Designing Verifiable Health Solutions

For Global Pandemic
Roadmap
Of Things To Come

1. About
   Myself + The Problem + The Scope

2. The Project
   Considerations + Concerns

3. Technical Solution
   Product + Policy + Cryptography

4. Future
   The Takeaway
Global Pandemic COVID-19 Timeline

- WHO announces mysterious disease
- US declares public health emergency
- Global air travel restricted
- California issues stay-at-home order
- The Project

- WHO declares COVID-19 pandemic
- US COVID-19 Cases Reach 2,000,000
- The Project

- WHO announces COVID-19 is airborne
- US COVID-19 deaths surpass 100,000
- Newer, more contagious strain of COVID-19 discovered

- People dying every 30 seconds in US from COVID-19
- US president tests positive, hospitalized
- Vaccine distribution begins

- US surpasses 100,000 cases in single day
- You are here

- US health officials state CDC will issue COVID-19 vaccination cards
The Project

Goals and Objectives

Health Policy

Compliance Check

Prevent

Contain

(image animations go here)
The User Experience
Making Compliance Easy

(image animations go here)
Safety
Safety Is Difficult
Due To Environmental Factors

The Virus Doesn’t Care
Super easy to contract, carry, and transmit. Estimated 50% of transmission is asymptomatic.

Incompatible Local Politics
United States is geographically large but easy to travel in. It consists of many states, counties, and cities... each with their own health policies.

Poor Health & Financial Support
With no public healthcare, a shortage of COVID tests, the US only offered its affected citizens a single lump sum of $1,200.
Safety Is Difficult
Due To Social Factors

The Asymptomatic
Might carry and transmit the disease, even while passing recommended self-assessments.

The Negligent
Won't follow rules because it inconveniences their lifestyle or personal liberties.

The Critically Misguided
Will actively attempt to circumvent health policies due to popularized disinformation.
Safety Assurances

What Information Has High Trust?

**Infection Status**
Proof that you were recently tested and your viral load is non-existent / undetectable.

**Immunity Status**
Proof that you received a vaccine or an antibody test that shows prior infection / immunity within a certain timeframe.

**Authenticity Status**
Proof that you are who you say you are, and that all presented credentials belong to you.
Centralized Design
Single point of trust is conceptually easy to model, difficult to protect against exposure.

Peer-To-Peer
Trust becomes more difficult to model. Users share data directly with each other.

Self-Sovereign Identity (SSI)
Similar to P2P regarding trust, but with greater privacy risks, since users publish data to public ledgers and share distributed identifiers.
Centralized Design
Are The Stakes High Enough To Warrant It?

(image animations go here)
Decentralized Design

What Are We Worried About?

Benefits
Interactions can occur between independent agents without a facilitating intermediary.

Trust Concerns
Lacking the integrity guarantees an intermediary typically provides, data must be signed by pre-established authorities.

Tracking Concerns
Maintaining long-term pseudonymity is difficult.
Hybrid Architecture
Where Is The Right Balance?

Decentralize Sensitive Info
Reduce exposure risk for identity, health, and location information.

Local Data Transfer
There is no need to store sensitive data in a public blockchain, which increases exposure risk substantially for little apparent benefit.

Collusion Is Impractical
Multiple parties colluding to share information should be either prohibitively costly or redundant.
Equity
Find The Right Balance
Or You're Better Off Doing Nothing

Rate ratios compared to White persons

- American Indian or Alaska Native persons: 0.6x
- Asian persons: 1.4x
- Black or African American persons: 1.7x
- Hispanic or Latino persons: 1.8x

Hospitalization

- American Indian or Alaska Native persons: 1.2x
- Asian persons: 3.7x
- Black or African American persons: 4.1x
- Hispanic or Latino persons: 4.0x

Death

- American Indian or Alaska Native persons: 1.1x
- Asian persons: 2.8x
- Black or African American persons: 2.8x
- Hispanic or Latino persons: 2.6x

(image animations go here)
Technical Solutions
Akers In This System
Summarizing The Moving Parts

Ephemeral Pass Authority

Identity Verifiers

Policy Admins

Individuals

Health Workers

Policy Checkers
What Do Policies Look Like?
Contrasting Different Capabilities

**Example A**
- Has verified state OR federal ID.
- Has continuity of self-reporting for 60 days
- No travel outside the US within 30 days
- No positive diagnostic test result in last 30 days

**Example B**
- Must have verified state OR federal ID.
- Must have negative FDA-approved test result taken within last 48 hours
- Must have FDA-approved vaccine administered within last 6 months
- OR
- No positive diagnostic test result in last 30 days
Key Properties

Features of the Protocol

No Online Identity
Decentralized offline storage (share QR codes).

