Consensas Information Passports

CCI Paper-based Verifiable Credentials Presentation

C4

David Janes, Consensas, david@consensas.com, March 2021

Introduction

Information Passports

- Our (Consensas / Me) spin on Verifiable Credentials
- Minimize centralization to minimize "creepiness"
- Minmize interactions
- Use existing web standards
    - JSON-LD, VC, W3C
    - Semantic Web / schema.org
    - X.509

What is a Claim?

Examples

- "David Janes received the second Moderna vaccination on January 20, 2021"
- "David Janes had a viral test for COVID-19 on January 3"
- "David Janes graduated from Memorial University in 1987"
- "David Janes was President of IBM Canada from 1933 to 1972"
- "David Janes won the Silver Medal in the Biathalon in 2004"

What is a Verifiable Claim?

- A claim that we can **independently** verify
- The claim contains **proof** to validate whether it is true
  - Data + Digital Signature
- The **independent** verification phase
  - Do I trust that signature
  - Do I recognize the data
- The claim is addressed by a **URI** (a web address)

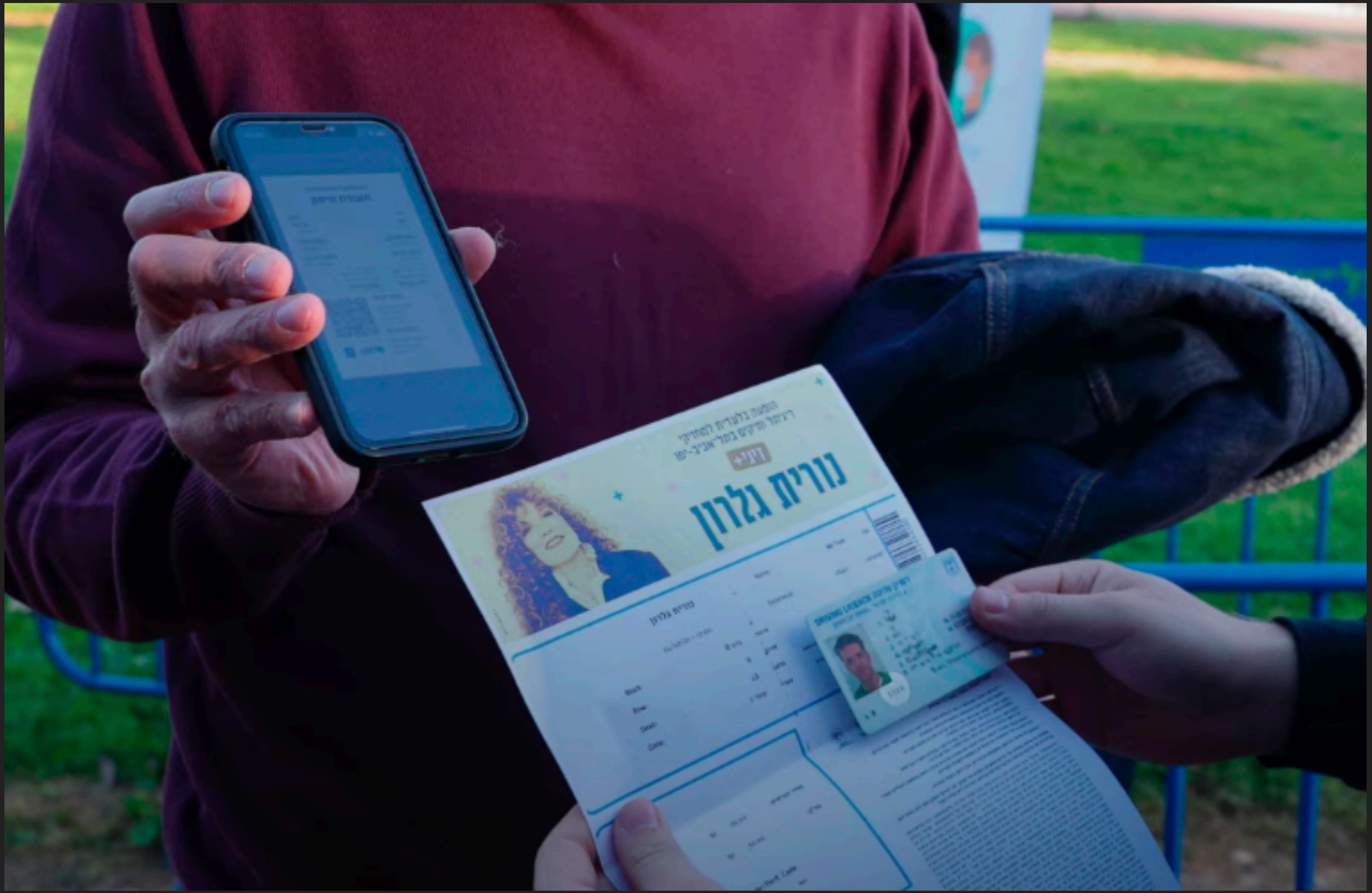
Assumptions

Use / Usability

- Needs to be understandable by "your grandparents"
- Needs to minimize work created for Health Care workers
- Interactions need to be minimized
- It’s OK to verify a credential with another credential (e.g. personal ID)
- Holders can use paper or electronic processes

Use / Usability

Validation with existing ID (Israel)



Problem Set Assumptions

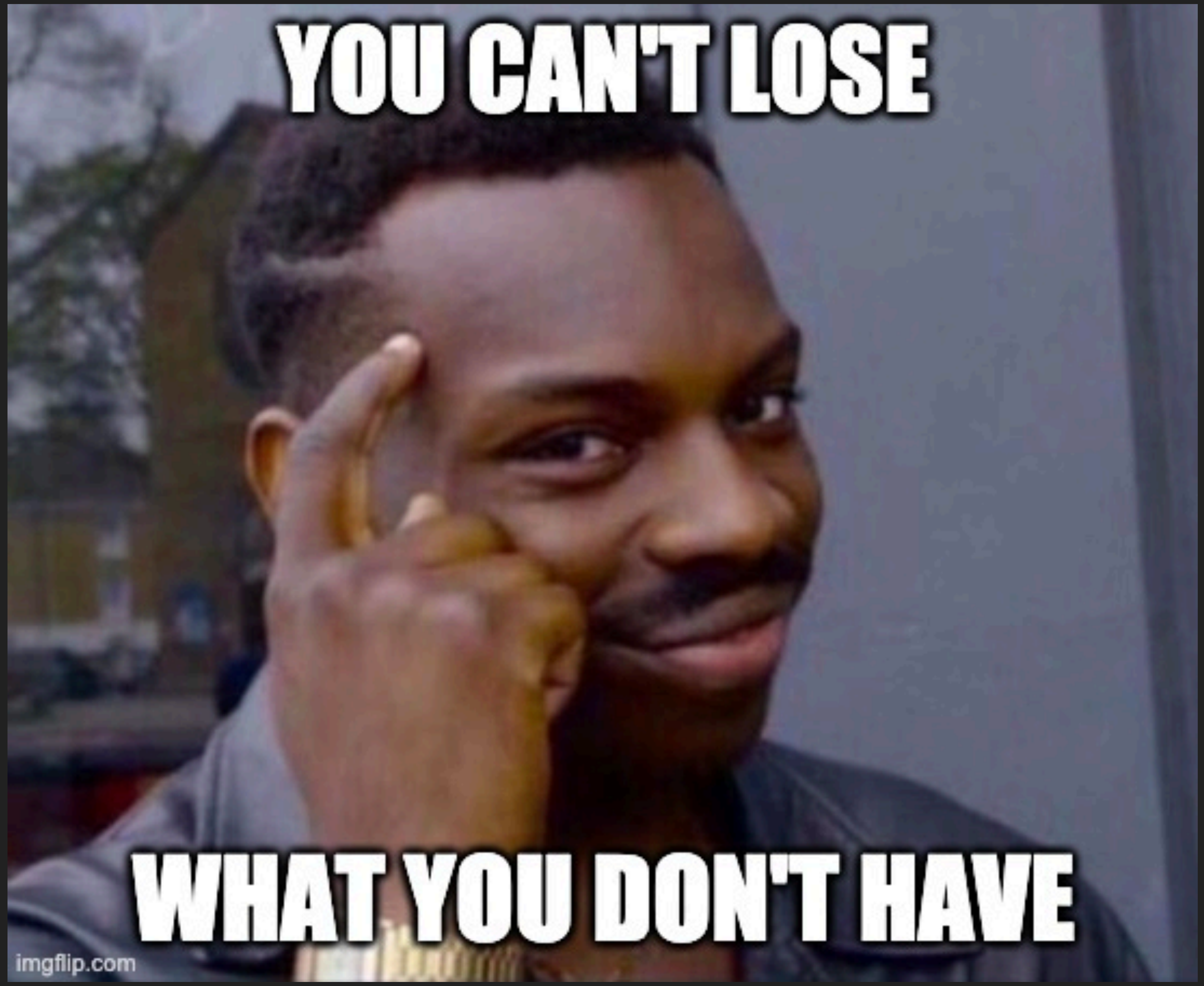
- Needs to be flexible to address a number of closely related problems
  - Immunization, Test Results, "I had COVID"
- There will be many implementations, so needs to be
  - Developer friendly
  - Semantically strong
- There will be no one consistent "coding" of medical data
- There "business rules" for Validation will constantly change

