
ENIGMA
A USENIX CONFERENCE
Designing Verifiable Health Solutions
For Global Pandemic

Roadmap

Of Things To Come



ENIGMA

A USENIX CONFERENCE

1. **About**

   Myself + The Problem + The Scope

2. **The Project**

   Considerations + Concerns

3. **Technical Solution**

   Product + Policy + Cryptography

4. **Future**

   The Takeaway



Mark Funk

Security, Privacy, Product, and Systems Engineer

ENIGMA

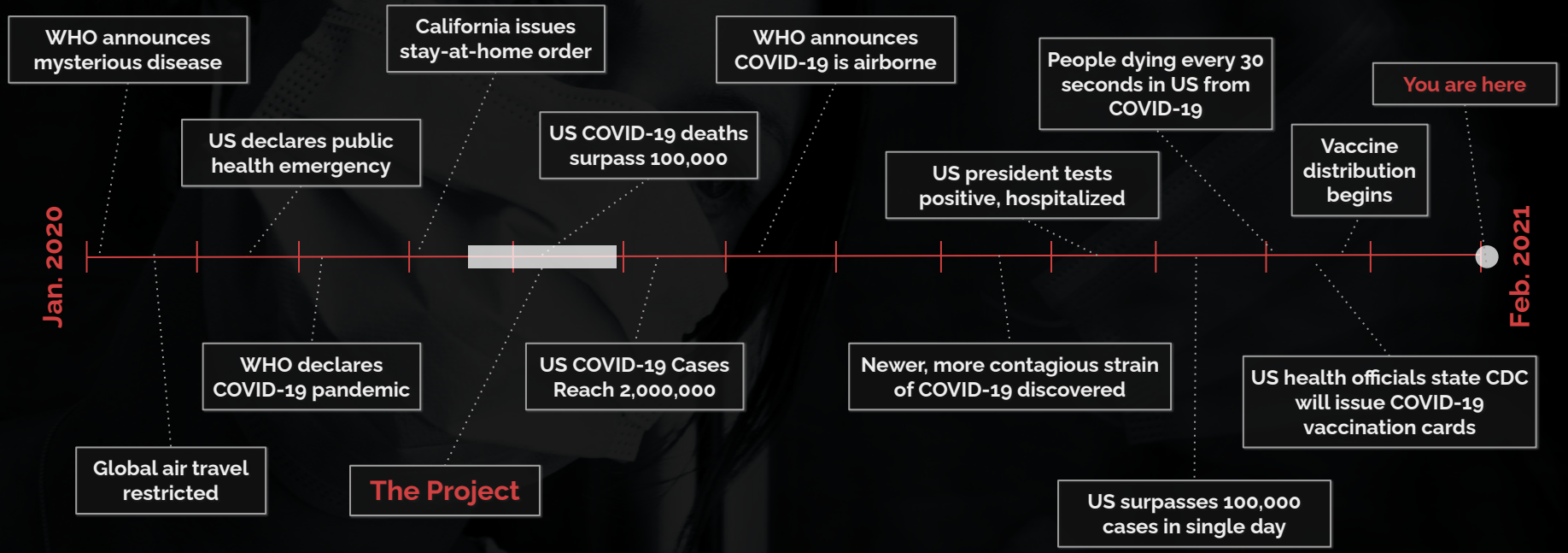
A USENIX CONFERENCE

Global Pandemic (from the US perspective)

COVID-19 Timeline

ENIGMA

A USENIX CONFERENCE



The Project

Goals and Objectives



ENIGMA

A USENIX CONFERENCE

(image animations go here)

The User Experience

Making Compliance Easy



ENIGMA
A USENIX CONFERENCE


ENIGMA
A USENIX CONFERENCE
Safety

Safety Is Difficult

Due To Environmental Factors

ENIGMA

A USENIX CONFERENCE

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.

(image animations go here)

Safety Is Difficult

Due To Social Factors

ENIGMA

A USENIX CONFERENCE

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.