Signature-Based Verification
Public-key cryptography and central authority.

Ephemeral Keys
Reduces identity tracking risks.
Core Protocol
Used For All Communications

Prover
- Generates ephemeral key pair.
- Signs request with trusted timestamp.

Verifier
- Validates integrity of assertion request.
- Signs response (containing request).

Summary
The Prover can take this response and use it to prove ownership in other contexts. Very useful if the verifier is a trusted authority providing proof of health status.
The prototype used ECDSA on the secp256r1 curve (NIST P-256), with sha256 as the hash function. Keys generated and stored in Android Keystore and iOS Keychain.
What You Give
To Acquire Some Form Of Proof

- Owner Photo (Visual Only)
- Physical Documents (Visual Only)
- Verification Data (Off Record)
- Interaction Key (For Record)
What You Get Back
Essentially A Digital Voucher Of Something

Physical Documents

(Scanned)

Interaction Key
Verifier Key
Outcome Metadata
Identity Verification

Credential Creation

What You Show

Physical ID / documents.
Name, photo, date of birth your app has locally-stored (encoded in QR code).

What You Get

A proof that represents a voucher that you are the device / app owner, and implicitly the owner of credentials you present, as shown by the photo your app displays.

It's entirely up to identity verification officials to determine what information is required to validate undocumented individuals. Not disenfranchising these individuals is critical to ethical deployment.
Health Verification

Credential Creation

What You Show
Nothing. The health care provider, lab, or clinic already has your electronic health record.

What You Get
A pseudonymous proof that contains the basic outcome of the test / vaccination record.

Determining how we construct policies around these credentials needs to be heavily calibrated through risk informed by patient statistics and emerging health research.
Now You Have Proof
But It's Not For The Policy Checkers

(Network Request)

Ephemeral Pass Authority
Ephemeral Pass Proof
With Many Tiny Policy Objects

(Network Response)

Ephemeral Pass Authority
Creating Ephemeral Pass

Credential Indirection

Device Automatically Sends

The wide area(s) you expect to adhere to policies in, all your pseudonymous proofs, new signatures to prove ownership thereof.

And Receives

An Ephemeral Pass. Additionally it contains signed policy hashes for all policy variants in your area.

The Ephemeral Pass Authority service does not store proofs or request metadata (IP Address, etc) it receives. It checks the key revocation database to determine if one (or more) proofs are invalid.
Now You Can Enter
Without Sharing Personal / Health Information

Owner Photo (Visual Only)
(Scanned)

Policy Checker

Ephemeral Pass
Policy Hash
Interaction Key
Handling Abuse
When Using Ephemeral Passes

Since Policy Checker's aren't inherently trustworthy, there must be some rules in place to prevent false positives from being recorded in the revocation database.
Extending The Framework
Enforcing Isolation
And Elevating Trust Elsewhere

Attestation Management
A special proof acquired during onboarding, to be revoked when self-attesting COVID symptoms or being tested positive.

Isolation Management
Acquired by providing a revoked attestation proof, has a time or testing requirement before it can be exchanged for a new attestation proof.

Exposure Notification
Receiving a notification triggers revoked one's attestation proof, requiring isolation
Example Isolation Timeline

Making It Clear When You Need To Stay Home

10 days isolation

3 days

Onboarding :)  Symptoms :)  Exposure Notification :)  Negative Test :)

COVID-19 Screening Tool

You'll answer a few questions about your recent travel, contact, and daily activity.

Your answers will not be shared with Apple or others without your permission.

By using this tool, you agree to its terms of service.
Future
COVID-19 Vaccination Record Card

Please keep this record card, which includes medical information about the vaccines you have received.
Por favor, guarde esta tarjeta de registro, que incluye información médica sobre las vacunas que ha recibido.

<table>
<thead>
<tr>
<th>Last Name</th>
<th>First Name</th>
<th>Patient Number (Medical Record or SSN)</th>
<th>Date</th>
<th>Healthcare Professional or Clinic Site</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Vaccine</th>
<th>Product Name/Manufacturer</th>
<th>Lot Number</th>
<th>Date</th>
<th>Date</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>1st Dose</td>
<td>COVID-19</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
STAY HOME
STAY SAFE
Thanks

Mark Funk

Inquiries: enigma2021@obscure.group

Images: Unsplash
Icons: The Noun Project, Slidesgo