Project Description

EU Digital Identity Wallet: Ecosystem Monitor

Realtime Accountability Platform

Executive Summary

The proposed transparency platform is intended to ensure that the EU's digital identity system (eIDAS) leaves no room for violations of fundamental rights, discrimination and manipulation. This is going to be made possible by creating transparency about which companies or institutions inquire about which information from users via the eIDAS wallet.

This information will provide the users of the wallet and the stakeholder groups impacted by the system actionable information about the whole ecosystem and real time information about any potential developments that are relevant to them. Our approach can encompass the whole ecosystem based on official transparency APIs on national levels that we will aggregate and normalize on EU level. This will empower users, researchers, businesses and civil society to effectively obtain credible information about Europe's digital identity ecosystem and how it evolves over time.

Subject Matter

The eIDAS Regulation (Electronic IDentification, Authentication and trust Services) is an EU-wide regulation that enables the secure and standardized use of electronic identities and trust services such as digital signatures, seals and time stamps. It ensures that citizens and companies can use digital identities across borders to identify themselves online or to sign contracts digitally with legal validity. To this end, the eIDAS Regulation (EU) 2024/1183 also obliges all member states to introduce a **digital wallet (eIDAS wallet)** for their **440 million EU citizens by 28. November 2026**. Like a physical wallet, this wallet is also going to be used to collect personal information in one place in order to be able to use it to identify themselves on occasion, so that the above-mentioned objectives of the regulation can also be achieved in practice. In contrast to the classic wallet, the digital wallet contains next to **name, address, a biometric photo**, etc. also attributes from other government or private sector sources such as **educational qualifications, health information or financial data**. The transfer can take place online/remotely or offline in physical proximity. The system can (and in many cases must) be used by both the public and the private sector - and in almost all areas of life: from dealing with public authorities to bank transactions, public transport and even logging in to digital services.

Risks for Fundamental Rights

The introduction of the **eIDAS wallet** entails considerable risks for data protection, informational self-determination and social justice. Due to its extensive use in everyday life and the particular quality of the data transferred, an infrastructure is being created that deeply reaches into people's lives. In contrast to conventional web or paper form entries, much of this data comes directly from government sources and is provided with a transferable cryptographic **certificate of authenticity**. While in the digital space often unreliable or manipulated information circulates, the eIDAS wallet offers **verified data with guaranteed truthfulness**. It is precisely this reliability that makes it particularly attractive for most companies and authorities - but also vulnerable to misuse. The

possibility to retrieve data that can be repeatedly verified beyond doubt increases the risk of it being used for commercial interests, targeted profiling or surveillance.

A central problem is the lack of an overview of **who has access to which data**. The group of so-called '**relying parties**' - i.e. companies, organizations and authorities that can potentially access data – is enormous. It ranges from small service providers to international tech companies to state institutions. In addition, there are hardly any restrictions on the categories of data that can be queried: Next to name, address and biometric photo, even sensitive information such as educational background, financial situation or health data can be recorded and transmitted. If this data is misused, there is a risk of discrimination, manipulation and social exclusion. Without transparent control, there are massive risks to fundamental rights and social justice. The wide-availability of government issued personal information combined with transferable cryptographic proofs of authenticity entails the **risk of far-reaching privacy harms by state and private actors and threatens individual autonomy**.

At the same time, access to essential services could become more difficult for people with limited digital access or for people with limited digital skills, further increasing social inequalities. The **risk of discrimination** also increases if employers or insurance companies use sensitive data to disadvantage certain groups. There is also the threat of a shrinking civil space: The widespread availability of cheap identification methods also creates the **risk of over-identification** in everyday situations. The obligation to provide digital identification can be a deterrent, especially for marginalized groups, and make anonymous participation in social or political movements more difficult.

Solution: eIDAS transparency platform

To counter the risks of the eIDAS Wallet described above, the **eIDAS transparency platform** provides much-needed clarity about **which organizations and companies request which data and how it is used**. The eIDAS Regulation obliges all **public and private organizations ('relying parties')** to register in a national register before they are allowed to retrieve data from the digital wallet.