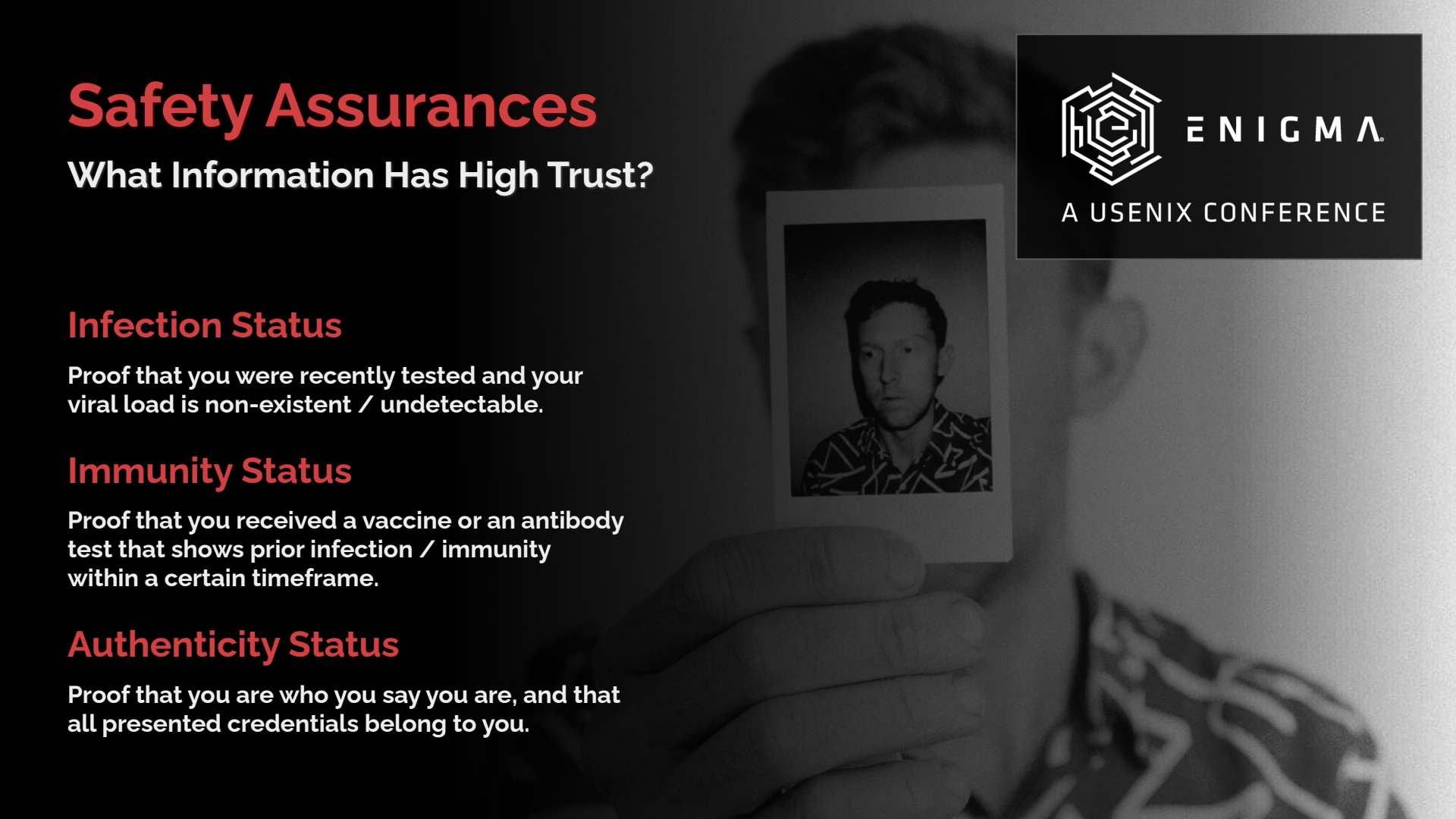
The Critically Misguided

Will actively attempt to circumvent health policies due to popularized disinformation.



Safety Assurances

What Information Has High Trust?



