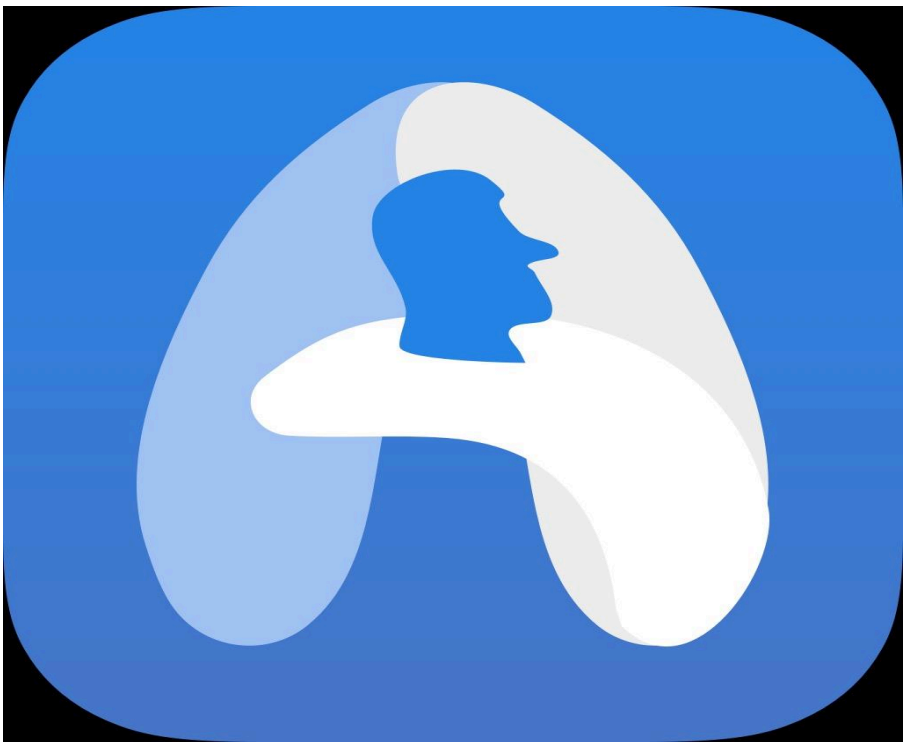
White Paper

DigiPort.me

Simplifying the world of digital identity



Executive Summary

DigiPort is a digital identity platform that empowers users to locally store and globally share attested identity data. Users have the ability to import their information from a variety of *Aggregates*—information providers—available to them, and share them with a variety of *Connectors*—service providers—on the platform. As the owners of their data, users can selectively share their identity data for onboarding or accessing data in a fraction of a time formally needed.

Developers can use our templates or create their own Connectors on our platform using our easy-to-use SDKs, allowing them to request specific pieces of attested information from the user for onboarding or compliance. For example, a bank in the United States could use one of our default setups or create a Connector to request a user's name, address, phone number, SSN, and a binary question on whether they have the right to open a bank account in the country. The user will receive a push request listing the information requested by the bank and asked whether they agree to sharing them. Through this process, Identifying Me allows entities to drastically cut the friction involved in onboarding new users, and the possibility of fraud—whether in person or online. We provide the necessary infrastructure to make the creation of Connectors a simple and seamless process that only takes minutes to set up.

The platform provides individuals with a significantly higher level of sovereignty over their data than they have come to expect from traditional identity platforms. Users are offered the opportunity to choose from a variety of information providers that offer social, financial, legal, educational, and medical data, amongst other things; allowing them to experience a more fluid and intuitive user experience.

Traditionally, dealing with onboarding has been a complicated matter. When an entity needs information from a user, especially in an online setting, they've had to outsource the demand or manually conduct it in-house, both of which are costly and time consuming, resulting in losing customers. Users have also had the burden of sharing much more information than they feel comfortable sharing, and suffering the consequences of data breaches. At Identifying Me, we strive for a frictionless user experience, especially in our highest value user flows. Frustrated with the current state of affairs, our team is committed to building a GDPR ready, Know your Customer (KYC)/ Anti-Money Laundering (AML) compliant ecosystem that alleviate these concerns.

We are a platform that is pro privacy, pro autonomy, and pro user-control. Whether an initial coin offering (ICO), a fiat exchange, or a city election office, entities can now use our platform to comply with all necessary government regulations without having to handle and store excess user data. Users on the other hand can use our platform knowing that their data is processed locally on their device and that they'll be explicitly warned if data ever has to leave their device.

A Portable Identity You Can Trust

At the moment, our digital identities are spread across the web, owned and operated by central repositories of data such as Facebook and our email providers. As users, we have very limited control over how our data is used and who it's shared with. Furthermore, central data repositories are highly vulnerable due to their susceptibility to large scale breaches which is why they are often described as a *honeypot* within the hacker community.

We believe users should be the owners of their data and have the ability to safeguard it's security. As a result, on our platform personally identifiable information (PII) is always stored locally on a user's device and the ownership of that data belongs to the user. A user has the ability to delete their information and to securely share it with outside parties.

We believe in the vision of Self-sovereign Identity (SSI)—an idea that empowers individuals by returning the ownership of their identity to them. We strive to integrate cutting-edge platforms such as uPort to remove the identity barrier for the traditional and decentralized web.

