COVID-19 Digital Passports and Verifiable Credentials Specification

Digital verification of vaccination will be an essential tool to opening economies and transportation systems as we work to get the COVID-19 pandemic under control. How these vaccination verification systems are designed and deployed is critical.

Careful consideration should be given to human factors, existing behaviors and workflows, equity, trust and privacy and patients should be able to opt-in to any digital passport system. Such standards should provide enough structure to facilitate broad adoption but not so much as to create implementation hurdles.

Digital vaccination verification should not store personally identifiable data in the credential registry. Instead, an encrypted key should be issued at the point of vaccine administration to the patient, or thereafter, and would be stored in the credential registry system.

# Overview

Digital tools are already playing a role in [how countries are granting access to individuals for travel](https://www.bahamas.com/pressroom/the-islands-of-the-bahamas-announces-updated-travel-and-entry-protocols?page=pressroom), how at-home test manufacturers are [providing diagnostic results](https://www.abbott.com/BinaxNOW-Test-NAVICA-App.html), and [how universities are checking the health status of students](https://www.clemson.edu/covid-19/testing/index.html) and staff.

In some situations, a tool may be used to solely provide proof of vaccine credentials. However, in other situations, a technical solution may need to combine vaccination and testing credentials to show that someone is both protected from illness due to COVID-19 by a vaccine and also not a risk for transmitting COVID-19 to others.

It will take months in some countries, and years globally, for communities to reach a level of vaccination that can be considered adequate to protect the community as a whole from significant disease transmission. In some situations, an entity may only require a vaccination credential. However, science is still developing around whether or not, and how much, those who have been vaccinated can continue to transmit disease to others even if they do not get sick themselves. Therefore, needing to show evidence of either the absence of current infection, the presence of prior infection or both will still be relevant as communities move towards reaching herd-immunity levels of vaccination. Testing credentials will also stay relevant for those without early or ready access to vaccination.

To complement (in addition to) or supplement (in place of) a digital vaccine credential, a digital testing credential can consist of the following, and may need to consist of both:

**Evidence of absence of current infection:**

* A negative diagnostic test credential (PCR, antigen test, NAAT or others) that can remain valid for 3 days after the test date.

**Evidence of presence of prior infection:**

* A positive diagnostic test credential that can become active 14 days after the test date, and remain valid for 90 days.
* A positive antibody test credential that can remain valid for 90 days after the test date.

## Proposed Solution

Fortunately, a set of globally recognized standards already exist and can serve as the foundation of a digital credential solution:

* [**Decentralized Identity Specification**](https://www.w3.org/TR/did-core/)**—**Authored by the [Decentralized Identity Foundation](https://identity.foundation/), this specification provides a standard for interoperable digital identities at scale.
* [**W3C Verifiable Credentials**](https://www.w3.org/TR/vc-imp-guide/)**—**Used in conjunction with decentralized identifiers, this specification provides a way to represent, prove, and verify credentials held by an individual without exposing all personal details. Examples of credentials include proof of vaccination, negative COVID-19 test results, proof of status as a healthcare provider, etc.
* [**Decentralized Distributed Ledger Technology**](https://en.wikipedia.org/wiki/Distributed_ledger)**—**Commonly referred to as “blockchain technology”, a distributed ledger provides a way to store an immutable log of data replicated all over the world without a single owner or point of failure. When combined with decentralized identity components and cryptography, data can be safely made available on a global set of nodes while protecting privacy and maximizing scalability.
* [**Interplanetary File System (IPFS)**](https://ipfs.io/)**—**IPFS provides a way to decentralize the storage of data files in the same manner as a distributed ledger. These data files, in this context, are those that provide evidence of valid credentials (e.g., PDF’s of negative COVID-19 test results, pictures of COVID-19 vaccination cards, and diplomas proving graduation from medical school).
* [**Fast Healthcare Interoperability Resources (FHIR)**](https://www.hl7.org/fhir/overview.html)**—**FHIR is a standard interface for integration with EMR systems that contain patient medical data. This includes vaccine requests and records, laboratory test results, etc. Integrating directly with EMR systems can automate the verification of vaccine and COVID-19 test credentials for organizations that support the standard.