ENIGMA

A USENIX CONFERENCE

Infection Status

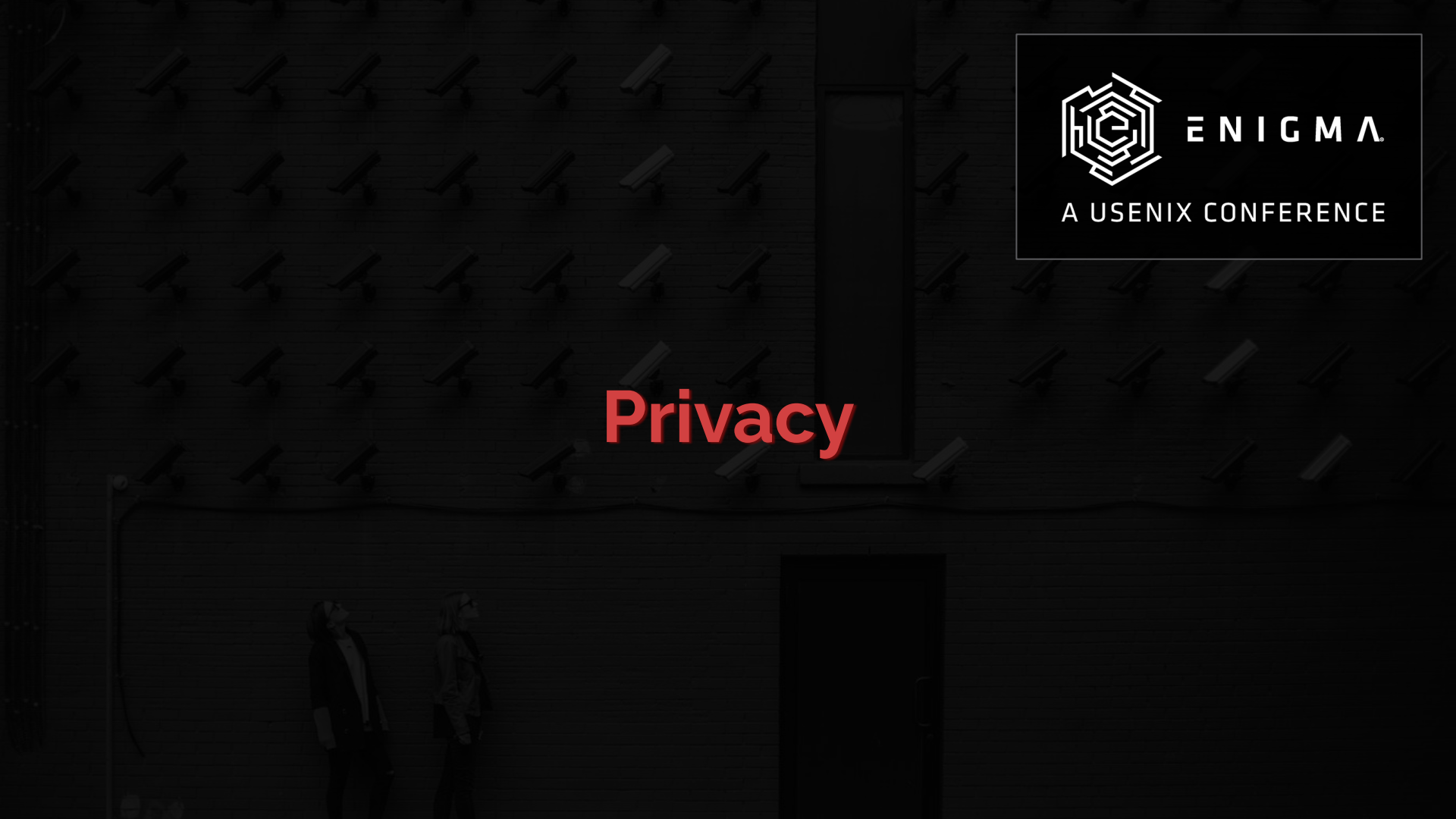
Proof that you were recently tested and your viral load is non-existent / undetectable.

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.


ENIGMA
A USENIX CONFERENCE
Privacy

General Architecture

Options For Sharing Health Information



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?

ENIGMA

A USENIX CONFERENCE

Benefits

Interactions can occur between independent agents without a facilitating intermediary.

Trust Concerns

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

Tracking Concerns

Maintaining long-term pseudonymity is difficult.

(image animations go here)

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.


ENIGMA
A USENIX CONFERENCE
Equity

Find The Right Balance

Or You're Better Off Doing Nothing



ENIGMA

A USENIX CONFERENCE

(image animations go here)



Technical Solutions

Actors In This System

Summarizing The Moving Parts

ENIGMA

A USENIX CONFERENCE

Ephemeral Pass Authority



Identity Verifiers



Health Workers



Policy Admins



Policy Checkers



Individuals



What Do Policies Look Like?

Contrasting Different Capabilities

ENIGMA
A USENIX CONFERENCE

Example A

Has verified state OR federal ID.

Has continuity of self-reporting for 60 days

No self-reported positive symptoms within 20 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.

OR

Must have FDA-approved vaccine administered within last 6 months.

No positive diagnostic test result in last 30 days.

Key Properties

Features of the Protocol

ENIGMA

A USENIX CONFERENCE

No Online Identity

Decentralized offline storage (share QR codes).

Signature-Based Verification

Public-key cryptography and central authority.

