Dear President and Vice Presidents MEP Metsola, MEP Karas, MEP Picierno, MEP Silva Pereira, MEP Kopacz, MEP Regner, MEP Wieland, MEP Barley, MEP Charanzová, MEP Šimečka, MEP Beer, MEP Zīle, MEP Papadimoulis, MEP Hautala, MEP Kolaja,
Dear Rapporteur, Opinion Rapporteurs and Shadow Rapporteurs MEP Jerković, MEP Terheş, MEP Arimont, MEP Ansip, MEP Terras, MEP Mituța, MEP Peksa, MEP Borchia, MEP Roos, MEP Kountoura, MEP Bielan, MEP Vandenkendelaere, MEP Pelletier, MEP Joron, MEP Maldonado López, MEP Maurel, MEP Benifei, MEP Breyer, MEP Melchior, MEP Kaljurand, MEP Toom, MEP Vilimsky, MEP Ernst,

1. February 2023

The undersigned 39 civil society organisations, academics and experts are concerned about the upcoming votes on the eIDAS Regulation (EU) 2021/0136 (COD) in the European Parliament. Digital Identity systems have raised severe fundamental rights concerns all around the world. The signatories of this letter want to hold the European Union to its responsibility to protect fundamental rights and create a system that's not exposing the most sensitive health, finance and identity information to third parties. If Europe wants to lead on this important issue, you have to get this right.

We acknowledge the well-developed data protection framework and legal basis underpinning the ongoing digital identity reform in Europe. These are necessary but insufficient preconditions for a system that might serve as the central, ubiquitous platform upon which access to eGovernment, commerce, education, social services and the labour market might soon depend upon.

It is vital that potential users have a real choice about using or not using this system. Therefore, it is necessary to enshrine strong non-discrimination protections in law for those parts of the population deciding not or not being able to use the new digital identity system. Senior citizens, less digital literate parts of the population and people without a smartphone shouldn't be hindered in their participation in society simply because of them not having a digital identity. Such protections need to apply to both the public and private sector. They not only avoid fundamental rights infringements and the amplification of social injustices, they also help create the trust among the population which is necessary so the system can become successful, as the tool of genuine choice for most users.

Subsequently, we expect a digital identity system created by the EU to follow the principles of privacy by design and by default. Hence, It should be technically impossible for issuers of the system, companies connected to them or the providers of attributes to obtain knowledge about how users are using the system. Should the system see wide adoption, it could provide a panoptical view about all aspects of daily life. Only strong technical protections on the architecture level can prevent data about user behaviour to

proliferate and be abused. This has been achieved with the EU Digital COVID Certificate (EU) 2021/953 and the same standard has to be upheld here.

Privacy by design also excludes the creation of a unique and persistent identifier, which can always be used to track user behaviour across interactions with individual companies or government departments. It would be blind eyed of the European Union to believe a unique and persistent identifier would not be abused by Big Tech companies to track and surveil their users. Such a "super-cookie" would not only raise serious constitutional concerns in several member states, it might also defeat the purpose of this regulation to provide privacy-friendly alternatives to the dominant Big Tech companies. Ultimately, The system will be judged by the robustness and effectiveness of its technical and legal safeguards against tracking and profiling of user behaviour.

Subsequently, the eIDAS regulation has to regulate which companies or government entities (relying parties) are allowed to ask users for which information. A system that can provide access to identity, financial and health information of hundreds of millions of people will always be a lucrative attack surface for bad actors. There needs to be – as a minimum – effective redress mechanisms in each member state to act upon consumer protection and fraud complaints in their territory, irrespective of where the relying party is established. A truly trusted environment can only be achieved if relying parties have to be unlocked by their member state of establishment for their use case before being allowed to request personal information from users via the new system. This idea was raised under the French Presidency in the Council of the European Union. Similarly, government certified identification information should not be available for use cases not based on legal Know-your-Customer obligations.