## Implementation

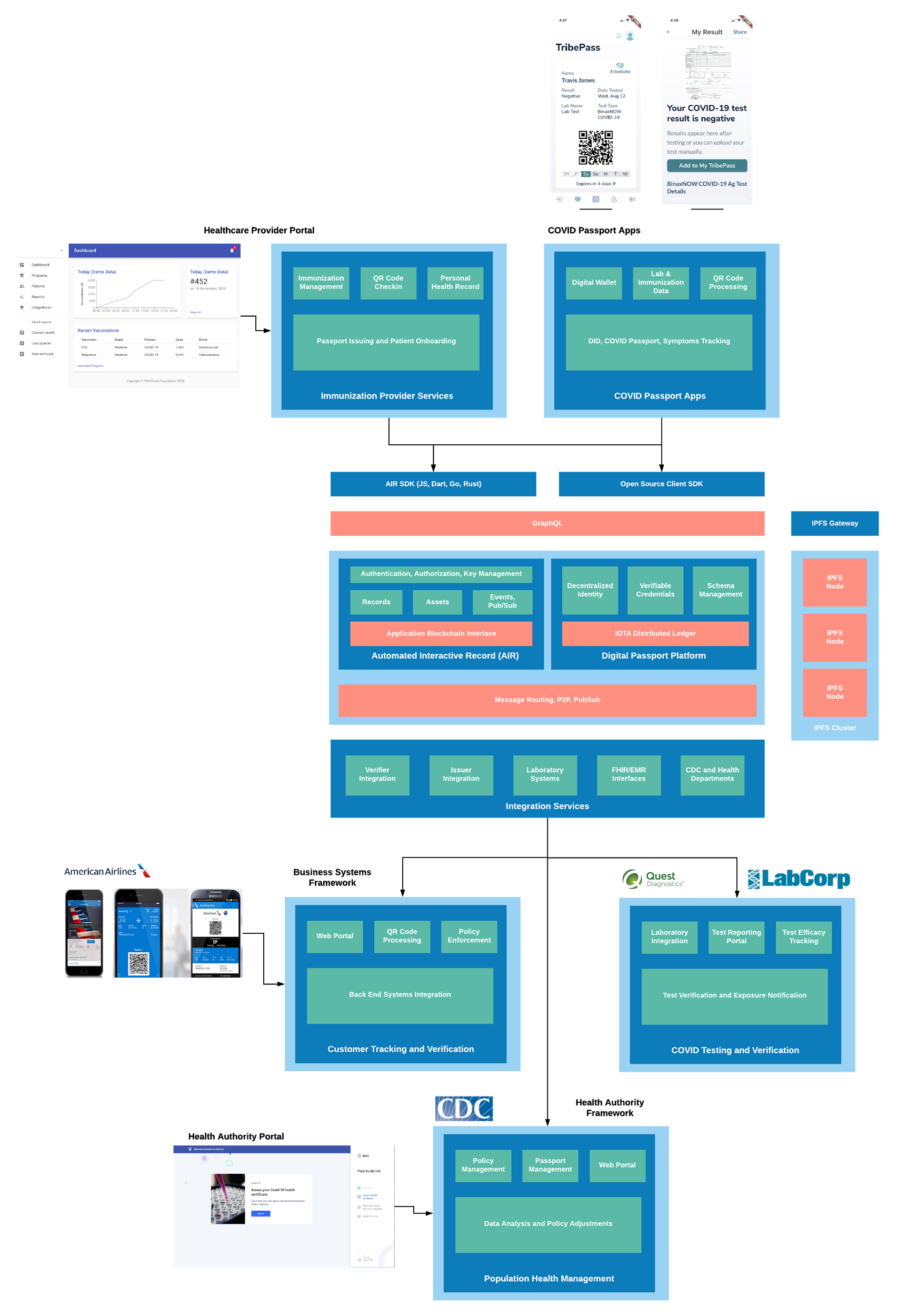
A successful implementation of the technical solution requires the design and deployment of the following:

* A decentralized identity implementation like [Iota](https://blog.iota.org/the-first-step-towards-a-unified-identity-protocol-7dc3988c8b0e/) that also supports verifiable credentials, which provides a scalable implementation that mitigates the [performance and cost concerns related to traditional blockchain technology](https://academy.ivanontech.com/blog/blockchain-vs-tangle-untangling-the-iota-tangle).
* A [verifiable credential schema](https://www.w3.org/TR/vc-data-model/) that includes all the data elements necessary to create and validate a COVID-19 test result or vaccination. Ideally, we would leverage existing standards for this, but these standards are still in development. As a result, any implementation should be adaptable in a way that any dominant standard can be integrated seamlessly when one appears to gain traction.
* An open source SDK and framework for building apps and services that support the workflow of establishing a decentralized identity and maintaining credentials. Client SDK’s should support iOS, Android, web, and desktop “wallets” that contain private keys and credential data on computing devices encrypted in a safe way.
* Open source portal frameworks and SDK’s to support the workflow for administrators to the system, identity providers, credential issuers and verifiers, and policy configurations for jurisdictions that process credentials.

## Architectural Design and Principles

### Overview

The following diagram illustrates the system architecture that supports the use cases and workflows associated with providing a complete decentralized identity and digital COVID-19 passport implementation:



## Solution Components

### Decentralized Identity

#### Identity Providers

The intent behind decentralized identity is that a user’s identity is self-sovereign and not dependent on any external service. However, identity providers assist in the support of allowing self-sovereign identities to find each other and communicate securely.

##### Wallets

Wallets provide a way to securely store the private keys and other information about a user’s identity in a private area controlled only by the user (e.g., a mobile device’s secure storage, a USB drive, or even a piece of paper).

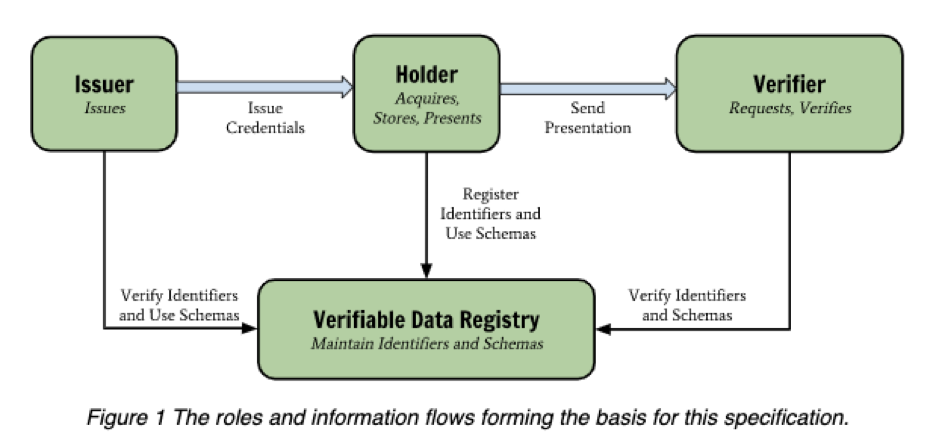
#### Verifiable Credentials

##### Roles

Roles are expressed as verifiable credentials that provide a user access to performing functions in support of the digital passport workflow (e.g., verifying a COVID-19 test result, verifying a user submitted vaccination record, etc.).

##### Schemas

Schemas specify what data must be collected and verified in order to issue and validate credentials. A verifiable data registry advertises the supported schemas for a system to support the following workflow:



##### Issuers

The W3C defines an issuer [here](https://www.w3.org/TR/vc-data-model/#dfn-issuers). For the purposes of a COVID-19 digital passport implementation, an issuer, such as a public health department or clinic, provides a service that can validate the creation of a passport credential.

##### Verification

The W3C defines verification in the following manner:

The evaluation of whether a [verifiable credential](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-credentials) or [verifiable presentation](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-presentations) is an authentic and timely statement of the issuer or presenter, respectively. This includes checking that: the credential (or presentation) conforms to the specification; the proof method is satisfied; and, if present, the status check succeeds.

Supporting this requires that portals and/or apps be built to support the registration and validation of “verifiers”, including configuring parameters for operation based on the needs of local jurisdictions or organizations.