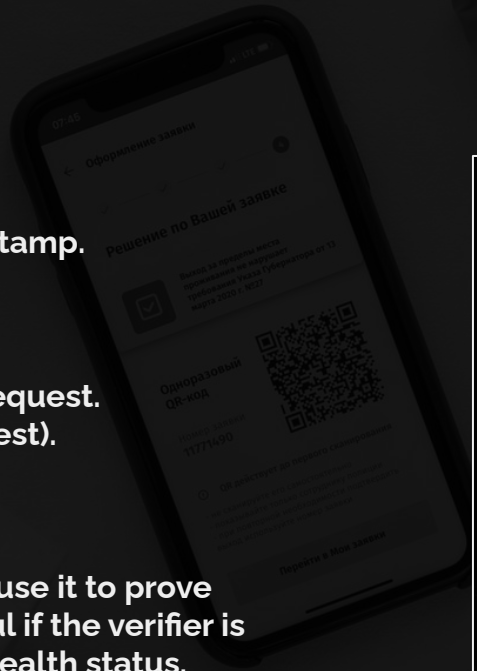
Ephemeral Keys

Reduces identity tracking risks.



Core Protocol

Used For All Communications



ENIGMA

A USENIX CONFERENCE

Prover

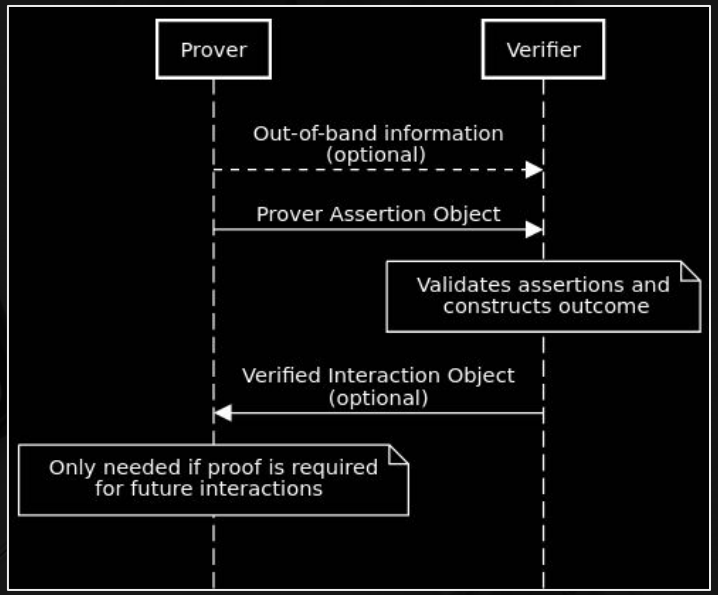
- Generates ephemeral key pair.
- Signs request with trusted timestamp.

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.



Core Protocol Data

From The Prover's Perspective

ENIGMA
A USENIX CONFERENCE

Request

Assertion Object
- (reserved for interaction-specific data)

Prover Object
- message
  - interaction public key
  - timestamp
- signature

Response

message
- public key
- Prover Object
  - ...
- Outcome Object
  - (reserved for interaction-specific data)

signature

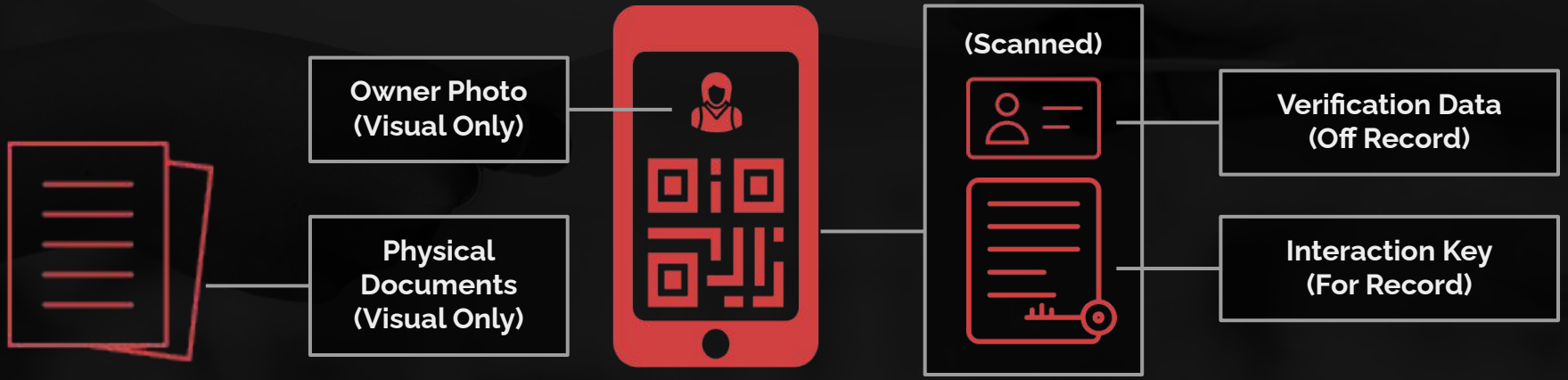
The prototype used ECDSA on the secp256r1 curve (NIST P-256), with sha256 as the hash function.
Keys generated and stored in Android Keystore and iOS Keychain.