Privacy Credential Assumptions

- URL guessing attacks should not work
- Holders should expect roughly the same level of security as a Credit Card
- Exposure of database should not be disastrous
    - e.g. minimize and redact data fields
    - Worst case scenarios is not awful
- Verifiers are not "verified"
    - Your local gym does not need to be "on the list" to verify

Privacy Credential Assumptions

Worst case scenario is not awful



Paper Credential Assumptions

- Holders should not require electronic devices (!!!)
- Verifiers will have access to the Internet
  - Edge cases (eg. remote mining) can be addressed
- Paper credentials need to fit easily on a credit card!
- If QR codes are used, they should resolve to a meaningful web page
  - Otherwise, why not just use PDF 417?

Validation vs Verification

- Verification
  - The Payload matches the Signature
  - This comes with W3C Verifiable Credentials
- Validation
  - The Signature is by someone we trust
  - The Payload matches flexible "business rules"
  - This needs to be easy to implement

Implementation Assumptions

- W3C Verifiable Credentials
- (Semantically strong) JSON-LD
  - E.g. not a POJ claim inside a JSON-LD wrapper
- Claim should be easy to validate
  - Document-model, not network model (e.g. FHIR)
- Schema provides 90% of fields and types needed, and is extensible

How it is used

Issuing a Claim

Example

- Patient visits Clinic and gets a Vaccination
- The clinic issues a Vaccination Passport
  - This is simply a URL, with a large random component
  - Can be sent via email, SMS, QR code, loyalty account or even physically
- The Patient receives the Vaccination Passport and stores it
  - Bookmark, Apple Wallet, piece of paper in real wallet…