#### Storage

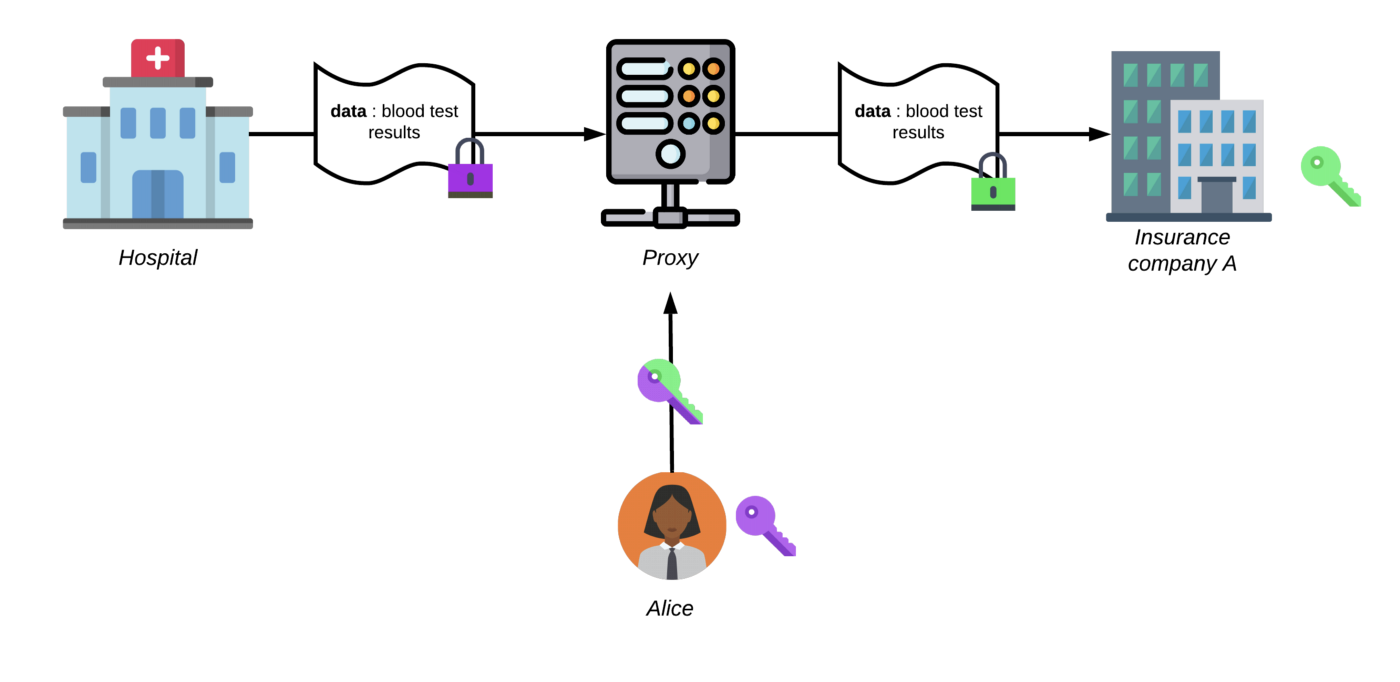
To ensure the validity of credentials and support their creation and verification, the system needs to support the upload and storage of supporting documents and files.

##### IPFS

[IPFS](https://ipfs.io/) provides the means by which necessary data can be stored, replicated, and pinned throughout a worldwide infrastructure of nodes. This ensures the fastest possible processing and resolution of credentials.

##### Security, Sharing, and Encryption

When sharing sensitive data between users and systems in the name of a user, [proxy re-encryption](https://medium.com/@teamtech/decentralized-identity-granting-privacy-with-proxy-re-encryption-e0bf68ad465c) utilizing an individual’s decentralized identity is a way to support one-to-one and one-to-many sharing in a standard way. The following diagram illustrates how this works:



#### COVID-19 Passport Apps

These are mobile apps built using open source frameworks that individuals can use to request and manage COVID-19 passports associated with negative COVID-19 or positive serology test results and/or vaccination records. All instances of these apps interoperate, as they all utilize the same decentralized network of nodes to manage individual data. A user’s single decentralized identity works to authenticate them with ALL instances anywhere, so a user always has access to their passports and data. These apps allow an individual to:

* Display a QR code for their identity and/or digital passports for verification by a relying party (e.g., airline, local business, employer, etc.)
* Upload laboratory test results for verification
* Upload pictures of vaccination records for verification