Lastly, we want to highlight the IT-security risk that is introduced by mandating support for Qualified Website Authentication Certificates (QWACs) from web browsers.[1] Although this is not a direct digital identity issue, it is undermining the security architecture of the world wide web for questionable commercial motives of Trust Service Providers. Not only has this approach historically failed to increase security by providing confusing information to users, it also enables government surveillance of internet traffic on a large scale.[2] Ultimately, such provisions are detrimental for the security of all users and risk the popular support for this proposal as a whole.

---

1 https://www.eff.org/de/deeplinks/2022/02/what-duck-why-eu-proposal-require-qwacs-will-hurt-internet-security

2 https://blog.mozilla.org/netpolicy/2020/10/08/the-eus-current-approach-to-qwacs-qualified-website-authentication-certificates-will-undermine-security-on-the-open-web/

The organisations signing this letter believe a European system that respects fundamental rights could be a global game changer. We urge you to take these points into consideration in the upcoming votes in the ITRE committee and in plenary, as well as in the upcoming trialogue negotiations. Please take the citizens' perspective into account in this important discussion. We remain available for further consultation.

To summarise, these are our main points[3]:

- Ensure free choice about using the digital identity system by non-discrimination protections for public and private services
- Prevent observability of user behaviour and any transactions of personal information conducted in the system by governments, issuers and attribute providers
- Uphold privacy-by-design by not establishing a unique and persistent identifier
- Effective regulation of use cases, prevent excessive information requests, limit government issued identification information to legal KYC obligations
- Remove provisions that mandate support of Qualified Website Authentication Certificates from web browsers.

Sincerely,

Epicenter.works - for digital rights (NGO, Austria)
European Digital Rights (NGO, EU)
Privacy International (NGO, International)
Civil Liberties Union for Europe (NGO, EU)
Electronic Frontier Foundation (NGO, USA)
R3D: Red en defensa de los derechos digitales (NGO, México)
DFRI - Föreningen för digitala fri- och rättigheter (NGO, Sweden)
Unwanted Witness (NGO, Uganda)
Temple University Institute for Law, Innovation & Technology (Academic, USA)
La Quadrature du Net (NGO, France)
Chaos Computer Club e.V. (NGO, Germany)
Digitalcourage e.V. (NGO, Germany)
Homo Digitalis (NGO, Greece)
Thai Netizen Network (NGO, Thailand)
Fundación Karisma(NGO, Colombia)
Digital Access (NGO, Cameroon)
Citizen D / Državljan D (NGO, Slovenia)

[3] For a more detailed analysis of these points in light of the Commission proposal and the Council general approach: https://en.epicenter.works/document/3865 and https://en.epicenter.works/document/4384

Association for Technology and Internet (ApTI) (NGO, Romania)
Electronic Frontier Finland (NGO, Finland)
IT-Pol (NGO, Denmark)
Instituto de Tecnologia e Sociedade (NGO, Brazil)
TEDIC (NGO, Paraguay)
Deutsche Vereinigung für Datenschutz e.V. (DVD) (NGO, Germany)
Kenya ICT Action Network (KICTANet) (NGO, Kenya)
ICT Users Association (ASUTIC) (NGO, Senegal)
Superbloom (previously Simply Secure) (NGO, USA/Global)
Usuarios Digitales (NGO, Ecuador)
Ideate Tech Policy Africa & Ochieng Oginga and Company Advocates (NGO, Kenya and Africa)
Nationality For All (NGO, Asia Pacific Region)
Data4Revolution (NGO, Africa)
People's Privacy Network (NGO, USA)
Anglican Church (Faith Based Organization, USA)
Ine van Zeeland (Academic, Belgium)
Douwe Korff (Prof.) (Academic, Europe)
Verónica Arroyo (Expert, Latin America)
Jose M. Arraiza (Expert, Spain)
Markus Sabadello (Expert, Austria)
Jaap van der Straaten, Civil Registration Centre for Development-CRC4D (Expert, the Netherlands)
Javiera Moreno Andrade (Expert, Chile)