Each registration contains information on the particular use case and the detailed personal data requested. These national registers can be accessed in real time via a API programming interface and contain **live data, as well as a ten-year history.**[1]

The platform **aggregates and analyses these national registers** in order to create transparency and prevent abuse. It focuses on the following central functions:

- **Database of all relying parties:** An overview of all registered companies and institutions in all EU member states with detailed information on their use cases and the data requested. Optional: Blockchain technology allows us to decentralize this transparency record and ensure tamper-resident truthfulness of the data.
- **User side reporting system:** A simple way[2] for users to report problematic data queries or violations, including instructions on how to appeal, submit a complaint and connect to local NGOs dedicated for particular constituencies. This includes any form of coercion or mandatory use of the digital wallet, which is illegal according to EU law.[3]

1 See Article 5b of Regulation (EU) 2024/1183 and its Implementing Regulation (EU) 2025/848 for the technical spec.
2 Through SEO we will make the pages for each relying party easy to find for users in local languages.
3 See Article 5a(15) of Regulation (EU) 2024/1183.

- **Analysis and classification:** Segmentation of companies by business type, use case and queried attributes in order to enable **risk assessments** and recognize misuse at an early stage.
- **Register of attributes:** Documentation of new personal data in the eIDAS ecosystem to identify impacts on data protection and usage practices at an early stage.
- **Real-time information for NGOs:** Consumer protection organisations, worker unions and NGOs receive automatic notifications about new data queries or changes in usage practices in order to react quickly to injustices.
- **Open source & open data:** The source code and - where legally possible - aggregated data are made freely accessible to ensure maximum transparency.
- **Stakeholder integration:** The platform is developed **together with worker unions, consumer organisations and NGOs** in order to incorporate their requirements directly.
- **Information & assistance:** Those affected receive **target group-orientated information about their rights** as well as support in the defense against abuse or negative consequences of the system.

Social Relevance of the eIDAS Transparency Platform

The introduction of the eIDAS Wallet fundamentally changes how digital identities are managed and used. While such systems are gaining in importance worldwide, there is still a lack of independent mechanisms to control their use. Without transparency, there is a risk of misuse, unjustified data queries and a creeping expansion of digital surveillance. The **eIDAS transparency platform** addresses precisely this issue and creates an **independent structure to control the use of the digital wallet.**

By making the requests for access to personal data traceable, it strengthens **individual rights**, increases the **accountability of companies and institutions** and helps **recognise undesirable developments at an early stage and counteract them**. Particularly **marginalised groups**, who are often affected by digital inequality, benefit from a **protection mechanism** that prevents discrimination and ensures equal access to digital services.
Should misuse of personal data or discrimination nevertheless occur, affected persons or civil society actors such as NGOs can quickly recognize this through the transparency platform, companies and institutions can be held accountable and **help those affected to assert their rights**.
The platform thus closes a key gap in the digital ecosystem and sets new standards for **transparency, digital justice and democratic control** in Europe.

About our Organization

Epicenter.works is a digital rights NGO based in Vienna that has been campaigning for fundamental rights in the digital age for 15 years.[4] The organization endeavors to find viable paths on the basis of human rights in the midst of the technical and social changes of the digital age. We see ourselves as an advocacy organization for fundamental rights and freedoms and, as a strong voice of civil society, we campaign for a human-centered approach to the opportunities and risks of technology.

The non-profit organization epicenter.works is 50% funded by donations and now employs 9 people. It is run by Thomas Lohninger as the Executive Director and Tanja Mally as Managing Director. The

4 https://epicenter.works/en/history

remaining budget is provided by external funding from organizations that share our values.[5] We are independent from all industry groups and political parties.[6] Epicenter.works works close to the legislative process in Austria, at EU level as well as internationally at the United Nations and sees itself as a civil society 'watch dog' on digital rights issues. We are best known for our work in abolishing the data retention surveillance law in Europe, establishing net neutrality protections in EU law and enshrining human rights protections in the EU's digital identity law.

Why we want to work on this project

Epicenter.works has been working on the topic of digital identities since 2017 and has been significantly involved in the negotiations on behalf of civil society since the start of the eIDAS reform in 2021. In countless joint submissions,[7] analyses,[8] interviews,[9] and presentations[10] we have accompanied the topic. In addition, we have experience with the project management of large open-source software projects and work closely with NGOs on various topics.[11]

Many of our proposals for improvements were incorporated into the EU law, such as the obligation to register relying parties, the obligation to publish national registers online, protection against discrimination for people who do not use the digital wallet and countless improvements to the data protection of the digital wallet (unlinkability, unobservability, zero-knowledge proofs, etc.).[12] Now that the legislative process has concluded, we want to shift our attention to enforcement and field building to empower affected communities to uphold the rights of people that will be affected by the EU's digital identity system.