Issuing a claim

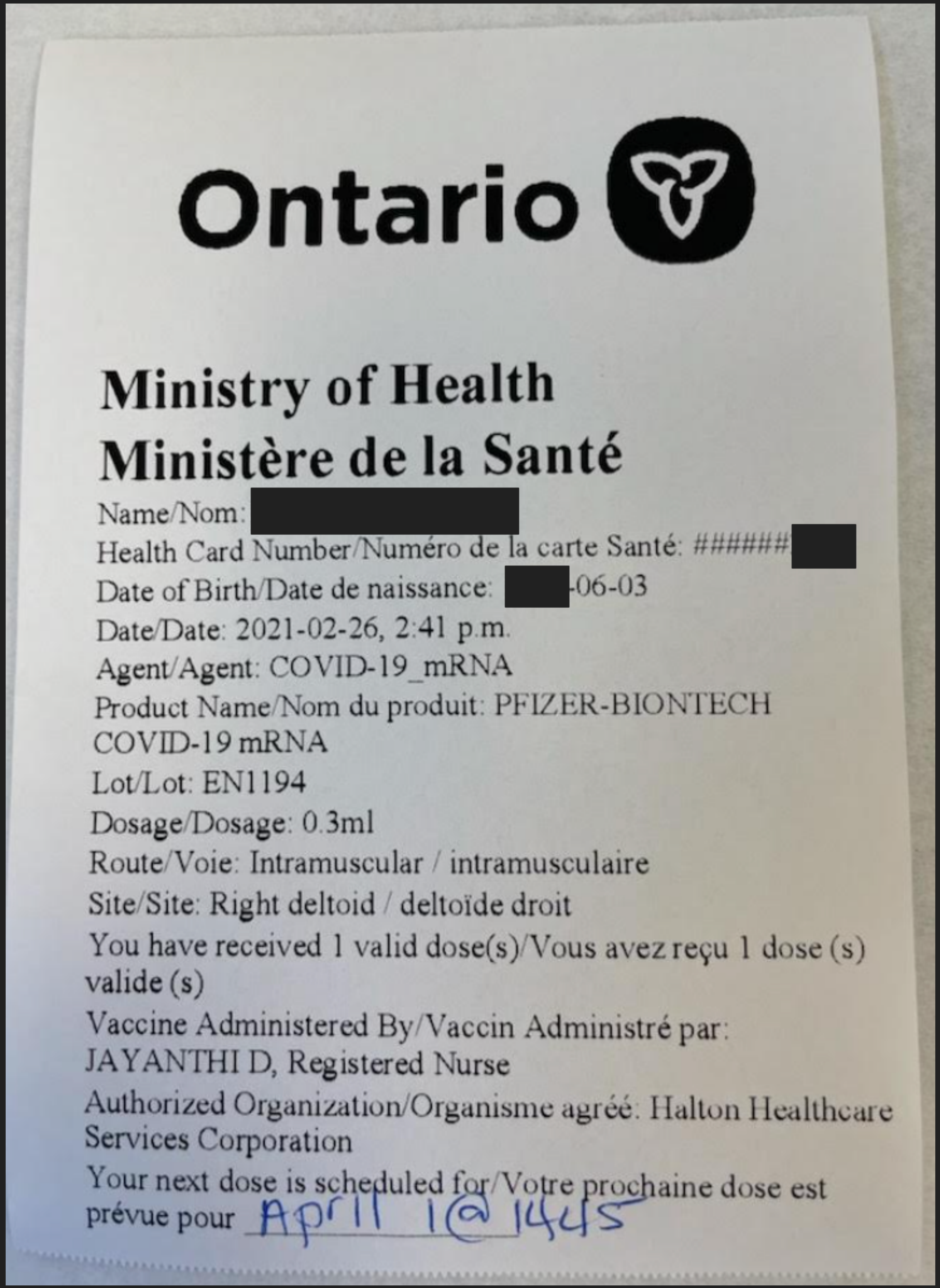
Notes

- No additional work created for the doctor / clinician
- No additional work created for the Patient
    - It’s literally like a receipt, just like shopping
- Some additional work created for the Clinic
    - IT / backend related
    - Claims documents are held by Clinic - holders have URLs

Issuing a claim

Just add a QR code

- Obviously from a computer
- They are comfortable with sharing
  - Full Name
  - Last 4 digits of Health Code
  - Full Date of Birth



Ontario

Ministry of Health
Ministère de la Santé

Name/Nom: [redacted]
Health Card Number/Numéro de la carte Santé: ######[redacted]
Date of Birth/Date de naissance: [redacted]-06-03
Date/Date: 2021-02-26, 2:41 p.m.
Agent/Agent: COVID-19_mRNA
Product Name/Nom du produit: PFIZER-BIONTECH COVID-19 mRNA
Lot/Lot: EN1194
Dosage/Dosage: 0.3ml
Route/Voie: Intramuscular / intramusculaire
Site/Site: Right deltoid / deltoïde droit
You have received 1 valid dose(s)/Vous avez reçu 1 dose (s) valide (s)
Vaccine Administered By/Vaccin Administré par: JAYANTHI D, Registered Nurse
Authorized Organization/Organisme agréé: Halton Healthcare Services Corporation
Your next dose is scheduled for/Votre prochaine dose est prévue pour April 1@1445

Verifying and Validating a Claim

Example

- A **Traveller** (previously the Patient) enters an airport in another province
- An **Officer** asks for proof of Vaccination or negative COVID test
- The Traveller presents their Vaccination Passport
- The Officer scans the Passport and gives the Traveller the go-ahead