#### Healthcare Provider Portals

Healthcare Provider Portals allow healthcare providers that offer COVID-19 tests and vaccinations to do the following:

* Onboard their patients to the passport infrastructure automatically via mobile app or QR code
* Collect symptoms tracking information
* Issue digital passport credentials
* Verify digital passport credentials
* Assist in automating check-in processes for COVID-19 patients

#### Business Systems Frameworks and Portals

Businesses that want to ensure that their employees and/or customers are COVID-safe use business portals to do the following:

* Set policies for what represents a valid COVID-19 health state for their business (e.g., number of days since last COVID-19 negative test, vaccination requirements—partial or full vaccination, which type vaccine is acceptable (e.g., only those currently authorized by the FDA) and level of validation etc.)
* Build apps that read QR codes presented by instances of COVID-19 passport apps for validation
* Generate QR codes for business locations to allow for customer or employee check-in. This can direct customers or employees to download the necessary apps automatically and onboard them.

Individual Privacy

Maintaining individual privacy is inherent in the design of the Decentralized Identity standard, but Verifiable Credentials can leave open the possibility of unintended leakage of information that an individual would rather remain private. To assure complete privacy and security in the processing and validation of credentials a [Zero Knowledge Proof scheme](https://techcommunity.microsoft.com/t5/identity-standards-blog/advancing-privacy-with-zero-knowledge-proof-credentials/ba-p/1441554) should be designed and implemented. Fortunately, [several interoperable standards for ZKP](https://medium.com/decentralized-identity/building-interoperable-zkp-credential-systems-70bc20a8a809) have been in development, including an open standard from [Microsoft](https://github.com/decentralized-identity/snark-credentials/blob/master/whitepaper.pdf) that can be implemented in an open source microservice that includes a way to revoke credentials.

Individual Ownership

To ensure security, the entire system must operate on the principle of individual ownership of data. This means ensuring that ANY transfer of data from the user to any other entity (issuer, verifier, relying party, etc.) MUST be explicitly approved by the user and implemented using secure cryptographic key exchange mechanisms to protect user data during transmission.

HIPAA

Adhering to HIPAA standards adds additional considerations that are accounted for in the proposed architecture:

* **Encryption of user-submitted materials.** When a user manually submits files used for the verification of credentials from an issuer or verifier, those files must be encrypted before being stored on IPFS to assure that given a hash, an intruder could not view the contents of a stored file without being granted a decryption key with the approval of the data owner. These keys are derived from the user’s decentralized identity and can be revoked.
* **Encryption at rest for data stored in relying party services.** A relying party, issuer, or verifier provides the means by which verifiable credentials can be created, validated, or presented. Any service storing data must provide the means by which data about users is encrypted at rest in any physical database to prevent bad actors with direct access to databases from compromising user data.

GDPR

The system design must allow for users to request to be forgotten in accordance with GDPR and other privacy laws across the world. Implementing this is complex given the fact that immutable decentralized distributed ledger technology is immutable—changes made to the chain are permanent and cannot be deleted. For this reason all data subject to GDPR standards cannot be stored directly on such ledgers. Instead, this data must be stored securely off chain with references stored on chain. In the event that a user wishes to be forgotten, data can be deleted from the off chain data storage with an entry added on chain indicating the deletion event.

Public Health

CDC and other organizations would benefit from building a secure data warehouse containing individual information that can be used to do the research and analysis necessary to formulate effective public health policies and guidance. This requires the user to authorize the sharing of their personal and credential data with authorized health departments and the CDC. This can be achieved using the proxy re-encryption methods described above, in which case public health departments implement services supporting encryption at rest for the data warehouses used or research and public health policy development purposes.

#### Business and Economy

One of the most important goals in the use of digital passports is to allow businesses of all types to return to serving customers in person. A successful system must support the following general high level use cases:

* Allow users to check-in to a location to initiate on-boarding and tracking whether a user has downloaded a mobile app or not
* Allow users to use ANY instance of an app connected to the global network of nodes to present a QR code for validation
* Provide support for multiple platforms (mobile, web, desktop, etc.) for businesses to validate QR codes presented
* Ensure secure end-to-end encrypted communication for any data transmitted
* Provide anonymous tracking data to public health authorities where necessary to demonstrate compliance with local public health policies

#### Interoperability

Interoperability is essential to ensure that individuals can leverage whatever supporting apps they have downloaded to work everywhere. This ensures that individuals do not have to download multiple apps to cover all supported use cases, which maximizes adoption.

