





# Dibran Mulder

CTO Yivi & Caesar Groep

Today:

- Yivi
- EUDI
- PostGuard



# Productvisie

Drie pijlers van ons productportfolio



EUDI

## Yivi voor Personen

*Erkende digitale identiteit*

- Europese digitale identiteits-wallet (EUDI-compliant)
- Veilig inloggen bij gemeenten, overheid en zorg, energie
- Privacy by design: minimale datadeling
- Paspoorten, ID-kaarten en rijbewijzen digitaal



SECURE

## PostGuard

*Veilig data delen*

- End-to-end versleutelde bestanden en berichten
- Veiligmailen voor overheid en bedrijfsleven
- Datakluis: veilig opslaan en delen van documenten
- Geen wachtwoorden, authenticatie via Yivi



TOEKOMST

## Yivi voor Bedrijven

*Cloud wallet voor organisaties*

- Organisatie-identiteit in de cloud/premise
- KvK-verificatie en bedrijfsattributen
- Machine-to-machine authenticatie
- Integratie met bestaande bedrijfssystemen



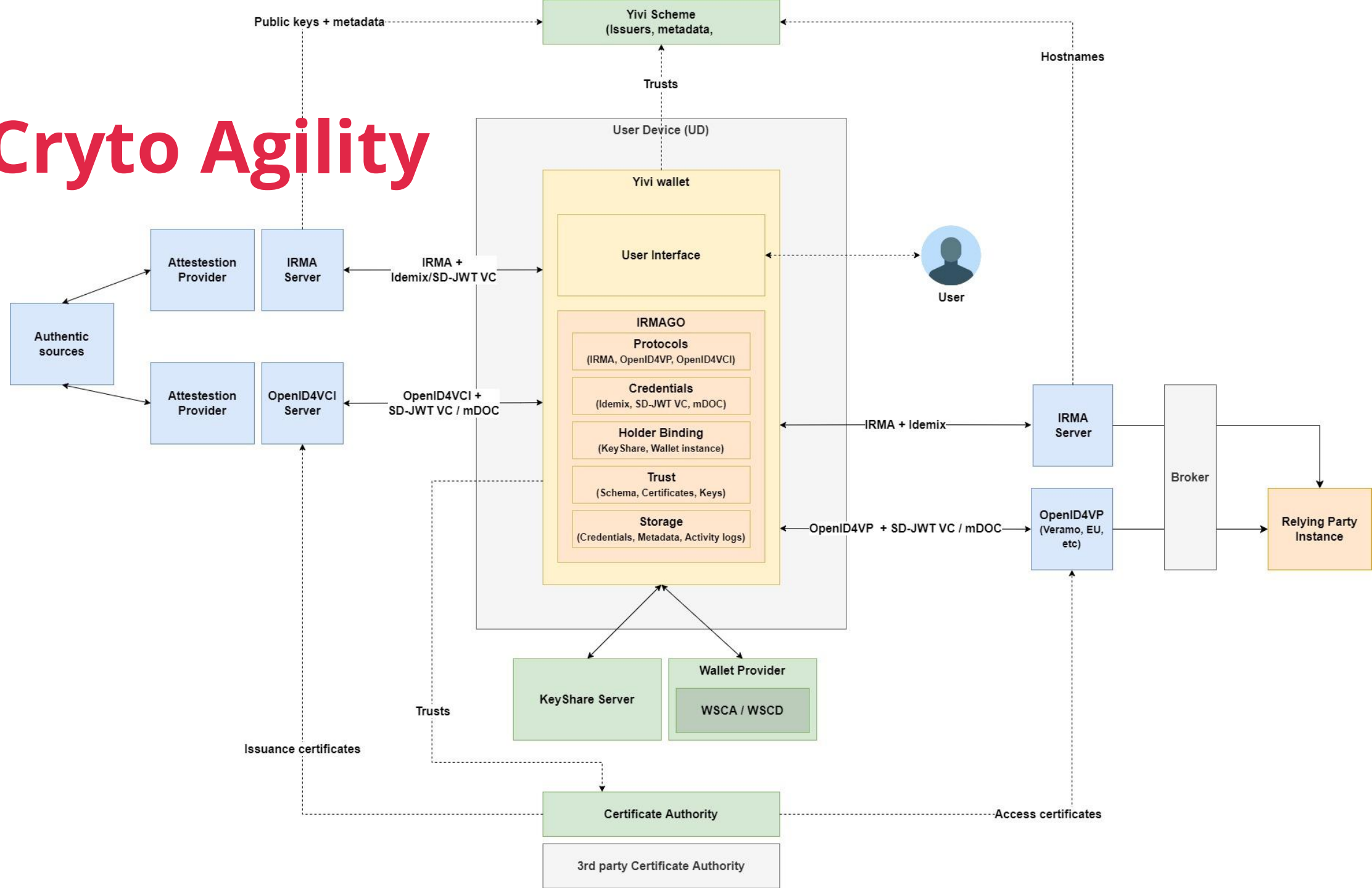
# Goals for Yivi

**Yivi stands for a secure, privacy-friendly digital identity fully under the user's control.**

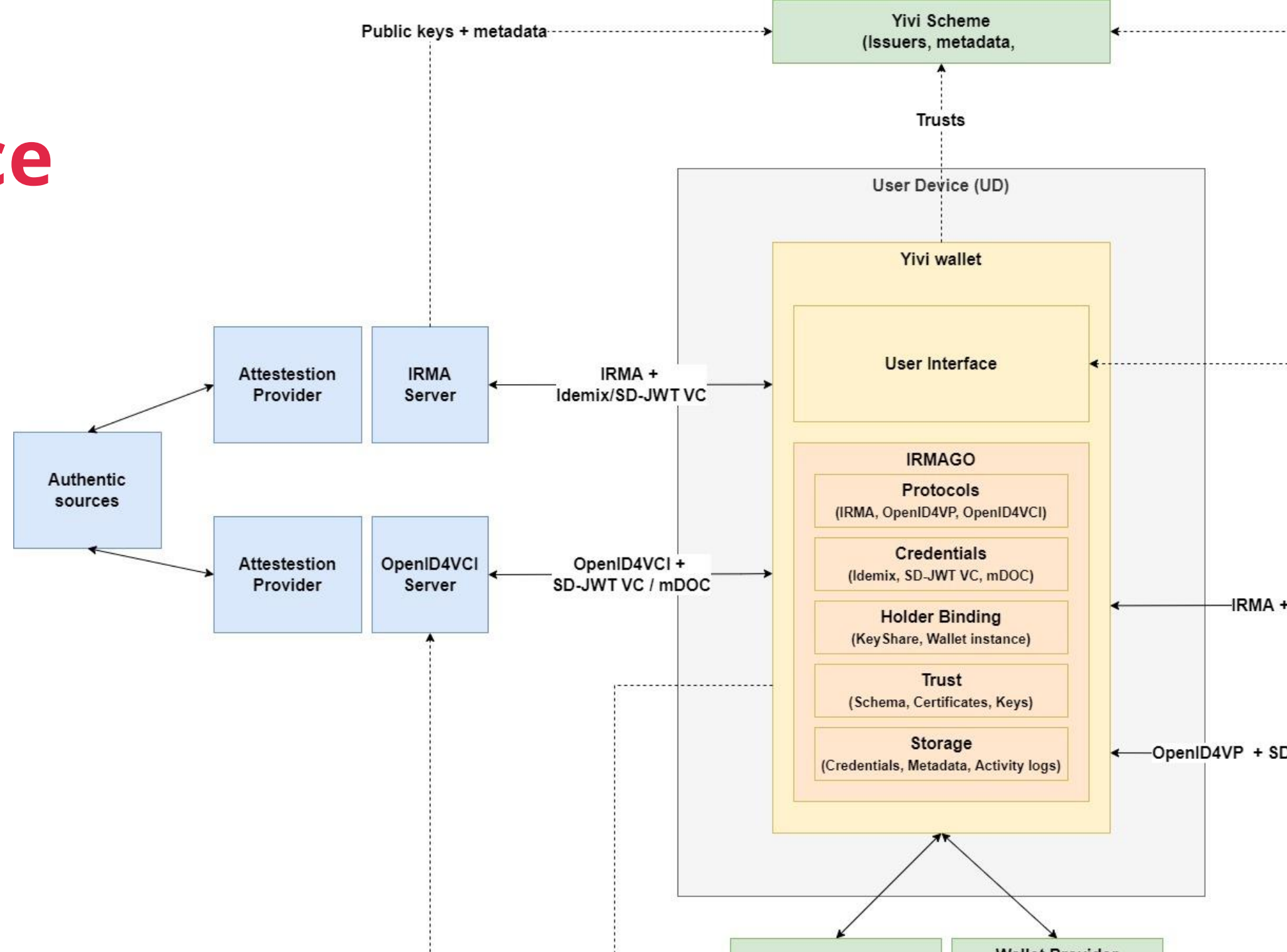
1. Yivi is the most **privacy and user friendly** ID-wallet out there.
2. Yivi is usefull in more and more scenario's **providing solutions for secure and privacy first identification.**
3. Yivi will provide and use **sovereign infrastructure** to **reduce** dependencies on BigTech
4. Yivi will become an **EUDI wallet** in the context of the eIDAS 2.0 regulation



