Position Paper

May 2026

Bitkom Consolidated Position on the European Business Wallet

Summary

Bitkom supports the European Business Wallet in principle as an important element of a European trust infrastructure for digital business and administrative processes. However, against the backdrop of the current negotiations on the proposed regulation and the recently discussed amendments, Bitkom sees a need for targeted improvements: Clear and swiftly adopted implementing acts are required, along with ambitious yet realistic implementation deadlines, binding acceptance obligations for the public sector, a strong principle of equivalence for digital and analog procedures, and practical requirements for security, compliance, and liability. It is crucial to design the EBW in such a way that a functioning, interoperable, and widely usable ecosystem can emerge.

Specific Comments

1. Is the European Business Wallet (EBW) suitable for meeting the needs of the business community? And are the relevant guidelines from the European Commission appropriately designed for this purpose?

The European Business Wallet (EBW) has the potential to meet the needs of the business community, as it is designed by the European Commission as a universally applicable infrastructure for digital business and administrative processes.

The intended use cases span the entire B2G and B2B context as well as cross-context scenarios, thereby addressing key business needs—from regulatory filings, procurement, and tax procedures to KYC/KYB processes, invoicing, and payment transactions, all the way to identification, power of attorney, the exchange of regulatory evidence, sustainability reporting, and digital product passports. Through the secure, verifiable, and cross-border digital provision of organizational identities, evidence, and authorizations, the EBW can reduce existing media discontinuities, lower transaction costs, and strengthen trust in digital business relationships.

The «wallet-by-default» principle underscores the goal of establishing the EBW as the fundamental standard for digital interactions between economic actors and public authorities, as well as among economic actors themselves, thereby enabling the scaling of efficient, legally binding, and automatable processes within the European Single Market. Against this backdrop, it is essential to make a future EBW available to all economic actors, thereby supporting the broadest possible adoption within the economy.

Furthermore, the effectiveness of the EBW depends on the quality, completeness, and digital accessibility of national registers (authentic sources). We recommend explicitly establishing the Once-Only Technical System (OOTS) as the primary infrastructure layer for cross-border retrieval and verification of data from authentic sources. However, it must be ensured that the responsibilities of the respective competent authorities are preserved. Access to registry data must not result in qualified trust service providers being able to issue attribute certificates independently, insofar as this falls under the authority of a government agency. Rather, issuance by private service providers should remain possible, provided it is carried out on behalf of, under the responsibility of, or in accordance with the instructions of the competent authority.

An important prerequisite for this is that the EBW be fully embedded within the existing eIDAS framework. Identification, authentication, and identity data must be based on eIDAS-compliant mechanisms. This ensures interoperability and strengthens trust across Member States.

Furthermore, the EBW should enable identity and authorization solutions for industrial objects, smart products, and digital and AI-supported agents, so that automated transactions based on verifiable evidence can be conducted securely, interoperably, and auditable.

Ultimately, for broad and seamless acceptance and use of the EBW, a targeted adjustment of the legal framework is needed to remove bureaucratic hurdles and enable efficient implementation. In doing so, the legal framework should incorporate existing trust infrastructures and support market-driven scaling. This applies in particular to national digital identity law: The EBDIG should be designed to be flexible and modular so that the European Business Wallet can be integrated into the national legal framework without further fundamental adjustments once the relevant EU regulation enters into force.

2. Is there a need for such a tool, and how strong is the competition from existing solutions?

There is an urgent need for government-regulated organizational identities as well as an associated wallet solution. The exchange of data will increase significantly in the future, so that the previous analog interactions between economic actors will be largely replaced by digital business processes. The business world is thus undergoing a transformation in which digital interactions and transactions are becoming the new norm.

Against this backdrop, it is essential to view the EBW as a central component for building a Europe-wide (and eventually global) trust infrastructure. It enables the secure and trustworthy execution of business processes and transactions in the digital space and helps harmonize differing national requirements. Furthermore, implementing a high degree of automation within the EBW could significantly reduce transaction costs for economic actors. This not only creates efficiency gains but also strengthens the trust of all stakeholders in the digital economic environment. It also forms the basis for authorizing not only individuals but also machines to perform actions.

