor and a collection of service providers which are registered as compliant with the code.
* It is intended that it apply to other digital ecosystems as well.
  + The user has acquired a smart mobile device (such as a smartphone) that can protect the user credentials needed for authentication.
  + The user should have some level of identity assurance (IAL), but that is not part of this specification.
  + Issuers 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 identity and protection levels of any verifier before the user is requested to supply any personal information.

## Goals

This Digital Identifier Inclusion is a structured document that describes the application and mobile device which protects authentication secrets.

The goal for this specification is to enable a mobile device to support all eligible subjects in a secure and privacy-preserving process. Where eligibility is defined by terms of the credential desired.

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

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

The holder wallet holds the protected authentication secrets needed to give consent to intentionally choose to move protected data among verifiers that have communicated a need to acquire and protect that data.

The verifiers can use this Digital Inclusion Statement to show due diligence in authenticating user’s before sharing access to stored personal information.

The subject may have more than one identifier as required by the rights and privileges that they can access.

# What’s 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” (Elizabeth Garber, 2023) have made a point of saying how the new identity technology “creates broader opportunities for inclusion” The reality is that technological change brings insecurity and confusion to those who are not part of the change process. In particular, poor and marginalized communities do not have resources or capabilities to purchase the new technology and so are increasingly excluded from the rapidly evolving community that the well-off creators of these changes call home. And so, they are increasingly falling further behind. Some examples include: Women in Identity has 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 Idenity, 2022) An Indigenous man from the Heiltsuk Nation and his granddaughter were wrongly handcuffed outside a Bank of Montreal branch in Vancouver, His response: “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,” Phone transcripts revealed a BMO branch manager called 911 because she thought Johnson and his granddaughter were presenting fake ID cards. (Sterritt, 2022) These cases started with problems in existing ID card systems but get further exacerbated by the bureaucracy of getting digital IDs. Where do people go who cannot get the digital technology to accept their identity? While the United Nations has declared “the right to “recognition as a person before the law,” the mechanisms to assure this right are non-existent. By removing any human element from the identification process, technology has exacerbated the problem of marginalized populations accessing this declared right.

Technology innovation thrives on creating fast solutions for the 80% of the population that is already technology savvy. This approach is unsatisfactory for a process that requires “recognition as a person before the law” for all people on this planet.

I had to get my identity verified, and it was a pain

<https://www.thinkdigitalpartners.com/guest-blog/2023/09/27/i-had-to-get-my-identity-verified-and-it-was-a-pain/>

# Terms and definitions

This specification uses terminology and definitions from OpenID Connection and other specifications for JWT, JWE, JWS and JWK. In addition, OAuth **[RFC 6749]** and other specifications listed in the normative references at the end of this specification have defined terms.

Taxonomy

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 that can access any subject’s data that is in their care

Guardian = a human or role that has statutory ability to control access to the subject’s credentials and other data. (See below)

Holder = the person that “owns” the phone and has control of access (ISO 18013-5)

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

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

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

Local Connection = Other interaction modes like BLE, NFC, QR

Phone = network connected mobile computing device that may be unable to communicate at the present time

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

Proof of Presence = typically some biometric evidence of something you are. Note that this can be provided to the verifier by the Wallet, or the verifier can perform it themselves.

Receipt = signed data packet from the Verifier with purpose and list of the Subject’s credentials and related data.

Registry = trusted list of trusted issuers

Subject = the person that the credential is issued to, may be the holder

User = person the holder shared the phone with (friend or family member)

This is the human that is asked for consent to release data on subjects, usually the holder.

Verifier = the entity that receives and determine if the subject information is sufficient

Verified Claim = any attribute or license that has been issued to the subject.

Wallet = code running on the phone that will protect PII or authentication secrets and can collects consent

## Smart Mobile Device

1. The minimal requirement for smart mobile devices is that it can always be carried on (or in) the person. It is the source of any human digital identifiers and existing digital credentials.
2. There are two categories of smart mobile devices considered here based on existing technologies. Clearly this list could grow over time.
3. The smart card allows for protected storage of user secret identification information. It requires some sort of trusted chip reader to assure that user consent is honored.
4. The smart phone 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.

## 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 and working down.

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. This is not about the centralized naming system of the internet, which will be assumed to be in operation, but rather about the trust that one node of the network can have with other nodes.

## Guardianship

The terms [guardian](https://wiki.idesg.org/wiki/index.php/Guardian) or subject’s delegate are defined in the documents that can be accessed at that site. In general, a delegation statement is required when one user requests to view or alter information about another user.

## Accessibility

The term accessibility comes with pre-exiting legal ramifications. It should be noted that in the US all that is required by the US ADA is “Reasonable Accommodation.” The definition of Inclusion in this document goes well beyond that 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 confer that right or privilege.

# use caseS

This section serves two purposes: the first is an attempt to show the broad range of the underserved with special needs that must be addressed by an inclusive society, the second is a deep dive into four personas that explore not only two use cases of the underserved, but also to personas that are involved in support of special needs relatives of theirs. In other words, this section involves the underserved as well as the people who are living with those who need special attention by the evolving identifier technology.