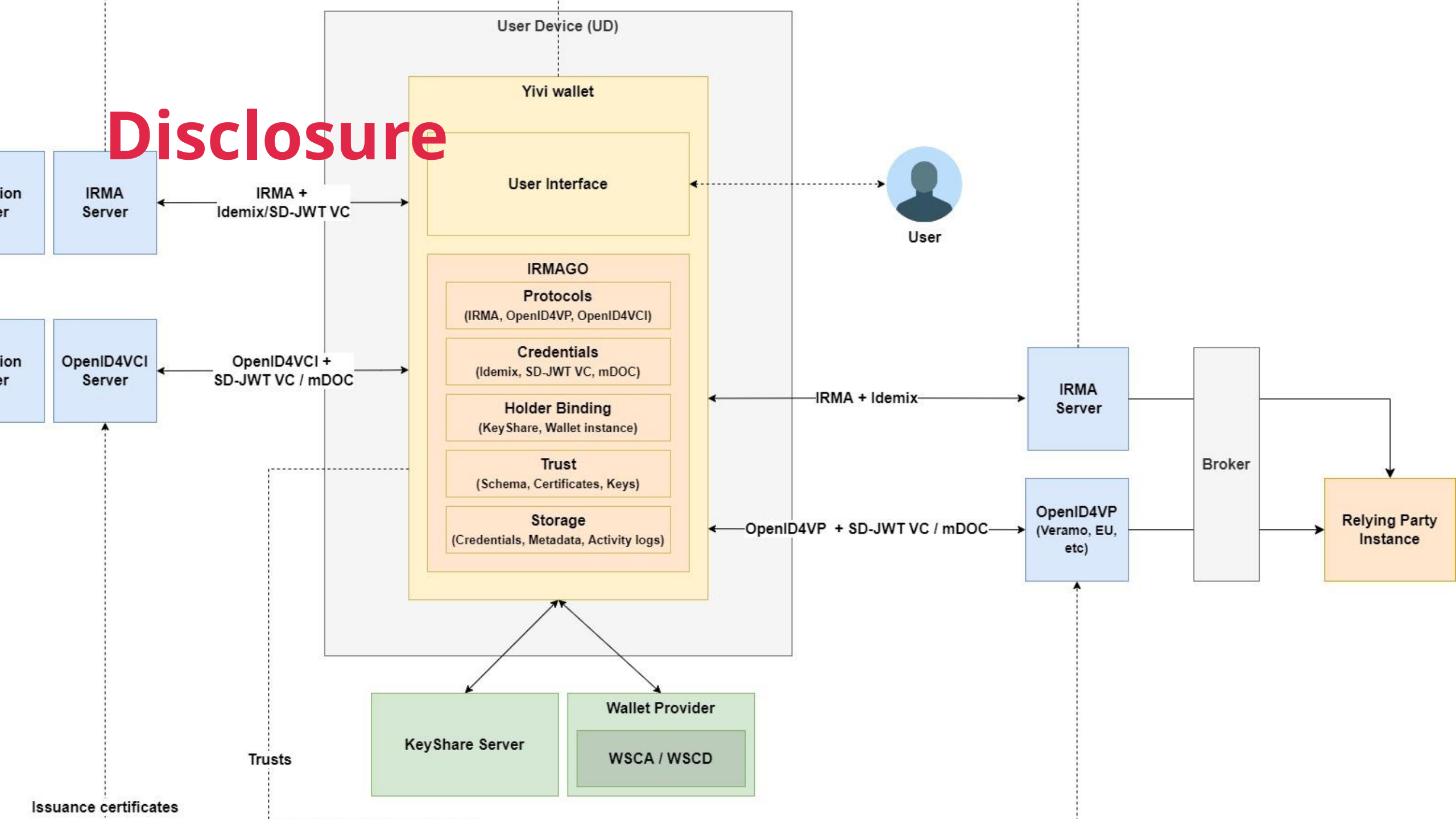
# Crypto Agility



# Issuance



# Disclosure



Announcing

# Full SD-JWT VC support

across all our issuers including  
Gemeente Nijmegen from the 18<sup>th</sup> of May



Start Session

Passport OR ID Card (choice) ▾

- Load preset...
- Mobile number
- Email
- Passport
- ID Card
- Driving Licence
- Email OR Mobile number (choice)
- Passport OR ID Card (choice)**
- ID + Email (multi-credential)
- Contact + Name
- Email + optional phone
- Age check (over18)
- Dutch nationality (predefined value)
- Over 18 = Yes (predefined value)
- Male or Female (predefined values)

```
1 v {
2   "type": "vp
3 v   "dcql_query
4 v     "credent
5 v     {
6
7
8     "passport" ] },
9 v
10
11
12
13
14   },
15 v   {
16
17     "meta": { "vct_values": ["pbd
18     "claims": [
19       { "path": ["firstName"] },
20       { "path": ["lastName"] },
21       { "path": ["dateOfBirth"] }
22     ]
23   }
24 }
25 ],