Integration

The design of the network provides interfaces for integration with external systems in the following manner:

* EMR systems for healthcare providers and other collaborators, so vaccination records and COVID-19 test results can be automatically sent to users with passports created and validated automatically
* Laboratory Information Systems for COVID-19 test providers and processors
* Automatic integration with CDC systems allow for data to be collected and processed in real time

All integrations involving individual data must be explicitly approved by individual users with data always being transmitted using end-to-end encryption and encrypted at rest in approved target systems.

#### Use Cases

The W3C has defined many [use cases](https://www.w3.org/TR/vc-use-cases/) for the use of Verifiable Credentials, including those for healthcare and professional credentials, which are particularly relevant for COVID-19 digital passport use cases. The following diagram illustrates how credentials are created and resolved for all use cases:

### Variations on General Use Cases

For the purposes of digital passports, there are variations on the standard verifiable credential use cases that must be supported:

* **User provided credentials.** A user must be able to upload the digital material representing credentials manually, since digital integration will not be possible in most cases. This requires manual validation by humans examining materials submitted.
* **Credential Expiration.** Credentials related to COVID-19 test results must automatically expire given some configured context and policy (e.g., a COVID-19 test result is only valid for a specified number of days depending on usage).
* **Composite Credentials.** For vaccines that require multiple dose regimens, credentials should only be considered complete when the entire regimen has been completed.. However, policies can be adjusted to be validated in some contexts with partial vaccination

Policies are configured and administered by instances of portals (healthcare, business, etc.) that establish the context for issuance and validation.

#### User Experience

It is extremely important for the adoption and success of the system to ensure a fluid user experience in the following areas for all personas:

* Creation and management of decentralized identifiers
* Wallet management and recovery
* Presentation and validation of credentials
* Registration for users of business portals and policy configuration
* Registration and validation of healthcare provider portal users
* Configuration, deployment and management of public health authority systems and portals

#### Personas

The following personas must be supported across the system in various contexts:

* **Individuals.** Public users can potentially log into and make use of COVID-19 passport apps, healthcare provider portals, business portals, and health authority portals. A single Decentralized Identity (DID) should allow authentication to all of these systems.
* **Healthcare Providers.** Doctors, nurses, and administrative staff at healthcare provider organizations must be able to verify their roles (via verifiable credentials showing them to be a physician, registered nurse, etc.) to execute the workflow they are authorized for based on those verified roles.
* **Public Health Officials.** These are employees or administrators at the CDC or health departments. Depending on role, they should have the appropriate access to integrated data for analysis and policy management.

## Implementation and Deployment

### Open Source

All system software components pictured in the architecture diagram should be made available as open source to allow any jurisdiction to deploy instances of the components for themselves if desired. Organizations also have the option to allow implementers, like Tribe Health Solutions, to stand up and manage instances of the infrastructure on their behalf. All instances anywhere adhere to the standards outlined in this document to ensure interoperability. Open source components ensure the following:

* Code can be audited and analyzed by security experts to assure continued safety
* The open source community of developers can contribute to the code to evolve and extend it for the benefit of all
* Strict adherence to standards as they evolve can be assured
* Trust and transparency are maintained for the entire system

### Collaboration

The Verifiable Credential Data Model standards does not define the data structures necessary to implement the desired digital passport functionality. The data model is a metamodel language for the definition of what credentials mean and how they are validated. As a result, there are many variations and competing standards in development all intended to solve the same problem. It is essential that the design of the system be able to leverage ANY of these standards in isolation or together to ensure maximum adoption and interoperability. The following organizations are known to be working on versions of these standards, and efforts have already been made to collaborate with them:

* [**The Commons Project**](https://thecommonsproject.org/)**.** This foundation has defined an intent to build [CommonPass](https://thecommonsproject.org/commonpass) (immunity passports) and [CommonHealth](https://thecommonsproject.org/commonhealth) (personal health record).
* [**Microsoft/Salesforce/Oracle Vaccine Passports**](https://www.cnn.com/2021/01/16/tech/coronavirus-vaccine-records-microsoft-salesforce/index.html)**.** Microsoft, Salesforce, and Oracle have announced plans to collaborate on building immunization passports, but specific standards and schemas have not been announced. Microsoft already provides the [Ion framework](https://techcommunity.microsoft.com/t5/identity-standards-blog/ion-booting-up-the-network/ba-p/1441552) supporting decentralized identity and verifiable credentials on top of the Bitcoin blockchain, but it is unlikely that this framework would be used as a basis of a worldwide release.
* [**European Consortium**](https://www.ledgerinsights.com/european-consortium-develops-blockchain-covid-19-immunity-passport/)**.** A consortium of technology companies has started to define how to use the [Baseline protocol](https://www.ledgerinsights.com/blockchain-baseline-protocol-explores-covid-19-contact-tracing-medical-testing/) on top of Ethereum blockchain to support medical records management and immunity passports.

While none of these projects have actually released apps yet, it is important to note that the design of the system proposed here is agnostic to specific decentralized identity or verifiable credentials implementation. This document fully specifies a scalable, full featured option using Iota, but the architecture is not bound to it. If another offering gets traction, that part of the system can be replaced by a more dominant implementation without side effects.

### SDK’s and Frameworks

SDK’s and frameworks allow for extensibility and customization of the proposed decentralized network for specific jurisdictions and businesses. There will be well defined component interfaces for user interface and back end service integration that allow for customization at multiple levels.

#### Web

Web components will leverage the following tools and technologies in SDK’s:

* [**GraphQL**](https://graphql.org/)**—**Provides a consistent query, subscription and mutation interface to back end services that allows for quick building of responsive real time visual components.
* **React—**[React.js](https://reactjs.org/) has a huge community, tight integration with GraphQL in base components, and allows for the publishing of shared components that support theming and customization for branding instances for use in various portals.

#### Mobile

To support maximum flexibility and maintainability in supporting the fast development of mobile applications, the following components will be built and open sourced:

* **Flutter SDK and Components—**[Flutter](https://flutter.dev/?gclsrc=ds&gclsrc=ds) allows for the simultaneous development of high performance mobile applications for web, iOS, Android, MacOS, Windows, and Linux. Flutter components that are published will integrate native components published to native plugin repositories (e.g., Carthage, Maven, CocoaPods, etc.).
* **React Native SDK and Components—**[React Native](https://reactnative.dev/) also allows for the simultaneous development of mobile and desktop apps on multiple platforms using JavaScript. Native plugins will use the same native components that are referenced by Flutter components to ensure compatibility.
* **MacOS and iOS Native Components—**Native components necessary for iOS and MacOS will be published to [Carthage](https://github.com/Carthage/Carthage) and [CocoaPods](https://cocoapods.org/) for integration directly into native mobile apps.
* **Android Plugin Components—**Android native components will be published to [Maven](https://developer.android.com/studio/build/maven-publish-plugin) repositories for integration with native Android apps.

#### Desktop

[Flutter desktop](https://flutter.dev/desktop) and React-Native via [Electron](https://www.electronjs.org/) will be supporting or building native desktop applications. The same tools and chains for building mobile applications will be used to support building desktop apps for MacOS, Windows, and Linux.

### Governance

Governance and policies are enabled by the proposed decentralized platform but must be configured. To finalize how governance will be implemented the following must be considered:

* What role does the CDC play in determining global governance that must be adhered to by all instances (e.g., those implemented directly for public health departments)?
* What credentials are necessary to support human validation of vaccination records and negative COVID-19 test results?
* What type of data would the CDC wish to collect on users with their permission and what are the policies around the use of that data?

### Next Steps

To provide a functional, scalable digital passport system as soon as possible, the following next steps must be executed:

* Governance decisions must be made
* Schemas for verifiable credentials must be finalized
* Policy management features must be finalized or each organization persona
* A method of verifying healthcare provider credentials for each supported system role must be finalized (e.g., should KYC be required or is manual submission of supporting materials enough)?
* Discussions with airlines should commence to determine and finalize portal and system requirements for them. Tribe Health has started this process.
* For a pilot release, a specific jurisdiction should be chosen where all collaborating personas exist for end-to-end system testing
* Initial deployment and dev ops details must be finalized and tested