In all cases, the device holder presents credential data to an enterprise or to a care giver **or delegate** working on their behalf.

* Enterprises can be federal government agencies or just the local pub.
* For this discussion the user agent will be called a wallet, it protects user secrets.
* The relying party will be called a verifier which is typically contained in a mobile smartphone.
* This document only addresses use cases where the internet is not always available.

Scenarios

The following long list of potential use cases were collected from several sources including the campaign by ID4Africa seeks worldwide recognition of the fundamental right and practical necessity of having proof of identity in today’s digital age. The chosen date symbolizes UN Sustainable Development Goal 16.9, which aims to provide legal identity including birth registration to all individuals by 2030.

1. The bouncer at a bar wants to use their smart phone 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 Real ID or similar for access.
4. The user is comatose and the EMT (ambulance) needs some history (break the glass)
5. During a disaster the emergency agency wants to deliver services while limiting fraud
6. During a pandemic extraordinary actions require extraordinary identification.
7. A person that needs emergency care may require a temporary identifier.
8. Law enforcement needs to assure the holder is eligible to be where they are located.
9. Food or liquor delivery needs proof holder is legally able to accept delivery.
10. A homeless teenager with phone needs to access shelter or social services.
11. A device is assigned to a job, and the user is the person who is taking that shift for that job.
12. Wards of the state that are not competent to demand their own rights.
13. With his identity, Josias can cross the border to trade his produce with ease.
14. With her identity, Maya is registered for school and has a chance to realize her potential.
15. With timely birth registration, Akina will never be invisible.
16. With her identity, Sumita owns a bank account and is financially empowered.
17. With his identity, Juan doesn't need to feel helpless but can easily access his disability benefits.
18. With her identity, Evelyn can get proper health care.
19. With her identity, Liu Ming can own a SIM card and stay in touch with loved ones.
20. With his identity, John's vote can count in a free and fair election.
21. With his identity, Ivan can be legally employed and gain a proper salary.
22. With her identity, Nobantu receives her monthly pension to support her daily needs.
23. With her identity, Clara can register her new business license.
24. With his identity, Issac can register his land ownership & protect his children's inheritance.

Use Cases from the Identity Day <https://www.id-day.org/2023campaign?ref=blog.identity.foundation>

## Data Flows

These use cases focus on the data passed between the holder and the verifier using a direct wireless connection between their devices, which are imaged 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..

Holder gets a personal computing device like a smartphone.

Holder may need to load wallet and may create biometric proofing scheme for access.

Holder requests a subject credential to be securely stored in the wallet.

Verifier requests Holder supply information giving notice, authority and purpose.

Wallet interprets the request and displays a consent screen to the holder.

Holder accepts for the subject of the request and sends back a data packet.

Receipts are generated to serve two purposes: the holder has a record; the auditor has a trail.

## 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.

### Abbey the soccer mom balancing a work life with a family at home.

Abbey’s household consists of her, a spouse and one child with a smart phone and one that is too young to trust with a smartphone and is about to enter school for the first time.

### 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 is used for business purposes. He wants to keep his business and personal access separate. His wife has dementia and cannot be relied on to handle her phone by herself.

### 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 assure 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.

### Maya the teenager that is alone on the streets

Maya 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 continuing kidney malfunction. She depends on her smart phone for access to social services.

Problems

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

## Results

Failed Paths:

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

Accepted Risks:

1. The Patient loses the paper allowing some other person to attempt to steal their identifiers - mitigated by sign up process as described.
2. Recovery TK

Post Condition:

1. If validation accepted by the CSP, the Patient has a phone that can be used for sign-into any participating healthcare provider.

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 where-ever they may be.

## User Preparation of the Device for Secure Use

This message is sent by a user agent app on the user’s phone with some information known to the user to assure the CSP that the message comes from the user, and a software statement to indicate the level of protection and user-presence is adequate assurance of authentication level 2 (AAL2).

Registration Ceremony

The user needs to install the app on their mobile device before completing this step. The instructions from the EHR will tell the user how to acquire the app from the app store specific to their phone supplier. After the agent app is running the user will choose to create an identifier and add a binding of that identifier to the CSP. For IAL2 they will need the DIA code from the EHR as described above. 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 Phone, called the KeyStore on Android. The Agent needs to have its own certificate informing the CSP 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 CSP to prevent use of the code by anyone other than the Patient or guardian. The following is an example of one implementation of the user experience in providing proof that they are entitled to access the EHR record on themselves.

# 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

Sterritt, A. (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

Women in Idenity. (2022). *Code of Conduct: the Human Impact of Identity Exclusion.* Women in Idenity. Retrieved from https://www.womeninidentity.org/cpages/code-of-conduct

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> User-Centered Approach to Designing a User Interface for Rural Communities Industry Connections Activity Initiation Document (ICAID)