26   "credential_sets": [{ "options": [{"passport"}, {"idcard"}] }]
27 },
28 "nonce": "nonce",
29 "jar_mode": "by_reference",
30 "request_uri_method": "post",
31 "issuer_chain": "-----BEGIN CERTIFICATE-----\nMIICbTCCAHSgAwIBAgIUX8STjkv3TRF5UBstXlp4ILHy2h0wCgYIKoZIzj0EAwQw\nrjELMAkGA1UEBhMCTkwxDALBgNVBAoMBF1pdmkxKDAmBgNVBAMMH11pdmkgU3Rh\nZ21
32 }
```

IRMA

EUDI

**Veramo****Start Session**

eduID (inline DCQL) ▾

Load preset...

Test credential (given\_name + email)

eduID (by presentation ID)

eduID (inline DCQL)

```
1 v {
2 v   "dcql": {
3 v     "credential": {
4 v       {
5         "id": "eduid-credential",
6         "format": "dc+sd-jwt",
7         "meta": { "vct_values": ["https://issuer.dev.eduid.nl/vct/eduid"] },
8 v       "claims": [
9         { "path": ["given_name"] },
10        { "path": ["family_name"] },
11        { "path": ["email"] },
12        { "path": ["schac_home_organization"] }
13      ]
14    }
15  ]
16 }
17 }
```