System Description

- The core pillar of the system is a data base about every relying party registered in the EU. Each relying party will have a webpage with detailed and easily accessible information from their registration. The law obliges the relying party and Member States to keep the information in their register up to date. Since relying parties can interact cross-border, only looking at one national data base wouldn't be sufficient. We expect between 27 and 70 such registers that need to be scraped.
- Users of the Wallet can report issues with a particular relying party and exchange experiences, including means of redress.
- The system also allows the segmentation of companies according to their business types (where available), their use case, attributes they intend to request and user complaints received.
- The register of attributes allows us to also keep an overview about new personal information that becomes available in the eIDAS ecosystem.

5 https://epicenter.works/en/content/epicenterworks-fundraising-policy
6 https://epicenter.works/en/content/interne-policy-zur-unabhaengigkeit-des-vereins-von-politischen-parteien
7 Documents - epicenter.works
8 eID & Digital Public Infrastructures - epicenter.works
9 Recommended Articles - epicenter.works
10 Please Identify Yourself! - media.ccc.de, EU's Digital Identity Systems - Reality Check and Techniques for Better Privacy - media.ccc.de and EU's Digital Identity Systems - Reality Check and Techniques for Better Privacy - media.ccc.de
11 DearMEP - DearMEP
12 Analysis of Privacy-by-Design EU Legislation on Digital Public Infrastructures - epicenter.works

- NGOs working for particular user groups can obtain information about relying parties relevant to their constituency.

Scale and Estimated Storage Needs

The eIDAS Regulation contains legal obligations for certain actors to use the system. All eGovernment services in EU Member States on federal and local level are obliged to use the Wallet, as well as essential services that are legally obliged to identify their customers like water and waste disposal, banking, public transport and energy services. All Big Tech platforms[13] are obliged the offer the Wallet as means to login to their services.

Other private entities can chose to use the eIDAS ecosystem by registering with the eIDAS authority of their country. All parties that want to use the eIDAS ecosystem are called relying parties. The register of relying parties has to be made available by each Member State in machine readable format. It contains information to identify the legal entity, how it intends to use the system, which information it intends to request from it's users, if it falls under a legal obligation to identify their users (KYC) and other information.

The total number of relying parties registered throughout Europe is impossible to assess accurately at this point. It will certainly increase over time depending on the timing of national roll-outs, sector specific legislation and company uptake in any given country. Also the impact assessment[14] of the European Commission doesn't provide a clear estimate for this number. The specific sectors like that are legally obliged to use the wallet (water, energy, telecommunications and education) amount to ruffly 5,7 million companies in the EU. Currently only 26 companies qualify as big tech platforms that are legally obliged to support eIDAS. The number of public sector bodies offering eGovernment services that require eIDAS support can be estimated at 2977 public administration bodies on central, regional and local level and additional 89.000 municipalities.

Based on the implementing acts for relying party registration we calculate the required storage for one individual relying party between 45KB and 60KB with a peak maximum of 150KB, which includes estimates for versioning and multiple use cases per relying party. Based on these numbers we estimate to have a **total storage between 248GB and 830GB**.

Risks of this project

The three main risks we can identify are:

1. There will be technical differences between member states in the programming interfaces (APIs) via which we will obtain the official records about registered relying parties. Part of the project is adaptation to these differences and standardization of the information obtained from them. Since we know the implementing act that requires a certain level of harmonization, these technical difficulties can be mitigated.
2. We expect that a minority of EU member states will not meet the deadline of 28. November 2026 when they have to offer at least one digital identity wallet solution to their population. Nevertheless, the majority of member states clearly indicated they will meet this deadline. The

13 VLOPS according to the DSA

14 https://digital-strategy.ec.europa.eu/en/library/study-support-impact-assessment-revision-eidas-regulation?utm_source=chatgpt.com

eIDAS monitor will make those differences between countries transparent to the users and include new countries as they come online.

3. The total number of relying parties is unknown and might grow rapidly over time. With the proliferation of the eIDAS ecosystem into more countries and sectors the system has to sustain constant growth. We know that some sectors will participate because the law obliges them[15]. Others might join because they see benefit in it. The amount of data will not be the problem, but visualization and analysis will become more complex when the data set becomes bigger and more diverse. We will meet this risk by allowing for sementation, searching and alert functions and by making the full data set available to outside experts.

Technical Development Plan

Phase 1: Planing & Requirements

- Requirements Gathering from affected stakeholders. This will include participatory workshops that directly impact the design of the system. Output: Requirements document.
- Initial User Flows & Wireframes (UI/UX). Create high-level user journeys (e.g., how a user views registered organizations, sets alert filters). Draft low-fidelity wireframes for main screens (organization lists, data categories, etc.). Output: Preliminary wireframes and user flow diagrams.
- Technical Architecture Blueprint (Dev). Define overall system architecture (crawler design, database schema, potential microservices vs. monolith), ensuring flexibility for different country APIs. Output: Architecture diagrams, tech stack decision, initial data model documentation.

