

Digital Identifier Inclusion

**Version:** 1.0.0

**Date:** 2023-09-19

**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:** First Draft

 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%2BPolicies?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 them 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.

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%2BNon-Assertion%2BCovenant)

**Suggested Citation:** *Digital 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%2BRecommendations).

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 mobile computing 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 the user’s authentication secrets.

The goal for this specification is to enable a mobile device to support all eligible users in a secure and privacy-preserving process.

The holder wallet holds the protected authentication secrets they need 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.

# 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

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

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.

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

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

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

Issuer = entity that is trusted to issue creds

Registry = trusted list of trusted issuers

Phone = network connected mobile computing device that may be out-of-range

Local Connection = Other modes like BLE, NFC, QR

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

Credential = signed data packet from the Issuer about the Subject

Presentation = the data from the credential that is communicated to the Verifier

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

TK bio & authenticator TK

## Smart Mobile Device

The minimal requirement for smart mobile devices is that it can always be carried on the person. It is the source of any 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 allows for protected storage of user secret identification information. It requires some sort of trusted chip reader to assure that user consent is honored.
2. 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.

# use caseS

(This section is non-normative)

Scenarios

Generally, the device holder is presenting credential data to an enterprise.

* 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.
* We will only address the use cases where the internet is not always available.

The bouncer at a bar wants to check age prior to entry.

The unattended door provides access to a protected space.

The airport access lines needs to know if you have Real ID or similar for access.

The user is comatose and the EMT (ambulance) needs some history (break the glass)

During a disaster the emergency agency wants to deliver services while limiting fraud

Law enforcement needs to assure the holder is eligible where they are located.

Food or liquor delivery needs proof holder is legally able to accept delivery.

A homeless teenager with phone needs to access shelter or social services.

Failed Paths:

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

## Results

Accepted Risks:

1. The Patient loses the paper allowing some other person to attempt to steal their identity - 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 in to 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 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 chose 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.

**User Consent**

Note – must have notification address email or SMS phone number

The following is a non-normative example of what might be displayed to the user. This is only used to verify that this is the user that is identified in the activation code.