What You Give

To Acquire Some Form Of Proof

ENIGMA

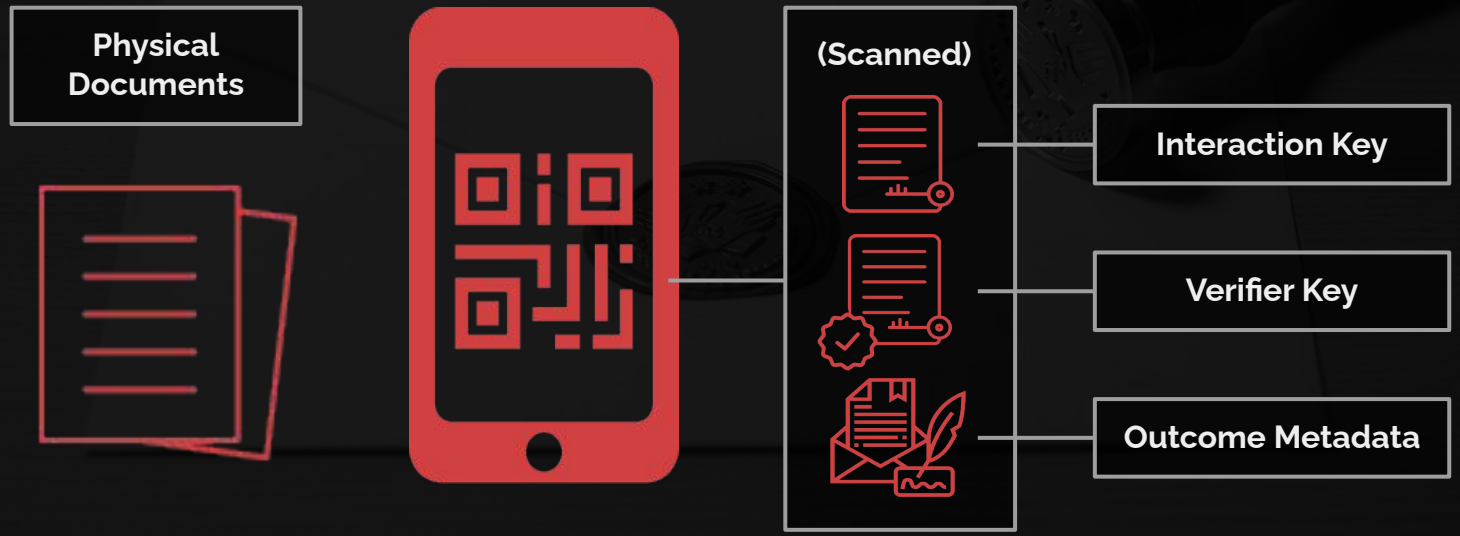
A USENIX CONFERENCE



What You Get Back

Essentially A Digital Voucher Of Something

ENIGMA
A USENIX CONFERENCE



Identity Verification

Credential Creation

ENIGMA
A USENIX CONFERENCE



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

ENIGMA

A USENIX CONFERENCE