How it works

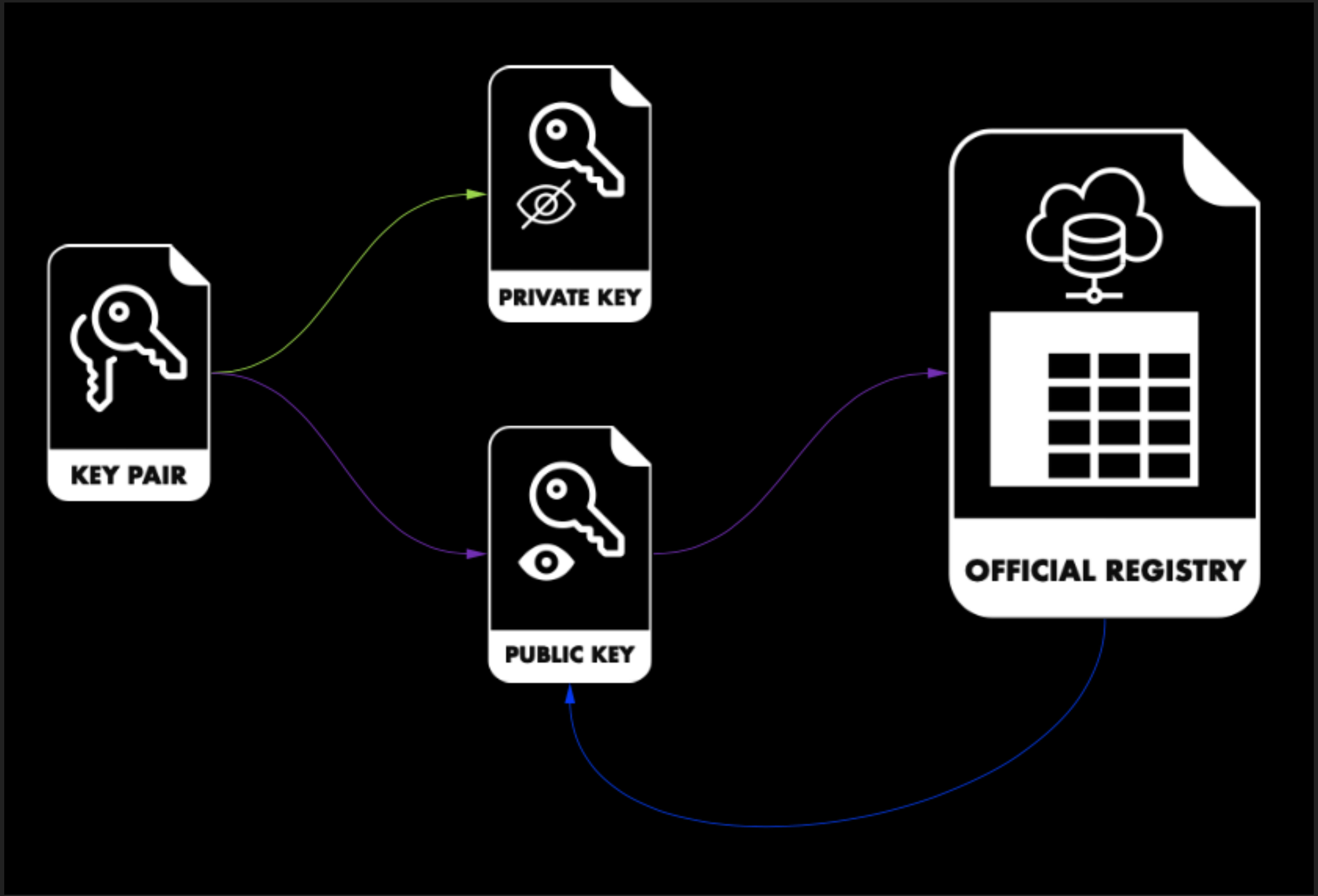
How it works

50,000ft

- Create an **X.509 Public / Private Keypair**
  - Public Key part of **Certificate Chain** from **Authority**
- Make **Claim** and sign with Private Key
- **Publish** Claim as semi-random URL
- **Verify** Claims using Public Key
- **Validate** Claims using certificate chain / business logic