The Barriers to a Better Future

An identity verification process should be **thorough**, yet **low-anxiety**, and **unintrusive**. Ideally, the process should be fast, flexible, and nearly invisible while providing the assurance of privacy and security. The lack of standardized methods for identity verification, especially on the web adds to this complexity. Here are a few problemes, we're currently faced with in the world of digital identity:

- **User Privacy:** In the times of GDPR, Facebook data sharing controversy, and the large amounts of profit generated by collecting customer data, users need a platform they can trust and feel comfortable storing identity data on.

- **Data Security:** Numerous highly publicized data breaches such as the Equifax and Yahoo hacks are putting users personal, financial, and digital life at the risk of fraud.
- **Re-verification:** If someone's identity is stolen, then their data can be used to make financial transactions or give consent to matters they are unaware of, as a result companies should re-verify their customers.
- **Regulatory Requirements:** Traditional financial institutions spend at least 10% of their operating budget on compliance.

These problems are significant and an important hurdle to overcome. The good news is that the tools and infrastructure for addressing them are available.

The vision

We are determined to solve the problems that are causing friction and frustration in the word of digital identity. We are doing this by:

- Creating a range of possible manners by which users can provide verification of their identity—referred to as *Aggregates*. Depending on the requirements of the platform and the preferences of the users, a user can import medical, financial, social, and biometric data onto their device. These feature offers more freedom and flexibility to the user while offering enterprises the data they need for their business.
- Making it easy for enterprises to request user data through the use of *Connectors* or our templates. By providing an SDK that developers can use to create a custom configuration or using one of our many default templates depending on the industry, an enterprise can request user data and offer their services.
- Locally storing and encrypting user data, and offering users the right to be forgotten and deleting their data records.
- Offering the option of generating a keypair on the blockchain as a proof of identity.

Data we can trust

There is a fair amount of reliable information already available about most people. Some of it is information provided by the state, and some of it are financial, social, and medical information available through 3rd parties.

Depending on the preferences of a user, our platform allows for storing an aggregate of all this information locally on a user's device. Importing information is performed through the integration of API's provided by these 3rd parties into our application. For example, a user living in the U.S. can use the Cognito and Plaid APIs to import and securely store their financial information and their Social Security Number on their device, allowing them to use a service that requires KYC/ AML compliance.

Credentials

Credentials (also referred to as attestations), are signed JSON Web Tokens (JWT) that are locally stored on a users device. They are provided to users by Trust Anchors and can be traced to the source to check for reliability. A JWT can store a wide variety of identity data, and shared with other individuals or entities for onboarding or access.

Connectors

Connectors are created on our platform through the SDK we provide developers. A user can browse through a store of connectors and pick the ones they would like to use to selectively share their identity information with.

Connectors utilize a user's identity to instantly provide access to services or verify their identity. For example, Synchrony Financial's connector can request a users financial and location data, and issue a retailer's credit card immediately after a user consents to sharing the information.

Goals

- To create a drag-n-drop identity verification system for institutions that is simple, secure, and compliant with government regulations.
- To provide a service that is committed to user privacy and the security of their data.
- To build an ecosystem that allows enterprises to offer their users with new services.

Platforms and Records

The aggregates below are incorporated into our platform to provide users with the opportunity to import attested identity information.

Aggregate Platforms	**Information Provided**
Digi.me	Financial, Medical, Social, Fitness & Health, Music & Entertainment
Plaid	Financial
Government	FBI Blacklist, Background Check, IRS
Open.epic	Public Health, Financial, Clinical,
Plaid (US), Yodlee (Canada, Australia)	Financial
LinkedIn	Social
Facebook	Social
????	Biometric
Experian	Financial, Credit History
Twilio	Phone Number Verification
Cognito	Social Security Number
Smartphone	Location Data, Face Recognition

All the credentials mentioned in the table above will be imported as a signed JSON Web Token (JWT), and encrypted locally on your phone. You'll have the ability to update your information over time, and share it with 3rd parties through the Connectors. In addition to the credentials above, as a user, you can import proofs such as your Driver's Licence and Passport to the platform.

In the table below, I am listing an example of few connectors we hope to build on our platform.

Connector Platforms	**Use case**
uPort	Self-sovereign Identity
Hyperledger Indy	Digital Identity
Synchrony Bank	Retail Credit Card Provider

Fiat Exchange	An online fiat currency exchange
CryptoAsset Exchange	An online digital currency exchange

New Possibilities

The Web of Trust

To illustrate why our approach and philosophy allows for new innovations, I will use an example we're all familiar with, the concept of Sign Sign-On. Most of us use a universal login at least for a few of our apps and accounts. It's simple to click on "login with Facebook" instead of creating a unique identifier for each platform; however, as we witnessed with the Facebook hack where 70 million records were exposed, central repositories of data are too vulnerable. Furthermore, most consumers would likely feel uncomfortable using central entities to access sensitive platforms such as their bank account. On our platform, you can import your credentials from a *Trust Anchor*, and export that to an SSI platform like uPort, once completed, you can use your uPort identity to login to your favorite services and apps without the limitations of traditional platforms, thus the possibilities are vastly expanded.

Countries of Operation

For our initial release, we are focusing on the U.S. and Canadian markets. Afterwards, we are looking at expanding into India, Mexico, and Australia. Some of our API's already provide services in numerous countries, and if you have business needs in other nations, we'd be happy to look into it.