Phase 2: Core Architecture

- Base Crawler & Mock Data Integration (Dev). Implement a minimal crawler against mock APIs to simulate future eIDAS data. Parse and store organizational info in the database. Output: A working backend prototype demonstrating how data ingestion would function.
- Basic Database & Backend Services (Dev). Set up the database structure and any core backend services to expose the crawler's stored data via REST or GraphQL endpoints. Output: Database schema, backend endpoints for data retrieval.

Phase 3: Prototype

- Basic Frontend UI / UX Design (UI/UX). Transform earlier wireframes into basic page designs for listing organizations, data categories, and sectors. Output: Design for a minimal working prototype design (end-to-end) demonstrating data flow from crawler to front-end
- Basic Front-End Prototype (Dev). Implement the front-end using the new backend services (e.g., display lists in real-time from the database). Output: Minimal working prototype (end-to-end) demonstrating data flow from crawler to front-end

Phase 4: Refinement & Testing

15 Article 5f of Regulation (EU) 2024/1183 requires companies and public authorities in the sectors education, social security, transportation, energy, finance, health, drinking water, postal services, digital infrastructures, education or telecommunication that are required to identify their users to support the Wallet, as well as eGovernment services and Big Tech companies.

- Enhanced Crawler Functionality (Dev). Improve the crawler to handle multiple data formats, scheduling, error handling; integrate with any pilot-level country APIs if they exist at this stage. Output: A more robust, flexible crawler ready for full-scale data ingestion.
- Reasonableness Rules & Flagging (Dev). Implement logic to compare an organization's declared sector to the data categories they request, flagging unusual or excessive requests. Output: Backend logic that marks suspicious or out-of-scope requests.
- UI/UX Enhancements & Feedback Iteration (UI/UX + Dev). Refine designs based on internal feedback; design how flags or "unusual requests" appear in the UI. Implement front-end features for displaying flags; possibly add sorting or filtering of flagged items. Output: Polished interface showing flagged items, improved navigation
- Testing & Documentation (Dev + UI/UX). Conduct broader testing (unit, integration, and usability). Update technical and user-facing documentation to reflect current features. Output: A beta-ready prototype with documented functionality

Phase 5: Alerting System & Pilot Launch

- Filter-Based Alerting Module (Dev). Implement logic for user-defined filters (e.g., "Alert me if a healthcare org requests financial data"). Enable automated or on-demand alerts. Output: Backend service supporting user-configurable alert rules
- Alert Configuration UI (UI/UX + Dev). Design screens or dialogs where users set/edit alert filters. Output: User-friendly front-end to create/edit alerts
- Pilot Integration & Feedback (Dev + UI/UX). If a Member State API is now available, integrate the crawler with real data in a pilot environment. Collect feedback from pilot participants. Output: Real data pilot, pilot report with feedback on system performance and usability

Phase 6: integrate eIDAS live API

- Integration with official eIDAS APIs (Dev). Connect the crawler to production APIs of each participating Member State; handle variations in data format. Output: Live aggregator pulling real registration data from multiple EU sources
- Performance & Security Hardening (Dev). Optimize performance to handle production-level traffic, conduct security audits/penetration tests, and finalize privacy safeguards. Output: A production-ready, secure platform
- Advanced UI/UX & Final Polish (UI/UX + Dev). UI/UX: Refine dashboards, add advanced filtering/sorting, finalize the visual design. Dev: Address any final feature requests, fix late-stage bugs, ensure cross-browser/device compatibility. Output: A polished, user-friendly interface prepared for public release

Phase 7: IPFS integration (*under consideration*)

- IPFS upload (Dev). Microservice which caches entires before upload to IPFS storage provider that contain a failsafe mechanism and retains the IPFS ID. Crawler adjustment. The crawler needs to send the data additionally to the new microservice
- UI/UX integration. Frontend needs to be adjusted to also query the new microservice for the IPFS IDs

Phase 8: continuous maintenance

- Maintenance & Updates (Dev). Continual bug fixes, security patches, performance monitoring, and adaptation to changes in Member States' APIs. Dependencies: Post-release environment; ongoing as APIs evolve. Output: A stable system that remains up-to-date and reliable
- UI/UX Enhancements (UI/UX + Dev). Description: Incremental feature updates (e.g., new alert types, expanded analytics, multi-language support) and regular UX improvements based on user feedback. Output: A continually evolving, user-centric platform