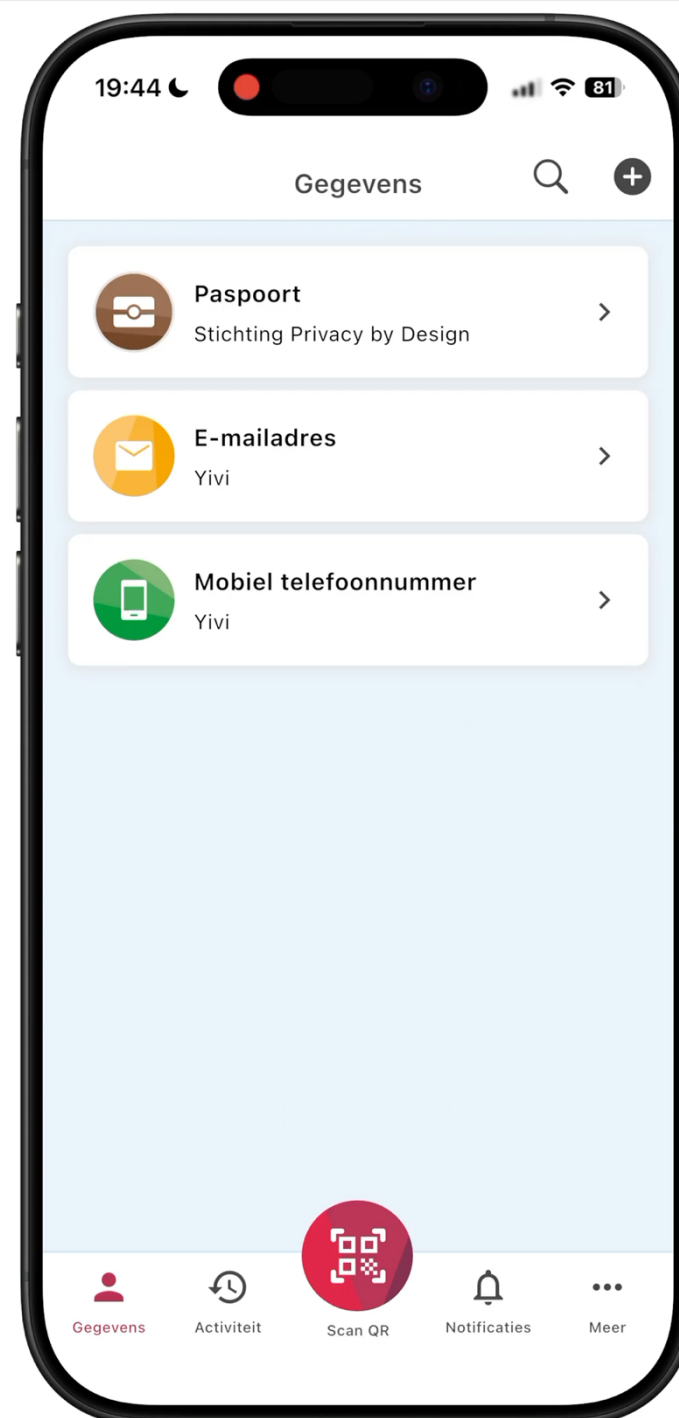
Announcing

# OpenID4VCI support + schemaless credentials



# Demo

## Eduld



# EUDI / ARF interoperability

## Protocols

- IRMA
  - Revocation
- OpenID4VP
  - DCQL
- OpenID4VCI
  - Authorization Code
  - Pre-Authorized Code
- *ISO/IEC 18013-5 proximity*
- *Revocation IETF Token Status List*

## Credential formats

- Idemix
- SD-JWT VC
- *mso\_mdoc ISO/IEC 18013-5*

## Trust

- Access Certificates (registration)
- Keyshare Server / Wallet Provider
- *WCSA/WCSD*
- *OpenID 4 Federation*





***ENISA launches a public consultation on the draft candidate EU Digital Wallet certification scheme, subsequent to the scheme's development with the dedicated Ad Hoc Working Group.***

# Certification Requirements Overview

227 requirements from two ENISA documents — assessed at assurance level “High”