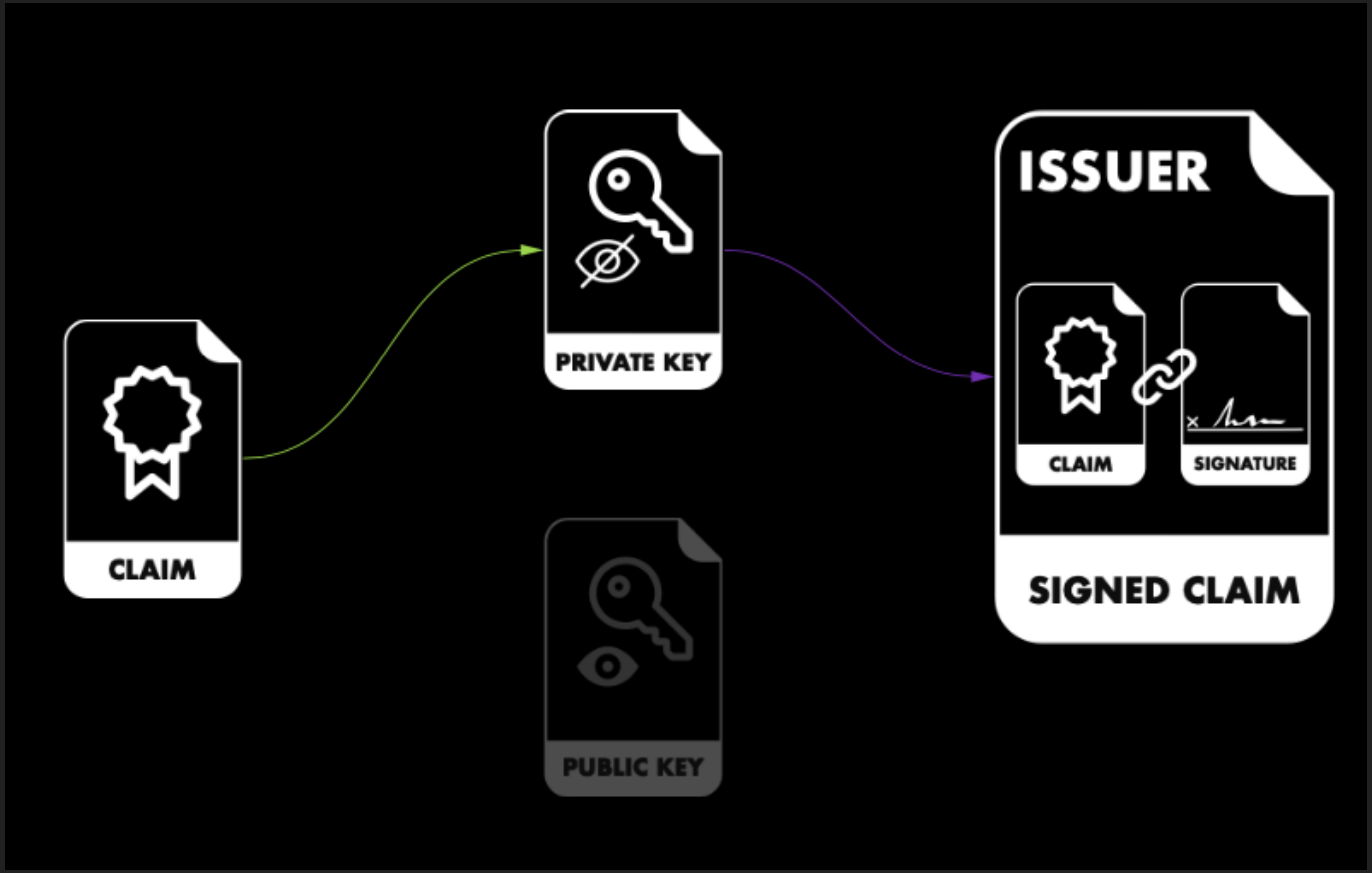
How it works

Public/Private Keypair Creation & Registration



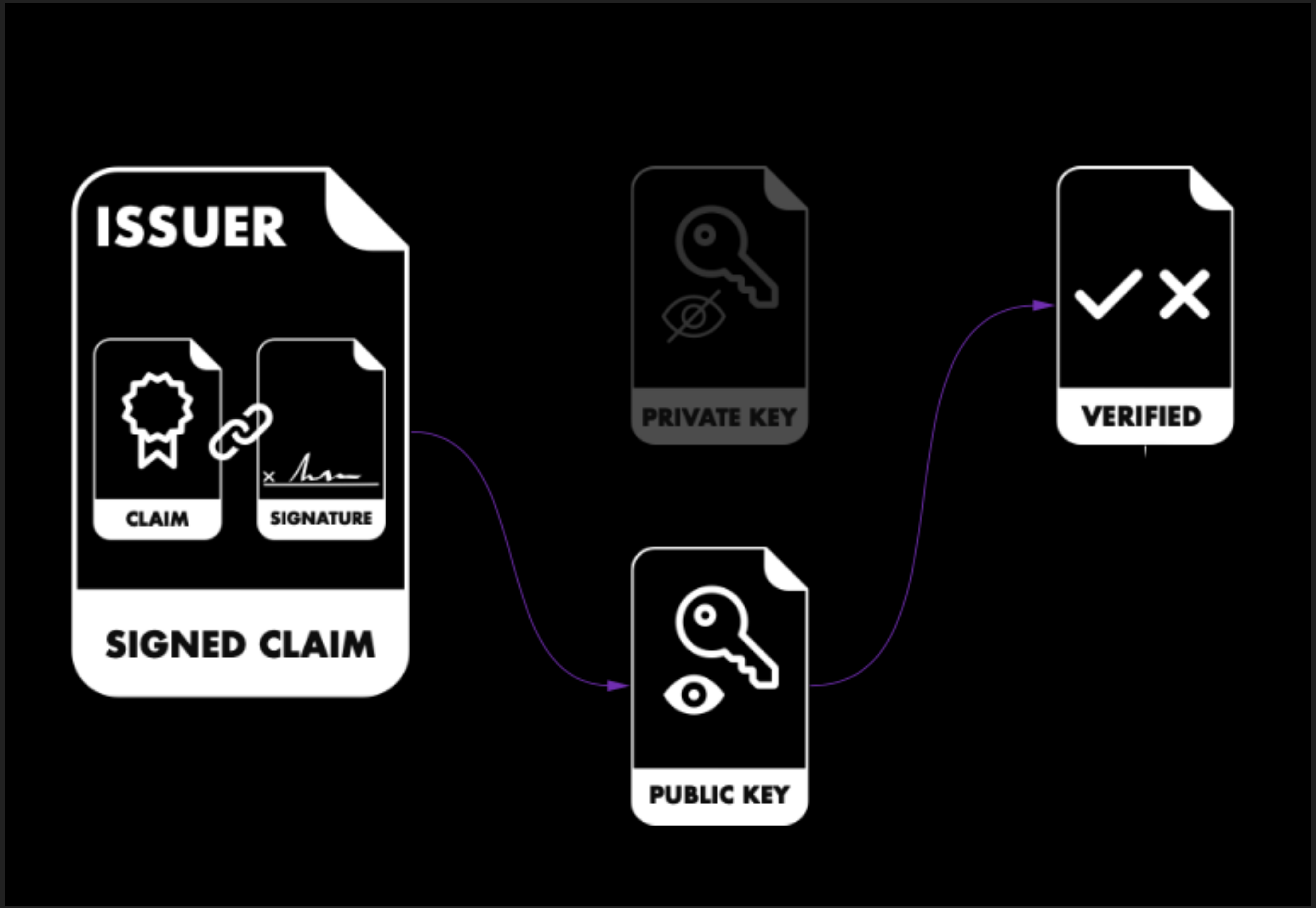
How it works

Claim Signing



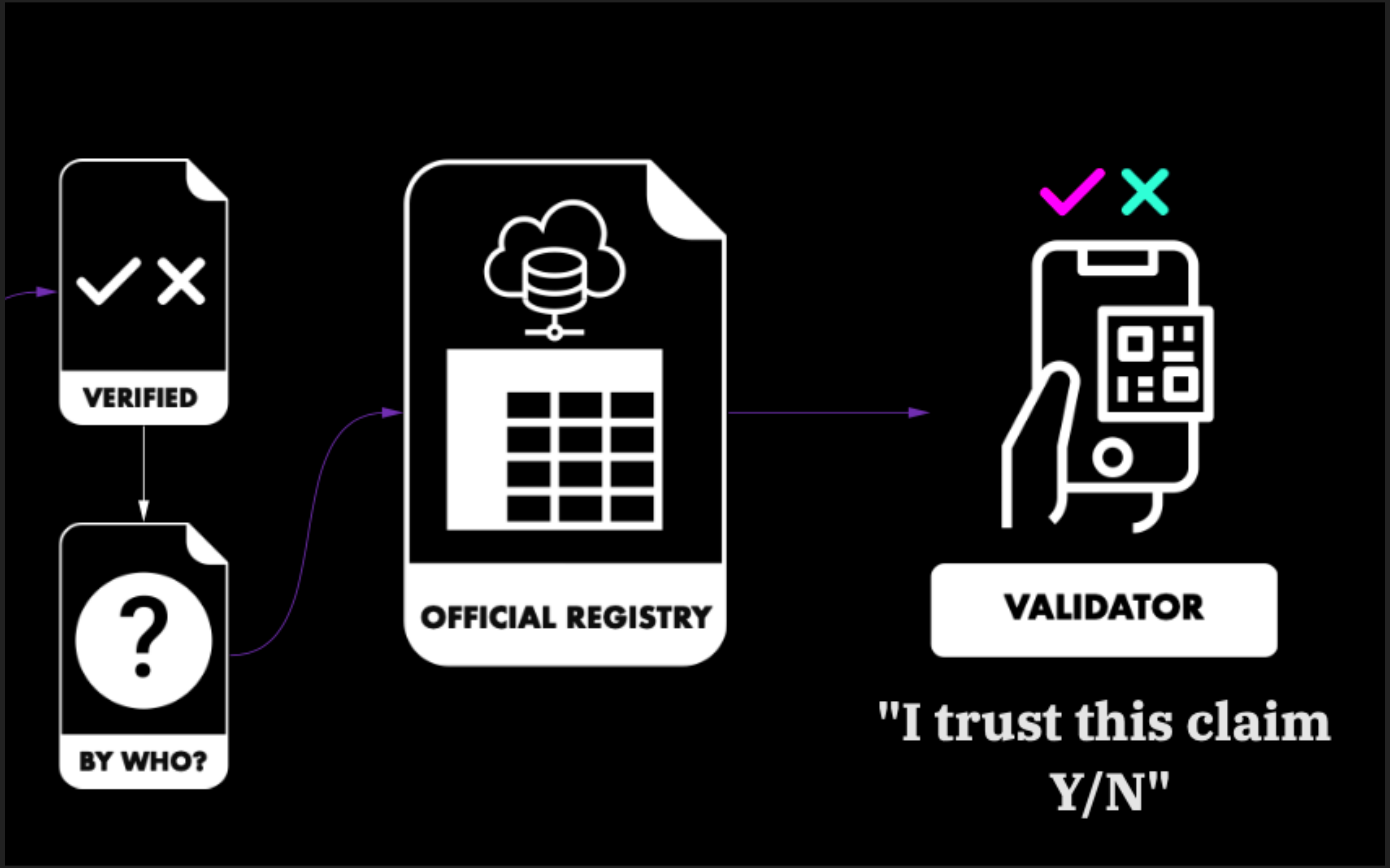
How it works

Verification - Does the Signature Match?



How it works

Validation - Who? What?



How it works

Business Logic

- Assume Claims are documents
- Write Rules as MongoDB-like queries
- Magic!

Find out more

- CCCC4 (JSON-LD Spec): https://cccc4.ca/

- Live Demo: https://passport.consensas.com/

- Open Source: https://github.com/Consensas/information-passport/tree/main/docs

- Video Demo: https://www.youtube.com/watch?v=crethRbfGrE

Thank you!

Contact Me

David Janes
CTO, Consensas
david@consensas.com
@dpjanes