// buergerservice.org e.V.

Initiative D21

bitkom

GDV Gesamtverband der Versicherer

EPICENTER.WORKS for digital rights

Die Deutsche Kreditwirtschaft

July 2025

Time Is Running Out: Five Political Imperatives for a Successful eIDAS Ecosystem

The state, civil society, and the private sector approach the introduction of the EUDI Wallet and the development of the eIDAS ecosystem from different perspectives. At the same time, there is broad consensus in many areas that these developments have the potential to fundamentally shape our digital society. The EUDI Wallet, as an interoperable interface, makes an essential contribution to achieving the digital sovereignty objectives of both the EU and the German federal government. For this ecosystem to succeed, it must offer added value to citizens and consumers, public administration, and the private sector alike. This added value derives from the number of available public and private credentials and acceptance points. Therefore, the ecosystem must be trustworthy, widely accepted, and facilitate the easy issuance and use of credentials.

Designing this ecosystem is a societal mandate, and the eIDAS Regulation must be the sole legal foundation for governing digital credentials and identities across Europe. This requires close cooperation between policymakers, the private sector, and society at large. Only through an inclusive, practical approach can the eIDAS ecosystem realize its full potential. Public interest is already there: 55% of citizens would like to use their national ID card via smartphone in the future[1]. The new federal government faces the significant challenge of setting the course for a future-proof implementation over the next 18 months, or by the end of 2026. Key decisions are necessary to position Germany as a strong player in the European identity ecosystem. Achieving this goal requires, alongside political will, clear policy guidelines and tight integration of all relevant stakeholders. Against this background, we present five core demands that are essential for the success of the eIDAS ecosystem.

[1] eGovernment MONITOR 2024

1) Strengthen Digital Literacy

Discussions about digital literacy often focus solely on end users, i.e., citizens. And indeed, these groups must be addressed at their respective levels of knowledge. Digital wallets and credentials, as well as the natural use of the digital ID card (eID) and electronic driving licence, must become an integral part of both digital and analog daily life, and people must be empowered to use them autonomously and securely. But this is impossible without modern legislation and forward-thinking administration. We therefore call for digital competencies, particularly regarding digital identities and trust services, to be developed within ministries, supervisory authorities, and the broader public administration. The goal is to raise awareness of the eIDAS ecosystem and the EUDI Wallet, to clearly communicate their functions, and to promote widespread adoption both within government and among citizens. A cautionary example is the electronic ID card (eID), which by 2024 is used by only 22% of citizens[2]. We need a genuine transformation, from outdated mindsets and analog processes to a digital way of thinking. This also means putting citizens' interests back at the center and recognizing that, according to a 2025 Bitkom survey, 82% of Germans aged 16 and older already use a smartphone[3].

2) Build Trust

Digital identities and credentials must foster trust in the digital sphere rather than reinforce mistrust. Therefore, it is essential that the three main actors – holders, issuers, and relying parties – trust each other. This requires that each party knows the identity of the others; every actor needs a digital identity. The same applies to digital credentials: their authenticity must be ensured. We therefore call for the widespread use of trust services such as electronic seals, electronic signatures, and other eIDAS tools to digitally verify authenticity and reliability. The eIDAS Regulation must be the sole basis for governing digital credentials and identities and serve as the binding reference in all national legal frameworks relating to these issues. The state should focus squarely on the EUDI Wallet, actively integrating existing, proven IT components and legacy solutions to avoid unnecessary duplication and siloed systems, thereby improving the efficiency and acceptance of digital public services.