#	Category	Reqs	What It Covers
1–2	<b>General &amp; CAB Process</b>	<b>17</b>	Scheme scope, assurance level, CAB accreditation — fulfilled by the certification process itself
3–4	<b>Risk Management &amp; Policies</b>	<b>12</b>	Risk register (CIR 2024/2981), ISMS, terms & conditions, information security policy
5	<b>Wallet Provider Management</b>	<b>39</b>	Internal org, HR security, access control, crypto controls (EN 319 401), physical security, incident response, supply chain, business continuity
6	<b>Wallet Unit Requirements</b>	<b>47</b>	PID/attestation issuance, management & presentation flows, RP authentication, trust anchor checks, orchestration & input validation
7	<b>Wallet Instance Requirements</b>	<b>16</b>	Mobile app security (MASVS), asset protection, user interaction model, web app security (OWASP ASVS L3)
8	<b>WSCA/WSCD Requirements</b>	<b>15</b>	Cryptographic hardware (HSM), two-factor authentication, key non-exportability, keystore assurance levels
9	<b>Wallet Provider Services</b>	<b>44</b>	WUA issuance & revocation, device eligibility, DoS protection, consent management (GDPR), app distribution
10–12	<b>Vuln. Mgmt, Monitoring &amp; Cert. Lifecycle</b>	<b>37</b>	CVD policy, SBOM, annual surveillance, 5-year certificate, CAB cooperation

NOS

14:17

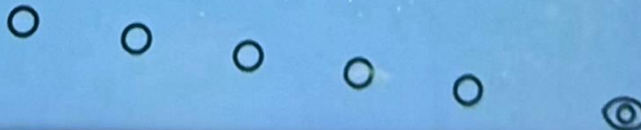


5G 58%

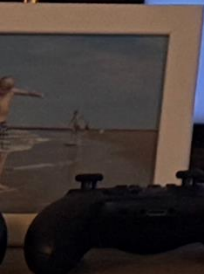


yivi

Voer je pincode in



NOS.nl



# Age verification

## If the European Age Verification app launches today, it will be broken tomorrow

March 10, 2026 · 23 min read



**Dibran Mulder**

CTO @ Caesar Groep



*A security analysis of the EU Age Verification Wallet reveals a privacy-first design with a critical trust gap that undermines its security guarantees.*

**⚠️ UPDATE, APRIL 2026: AN EXPERIMENTAL ZKP HAS APPEARED IN THE WALLET, BUT IT IS NOT A WORKING FEATURE YET**

Since this post was published, the EU Age Verification Android wallet has gained an **experimental Zero-Knowledge Proof implementation** based on Google's [Longfellow ZK](#) library. This partially walks back the "ZKPs are deferred for future work" position quoted below,



**Dibran Mulder** · You

CTO at Yivi and Caesar Groep | Helping organizations in their di...

[View my services](#)

3h · 🌐

This week the EU commission announced that they are ready with their Age Verification Solution, earlier I wrote a blog that the solution would be broken within 24 hours, I was wrong. It took a little bit longer, 48 ...more



**Denis Roio, Ph.D.** ✓ · Following

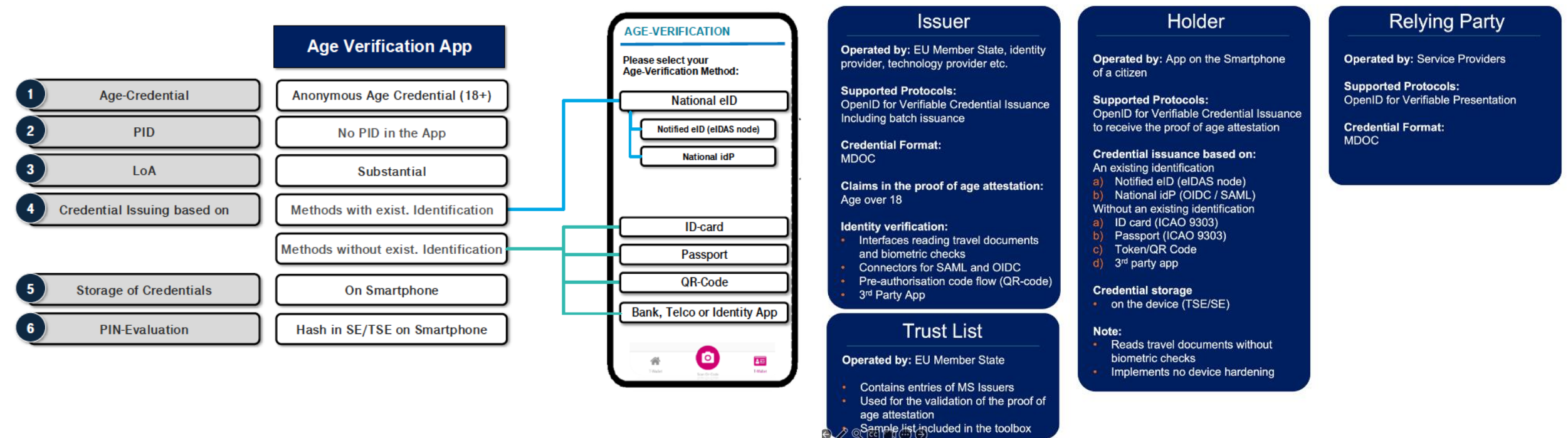
Cryptographer | Philosopher | Founder | Software author | Ethical h...

