caution: machine translation

// buergerservice.org e.V.

Initiative D21

bitkom

GDV Gesamtverband der Versicherer

EPICENTER.WORKS for digital rights

Die Deutsche Kreditwirtschaft

July 2025

The clock is ticking: Five political decisions for a successful eIDAS ecosystem

The government, civil society and the business community view the introduction of the EUDI wallet and the expansion of the eIDAS ecosystem from different perspectives – at the same time, there is broad understanding in many areas that these developments have the potential to significantly shape our digital society. In addition, as an interoperable interface, the EUDI wallet makes an essential contribution to the implementation of the digital sovereignty goals of the EU and the German government. For this ecosystem to be successful, it must offer added value for citizens/consumers, public administrations and the economy. This added value comes from the number of public and private sector credentials and acceptance points. The ecosystem must therefore be trustworthy, widely accepted and the issuance and use of credentials must be simple.

Shaping the ecosystem is a social responsibility, and the eIDAS Regulation must be the sole basis for regulating digital credentials and identities throughout Europe. This requires close cooperation between politics, business and society – because only through an inclusive, practical approach can the eIDAS ecosystem reach its full potential. There is interest among the population: 55% of citizens would like to use their smartphone to identify themselves with their ID card in the future[1] The new federal government faces the major challenge of setting the course for sustainable implementation in the next 18 months, or by the end of 2026. Key decisions are needed to position Germany as a strong player in the European identity ecosystem.

[1] eGovernment MONITOR 2024

In order to achieve this goal, clear political guidelines and close cooperation between all relevant stakeholders are needed in addition to political will. Against this backdrop, we would like to formulate five key demands that are essential for the success of the eIDAS ecosystem.

1) Increase digital literacy

Digital literacy is often only addressed in relation to end users, i.e. citizens. And indeed, these groups must be taught content at their respective levels of knowledge. Digital wallets with their digital credentials and the widespread use of digital ID cards (eID) and electronic driving licences must become an integral part of everyday digital and analogue life, and people must be empowered to use them independently and securely. But this cannot be achieved without modern legislation and forward-looking administration: we therefore advocate building digital skills, particularly in the area of digital identities and trust services, in ministries, supervisory authorities and administration – in other words, throughout the entire state apparatus. The aim is to significantly raise awareness of the eIDAS ecosystem and the EUDI wallet, to make their functions understandable and to promote their widespread use both within the administration and among citizens. A cautionary example is the introduction of the electronic identity card (eID), which will only be used by 22% of citizens by 2024[2] We need a genuine transformation process – away from traditional ways of thinking and analogue processes and towards a digital mindset. This also means putting the interests of citizens back at the centre and recognising that, according to a Bitkom survey from 2025, 82% of Germans aged 16 and over already use a smartphone[3]

2) Strengthening trust

Digital identities and digital credentials must promote trust in the digital space and not reinforce mistrust. It is therefore essential that the three key players – holders, issuers and relying parties – can trust each other. This requires that everyone knows who everyone else is. Each player therefore needs their own digital identity. The same applies to digital credentials. The authenticity of digital credentials must be ensured. We therefore call for the widespread use of trust services such as electronic seals, electronic signatures and other eIDAS tools to enable digital verification of authenticity and integrity. The eIDAS Regulation must be the sole basis for the regulation of digital credentials and identities and serve as a binding reference in all national legislation relating to these issues. The state should place a clear focus on the EUDI wallet, actively integrating existing, functioning IT components and existing solutions in order to avoid unnecessary duplicate structures and isolated solutions and to increase the efficiency and acceptance of digital administrative applications.

