EPICENTER .WORKS for digital rights

Mission Statement

whoidentifies.me

Independent transparency for wallet-relying parties in the EUDI ecosystem

Our mission

With whoidentifies.me, epicenter.works makes wallet-relying parties in the EUDI ecosystem accountable. We harvest and verify the registration data of every wallet-relying party from all 27 national registers and publish it as one EU-wide, versioned and independently verifiable dataset. Data protection authorities, researchers and civil society, who otherwise have no easy access to this data, can then check whether relying parties stay within their registered intended use, and detect over-identification before it becomes standard practice.

What we do

Relying-party registration under Article 5b of Regulation (EU) 2024/1183 is the framework's main safeguard against over-identification. Every wallet-relying party must register its intended use and the attributes it intends to request, and may not request more. Selective disclosure only protects users if relying parties ask for minimal attribute sets, and the registers are where that behaviour becomes observable.

As designed, this transparency stops at national borders. Implementing Regulation (EU) 2025/848 yields 27 national registers with national deviations, but no EU-wide register, no comparison across Member States and no independent verification of what registrars publish. Yet wallets work across borders by design, so the relying parties a user meets may sit in any of the 27 registers.

Access is also harder than the regulation suggests. Some Member States intend to expose only certificate events, such as issuance and revocation, through their registrar API. Knowing which relying parties are currently active, and for which intended uses, then means harvesting, verifying and replaying each Member State's full event stream. Without a project like ours, most watchdogs have no practical way to get at this data.

Users, meanwhile, see one presentation request at a time. The wallet dashboard and the right to report a relying party to a DPA act per transaction and after the fact. Systemic patterns stay invisible: a sector routinely requesting full PID where an age attestation would do, or relying parties in one Member State registering far broader attribute sets than their peers elsewhere.

whoidentifies.me provides the missing ecosystem-wide view. It does for the EUDI trust framework what Certificate Transparency does for the Web PKI: an independent, publicly verifiable record of what registrars publish, that anyone can query and re-verify.

Who we do it for

We build for those who hold the ecosystem to account, and through them for every wallet user.

- **DPAs and eIDAS supervisory bodies** find relying parties in their jurisdiction across all registers, spot excessive attribute requests and prioritise enforcement.
- **Researchers** get a reproducible dataset to compare sectors and Member States.
- **Consumer and digital rights organisations** learn of a problematic intended use, such as an insurer requesting health attributes, when it is registered.
- **Organisations representing groups at risk of exclusion** see the use cases affecting older people, people with disabilities, refugees or people living with HIV.
- **Registrars and the Commission** get an independent client that reports non-conformities with CIR 2025/848 and TS05.
- **Journalists and the public** get evidence on whether the wallet keeps its promises.

How we do it

whoidentifies.me is a four-stage pipeline built solely on legally mandated interfaces.

1. **Collect.** A register connector discovers all national registers and harvests registration data and access and registration certificates (WRPACs, WRPRCs) via the API of CIR 2025/848, as amended by CIR 2026/1730, and TS05. Where a registrar only publishes certificate events, it reconstructs the register's current state. It normalises national extensions into one EU-wide data model, covers intermediaries and logs deviations from the specification.
2. **Verify.** A verification library and CLI check each register response's JWS signature against the registrar's trust anchor and validate WRPRCs against ETSI TS 119 475, including suspension and revocation. Configurable trust stores handle key rollover; anyone can re-run the verification.
3. **Archive.** Signed originals are kept alongside normalised records with provenance and verification status, in a versioned history of each relying party's intended uses and attributes, linked across the eight optional identifier types.
4. **Monitor.** We detect new, modified, suspended and revoked registrations and changed intended uses or attributes, publish them and provide personalised alerts to our users.

The whoidentifies.me front end makes all of this searchable and comparable across sectors and Member States. Pilot: demo.whoidentifies.me; code: github.com/whoidentifies-me.

- **Open and reproducible:** free, self-hostable software; data ships with signed originals.
- **Shared infrastructure:** one reviewable implementation instead of a harvester per DPA or research group.
- **Built for scale:** some 5.7 million companies face mandatory acceptance (Art. 5f); we sync incrementally.
- **Built with its users:** requirements come from workshops with consumer organisations, NGOs and researchers.

Why epicenter.works

epicenter.works is a Vienna-based digital rights NGO, active since 2010, combining legal, policy and technical expertise with free software. We have worked on digital identity since 2017 and on the eIDAS revision since 2021, as the central civil society stakeholder for consumer and privacy interests, and contributed to the draft ETSI standards for the register API.

- **APTITUDE:** member of the European Ecosystem Advisory Board (2026–2027)
- **German Bundestag:** expert testimony on the national eIDAS implementation (2026)
- **SPRIND:** jury of the German EUDI Wallet and relying-party challenges (2025–2026)
- **Dutch government:** review of parts of its national eIDAS implementation (2025)
- **European Commission:** Ad-Hoc Technical Advisory Group on the EUDI Wallet (2024)
- **UN Tech Envoy:** our Executive Director chaired the DPI Safeguards governance WG (2024)

Endorsed by

Five institutions endorse the project and plan to use or support it:

- **Dutch Data Protection Authority (AP):** expects to use it in supervision and investigations.
- **TNO:** supports its development as free and open-source software.
- **IViR, University of Amsterdam:** will use it in the NWO project “Foundations for Identity and Trust at EU scale”.
- **Institute of Networks and Security, JKU Linz:** sees it as the “verifier directory” its CDL Digidow research called for.
- **Leuphana University Lüneburg:** academic support via the ERC project “Doing Digital Identities”.

The endorsements cover the software as an open resource, not any findings it produces.