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

ENIGMA
A USENIX CONFERENCE

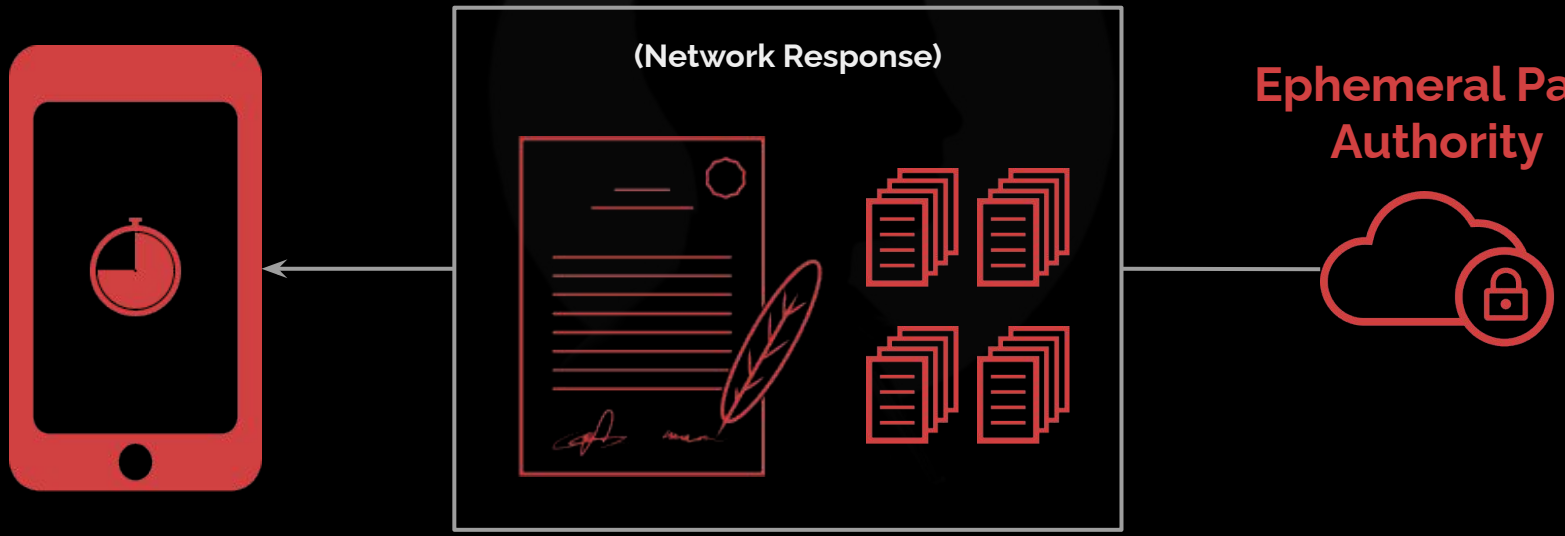


Ephemeral Pass Proof

With Many Tiny Policy Objects

ENIGMA

A USENIX CONFERENCE



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

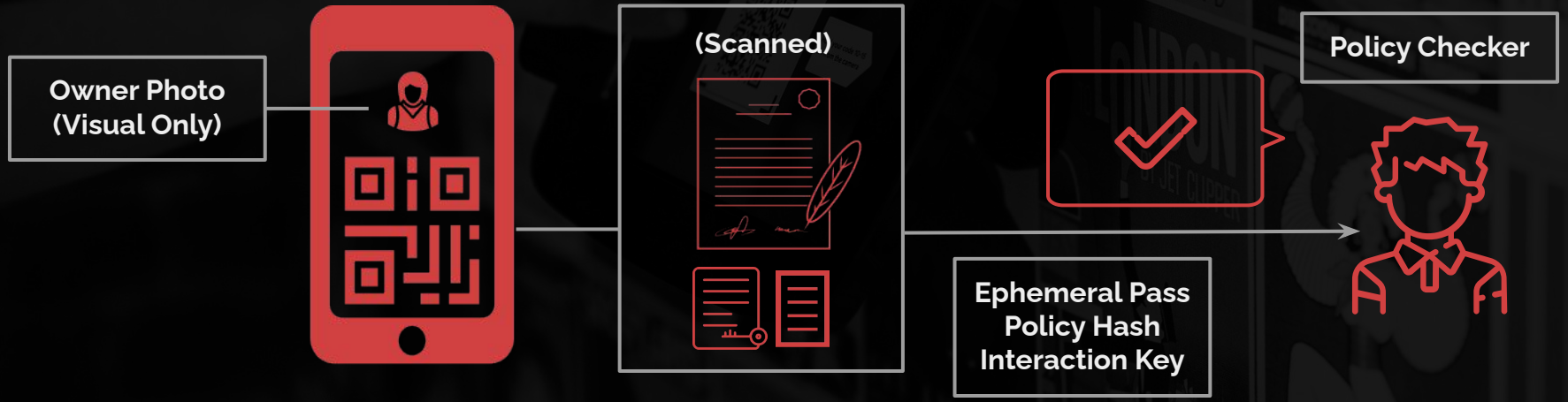
An Ephemeral Pass. Additionally it contains signed policy hashes for all policy variants in your area.