3) Protect consumers

Trustworthy data is highly desirable. Consumers must therefore be protected against surveillance, misuse and fraud. Effective protection is needed, ideally through technical measures that prevent "over-identification" while ensuring low-bureaucracy integration into use cases. At the same time, consumers must be empowered to decide who receives which evidence from the wallet and why. This requires

[2] eGovernment MONITOR 2024

[3] Bitkom 2025, "More than 40 billion euros in sales – smartphones"

A smart consumer protection concept is needed that protects consumers while empowering them to make their own decisions. We therefore call for consumer protection to be technically embedded in the wallet – including through adequate identification and verification of relying parties, including access rights – for a marketing concept to be developed to educate consumers about risks and the trustworthy use of the wallet, and for data protection requirements to be consistently taken into account. A central body should also ensure that the registration of relying parties complies with eIDAS requirements. The principle of data minimisation must be observed when transferring data to relying parties. In addition, users should be able to store a pseudonym in the wallet, which is selected as the default setting. Sensitive ID data should only be shared with service providers on the basis of legal requirements. We therefore advocate a clear distinction between use cases based on a legal identification requirement and those where identification is based solely on the terms and conditions. Optionally, the EUDI wallet should allow users to set their ID card with the eID function to require them to pause and enter a PIN for (security) critical processes. This allows users to decide for themselves whether they trust their smartphone or whether they want to provide additional haptic security for certain processes by pausing the eID.

4) Utilise existing structures and make them more efficient

The development of an eIDAS ecosystem requires continuity. In politics, it is necessary to build on the existing structures consisting of ministries and SPRIN-D, with vertical issues falling under the responsibility of the Federal Ministry for Digitalisation and State Modernisation (BMDS) in future. We call for a central point of contact who will also drive the issue forward within the ministry and inform other departments that are indirectly involved. With regard to the dissemination and increasing introduction of eIDAS rules in the German digital environment, a central body is needed to take responsibility for the organisation, monitoring and further development of the EUDI ecosystem. Under the umbrella of the BMDS, topic-specific expert committees should be set up to regularly evaluate which digital credentials are required by relying parties in different areas of application – with the aim of designing them in line with requirements and efficiently developing the eIDAS ecosystem. In addition, future regulatory legislation should always undergo a digital check with the aim of systematically considering the potential of the eIDAS ecosystem and actively integrating it where possible. For example, the EUDI wallet may only be used for payment transactions if it has been adequately taken into account in sector-specific regulations. This must consistently regulate both the technical (security) requirements and the liability regime, ensuring a clear separation of responsibilities between wallet providers and (financial) service providers in order to guarantee legal certainty and stability in the financial sector.

5) Promote use cases

It has been known since 2010 that digital identities suffer from the chicken-and-egg problem and that promoting use cases in public administration and the private sector is essential for their continued success. However, as a first step, the EUDI wallet should focus on its core function – digital identification and authentication, especially in the context of KYC processes. The BMDS should also concentrate on a few key use cases as an additional service that could trigger a snowball effect. We consider the following areas to be particularly important: the promotion of organisational identities (e.g. European Business Wallet), the issuance of digital driving licences, digital travel documents, the provision of organ donor cards as digital proof, a solution for anonymous or pseudonymous age verification, and the combination of physical and digital university certificates and enrolment certificates.

Early and broad involvement and acceptance by the relying parties is crucial for success.

Bitkom e. V., Albrechtstraße 10, 10117 Berlin
Tel.: 030 / 27576-0, email: bitkom@bitkom.org

buergerservice.org e. V. (registered office: Munich), Executive Office: Berliner Str. 5, 91522 Ansbach
Tel.: 0171 / 3366669, email: info@buergerservice.org

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

epicenter.works - Platform for Fundamental Rights Policy, Linke Wienzeile 12/19,
1060 Vienna Tel.: +43 670 404 98 89, email: team@epicenter.works

GDV e. V., Wilhelmstraße 43 / 43 G, 10117 Berlin
Tel.: 030 / 2020-5000, Email: berlin@gdv.de

Initiative D21 e. V., Reinhardtstraße 38, 10117 Berlin
Email: kontakt@initiatived21.de

Lilly Schmidt, spokesperson for the Working Group on Digital Identities in Administrative Digitisation NEGZ – Competence Network for Digital Administration – National E-Government
Email: ak-digitale-identitaeten@negz.org