3) Protect Consumers

Trustworthy data attracts interest. Consumers must therefore be protected from surveillance, misuse, and fraud. Effective safeguards are needed, preferably through technical measures that prevent "over-identification" while also ensuring low-bureaucracy integration into application scenarios. At the same time, consumers must be empowered to decide who receives which credentials from their wallet, and for what purpose. This requires a well-designed consumer protection framework that both protects and empowers consumers to make autonomous decisions. We therefore call for consumer protection to be technically anchored within the wallet, for example, through adequate identification and verification of relying parties, including access rights; the development of a marketing strategy to raise awareness of risks and promote the trustworthy use of the wallet; and rigorous consideration of data protection requirements. A central authority should also ensure that the registration of relying parties complies with eIDAS requirements. When transmitting data to relying parties, the principle of data minimization must be respected. Users should also be able to store a pseudonym in the wallet, which should be the default setting. Sensitive identity data should only be shared with service providers where legally required. We therefore advocate for a clear distinction between use cases based on legal identification requirements and those relying merely on contractual terms and conditions. Optionally, the EUDI Wallet should allow

[2] eGovernment MONITOR 2024

[3] Bitkom 2025, „Mehr als 40 Mrd. Euro Umsatz – Smartphones“ (in German)

users to require their eID card and its function to be physically reactivated (and a PIN re-entered) for (security-)critical operations. This gives users the choice to either trust their smartphone or add an extra layer of security for certain operations by physically re-enabling the eID.

4) Leverage and Streamline Existing Structures

Developing the eIDAS ecosystem requires continuity. Policymakers should build on existing structures such as ministries and SPRIN-D, while future vertical issues must fall under the Federal Ministry for Digitalization and State Modernization (BMDS). We call for a central point of contact to champion the topic within the ministry and educate related departments. As eIDAS rules become increasingly embedded in the German digital landscape, a central authority is needed to organize, monitor, and advance the EUDI ecosystem. Under the BMDS umbrella, topic-specific expert committees should be established to regularly assess which digital credentials are required in different application domains, and to tailor and evolve the eIDAS ecosystem accordingly. Furthermore, all future regulatory legislative projects should be subject to a digital check, to systematically account for and, where possible, actively integrate the potential of the eIDAS ecosystem. For example, use of the EUDI Wallet in payment transactions should only be permitted if it is appropriately considered in sectoral regulation. This regulation must consistently address both technical (security) requirements and liability regimes, ensuring clear separation of responsibilities between wallet providers and (financial) service providers, thereby guaranteeing legal certainty and stability in the financial sector.

5) Promote Use Cases

It has been well known since 2010 that digital identities face a chicken-and-egg problem, and that fostering use cases in public administration and the private sector is crucial to their success. Initially, the EUDI Wallet should focus on its core function consisting of digital identification and authentication, especially for KYC (Know Your Customer) processes. Additionally, the BMDS should focus on a select number of key use cases likely to generate a snowball effect. In particular, we see the following as essential: promoting organizational identities (e.g., the European Business Wallet), issuing digital driving licences, providing digital travel documents, making organ donor cards available as digital credentials, enabling anonymous or pseudonymous age verification, and combining physical and digital university certificates and enrollment proofs. Early and broad involvement and acceptance by relying parties will be critical to success.

Bitkom e. V., Albrechtstr. 10, 10117 Berlin
Tel.: +49 30 / 27576-0, E-Mail: bitkom@bitkom.org

buergerservice.org e. V. (Headquarters: Munich), Executive Office: Berliner Str. 5, 91522 Ansbach
Tel.: +49 171 / 3366669, E-Mail: info@buergerservice.org

Bundesverband deutscher Banken e.V., Burgstr. 28, 10178 Berlin
Tel.: +49 30 1663-0, E-Mail: bankenverband@bdb.de

epicenter.works - Plattform Grundrechtspolitik, Linke Wienzeile 12/19, 1060 Vienna
Tel.: +43 670 404 98 89, E-Mail: team@epicenter.works

GDV e. V., Wilhelmstr. 43 / 43 G, 10117 Berlin
Tel.: +49 30 / 2020-5000, E-Mail: berlin@gdv.de

Initiative D21 e. V., Reinhardtstr. 38, 10117 Berlin
E-Mail: kontakt@initiatived21.de

Lilly Schmidt, Speaker of the WG Digital Identities in Public Administration
NEGZ – Kompetenznetzwerk Digitale Verwaltung – Nationales E-Government
E-Mail: ak-digitale-identitaeten@negz.org