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

ENIGMA
A USENIX CONFERENCE

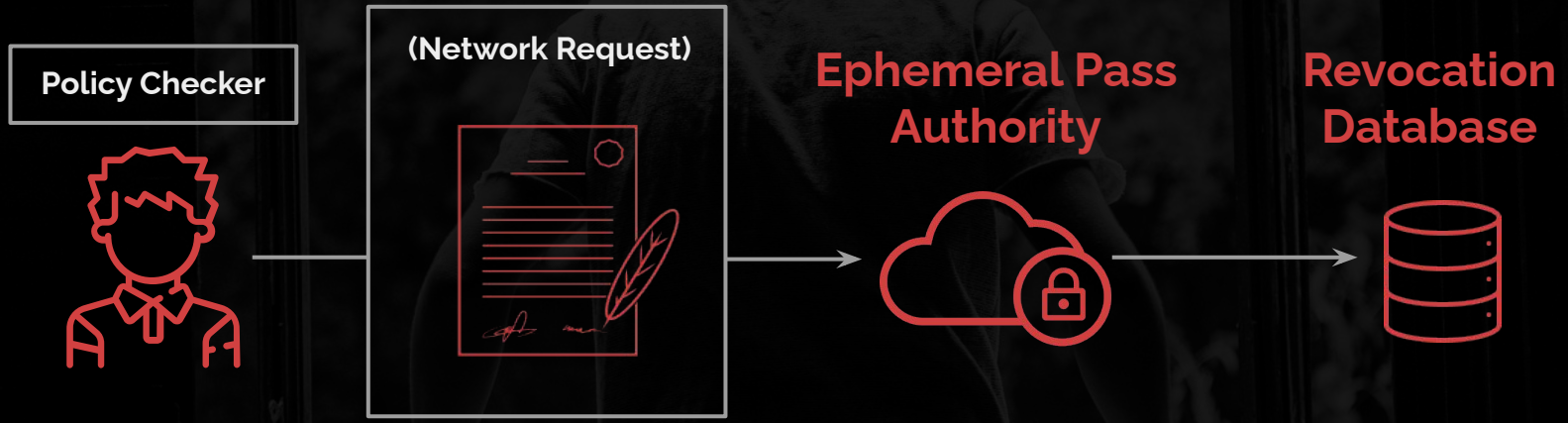


Handling Abuse

When Using Ephemeral Passes

ENIGMA

A USENIX CONFERENCE



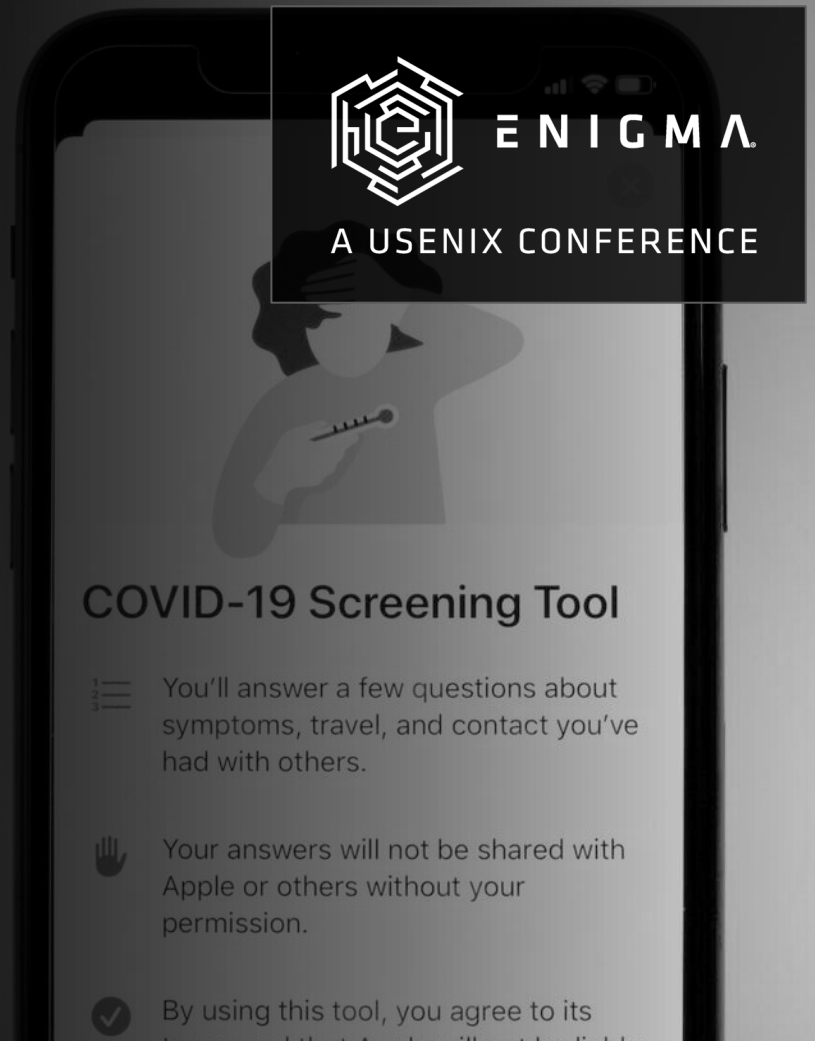
Since Policy Checker's aren't inherently trustworthy, there must be some rules in place to prevent false positives from being recorded in the revocation database.