6h · 🌐

When, in the not too distant future, a young hacker in Europe is caught exploiting a security flaw in an EUDI app, I hope the judge will not rush straight to punishment. ...more



# Age Verification - update



# Open-source Face Verification

- We are performing research on open source face verification aswell as commercial available options.
- Open source update, proof of concept with:
  - Face Recognition
    - GhostFaceNet (TFFlow Lite, 512-dim embedding, cosine similarity)
  - Passive Liveness
    - MiniFASNet (anti-spoofing)
    - rPPG (remote photoplethysmography, detects pulse from face video)
  - Active Liveness
    - 3 randomised challenges (blink, turn left/right, open mouth, smile)



# Goals for PostGuard

**PostGuard** stands for secure, privacy-friendly communication fully under the user's control.

1. **PostGuard** is the **most privacy and user-friendly** encrypted messaging/file sharing solution out there.
2. **PostGuard** is a **secure email communication solution** and a privacy-first **alternative to Zivver**.
3. **PostGuard** is **open source and extensible** framework and part of the CommonGround ecosystem.



## Securely send your files



Drag files here

or

Choose files

Maximum 2 GB

### Recipients

► What should I fill in here?

#### Email address

recipient@example.com

+ Mobile phone number

+ Date of birth

+ Add another recipient

### Message (optional)

This message will not be encrypted and will be included in the notification email.

Type your message here...

**yivi** Sign & send

Tip: In the Yivi app you can add optional data. This way you let the recipient(s) know for sure that these files come from you.

► What is Yivi?





# PostGuard

## Encryption based on identity, not keys

Send encrypted messages and files to anyone using just their email address. No key exchange, no certificates, no hassle.

[What is PostGuard?](#)[Core Concepts](#)[Getting Started](#)

### No key exchange needed

Encrypt data using nothing more than the recipient's email address. There are no public keys to look up and no certificates to manage.

### Identity verification built in

Recipients prove they own their email address (or other attributes) before they can decrypt. Sender identity can be verified too.

### Time-limited keys

Decryption keys expire automatically. Even if a key is compromised, it only works for a specific time window.

### Works everywhere

The JavaScript SDK runs in browsers and Node.js. Addons exist for Thunderbird and Outlook. A CLI tool handles server-side and scripting use cases.

## Quick Start

Install the SDK:

```
npm install @e4a/pg-js
```

bash

Encrypt files and send them to a recipient:

```
import { PostGuard } from '@e4a/pg-js';

const pg = new PostGuard({
  pkgUrl: 'https://pkg.staging.yivi.app',
  cryptifUrl: 'https://fileshare.staging.yivi.app'
```

ts



# PostGuard for Business

Secure, privacy-first email encryption powered by identity-based cryptography

- PostGuard for Business includes
  - File sending via B2C API identification
    - SDK support (.NET, TS, Rust)
  - Audit trails
  - Revoking
  - Custom domains for communication (email)
  - Email clients (Thunderbird & Outlook, others)
  - Bring your own storage



Procolix



# Demo





# Questions



d.mulder@yivi.app



yivi.app / caesar.nl



Dibran Mulder



DibranMulder