Extending The Framework

Enforcing Isolation

And Elevating Trust Elsewhere



ENIGMA

A USENIX CONFERENCE

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

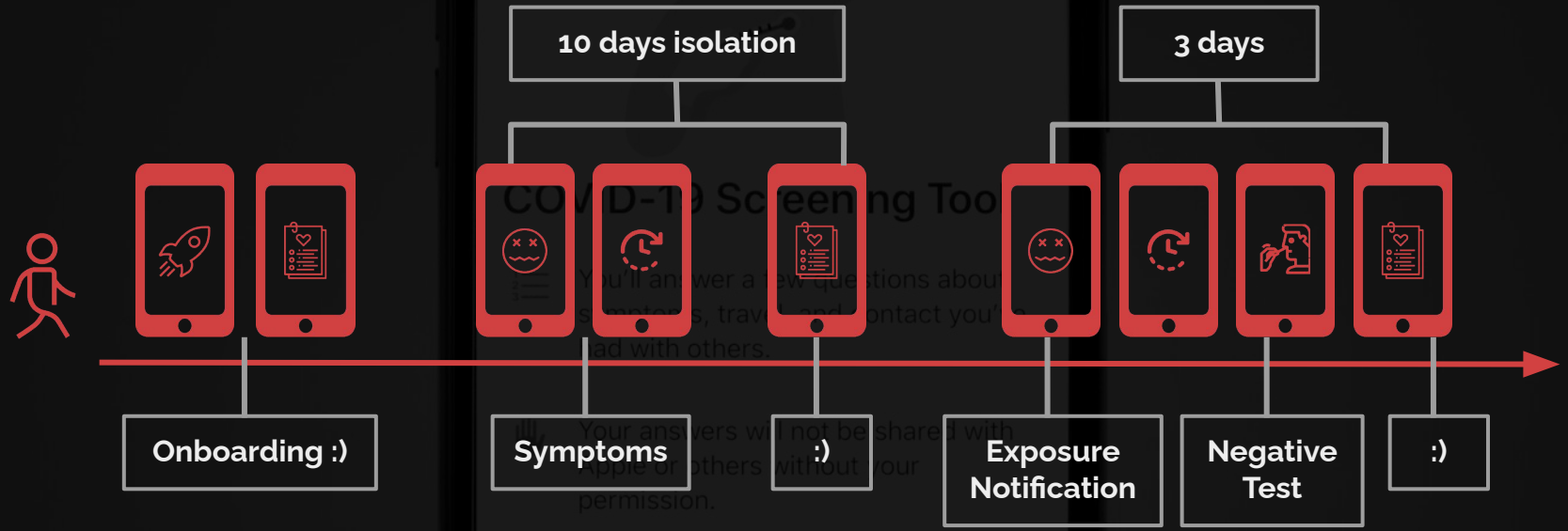
Receiving a notification triggers revoked one's attestation proof, requiring isolation

Example Isolation Timeline

Making It Clear When You Need To Stay Home

ENIGMA

A USENIX CONFERENCE





Future


ENIGMA
A USENIX CONFERENCE


ENIGMA
A USENIX CONFERENCE



ENIGMA

A USENIX CONFERENCE


ENIGMA
A USENIX CONFERENCE


ENIGMA
A USENIX CONFERENCE



ENIGMA

A USENIX CONFERENCE



ENIGMA

A USENIX CONFERENCE



Thanks

Mark Funk

Images: Unsplash
Icons: The Noun Project, Slidesgo

Inquiries:
enigma2021@obscure.group