Existing solutions such as «Mein Unternehmenskonto» demonstrate that Germany has already established a conceptually sound foundation for digital corporate identity that competes with the European Business Wallet. However, «Mein Unternehmenskonto» is limited to the B2G sector and cannot be used for B2B use cases. Furthermore, there are no plans to integrate this user account into the existing IT systems of economic actors, which limits the use and automation of business processes and thus significantly impairs user-friendliness.

The management of representation rights is fragmented in the current system, as they must be maintained individually both in the OZG-PLUS mailbox (Module 5) and in the authorization control (Module 6). This results in a non-uniform user experience, which impairs efficiency and clarity. For this reason, it makes sense to either further develop «Mein Unternehmenskonto» into the European Business Wallet for public administration or to replace it entirely with this solution to create a consistent and integrated solution.

In addition, the Qualified Electronic Registered Delivery Service (QERDS) offers the possibility of consolidating the multitude of communication and mailbox solutions in public administration or achieving compatibility between the various systems, thereby enabling a more efficient and seamless exchange between the parties involved (see the ZAPuK project: Target Architecture for Mailbox and Communication Solutions).

Thanks to its interoperability and the European legal framework, the EBW provides the foundation for resolving these issues and addressing these requirements in a systematic manner. Where possible, it should build on existing national infrastructures to minimize migration efforts and leverage existing user trust. Competition between existing and new solutions is expressly encouraged in this context, as it promotes innovation, quality, and market penetration.

3. What risks do you see for the success of the EBW?

The success of the European Business Wallet (EBW) faces significant challenges, which can be divided into four key risk areas:

a) Willingness to invest and government prioritization

For larger economic actors, investment decisions are typically made at the C-level. However, senior management often expresses uncertainty when the return on investment (ROI) or the concrete benefits of a new solution like the EBW are not clearly apparent. Government projects are viewed with skepticism due to past experiences, such as with the national ID card. To alleviate these uncertainties for decision-makers, it is necessary for the legislature to give the EBW clear priority and to make a clear commitment to this project. Such signals from the public sector are of great importance, as they build trust and increase the willingness to invest. Currently, no such signals are evident. Instead, there are considerations to reduce the obligations of public authorities under Article 16 of the EBW Regulation or to restrict the principle of equivalence under Article 4(1) of the EBW Regulation.

b) Strategic Roadmap

A key aspect is the creation of a roadmap that transparently outlines the development path of the EBW. This includes the planned integration into existing business and administrative processes as well as a concrete plan for adapting relevant legal frameworks. The EBW must be perceived by companies as a genuine simplification and as an indispensable tool («must-have»). Only under these conditions will the necessary investment decisions be made.

c) Economic Incentives

Targeted support measures, such as the reduction of administrative costs, can also create further incentives for economic actors. Without suitable incentive mechanisms, there is a risk that necessary investments in development, operation, and scaling will not materialize. Therefore, framework conditions should be created that enable viable business models for the private sector as well, for example through clear monetization prospects or targeted support and compensation mechanisms. Only in this way can a sustainable and innovation-driven wallet ecosystem emerge.

d) Unclear allocation of liability

An additional risk lies in the unclear allocation of liability among EBW providers, operators of authentic sources, certificate issuers, and public authorities. Without a clear demarcation, there is a risk of simultaneous and potentially conflicting liability risks under the EBW Regulation, NIS2 (Directive (EU) 2022/2555), the GDPR, and eIDAS. The delegation of sanctioning provisions to Member States (Article 13) also carries the risk of divergent enforcement regimes.

e) Impact Assessment and National Implementation Architecture

Another problematic aspect is that the practical implementation requirements for the EBW have not yet been sufficiently specified. The Commission did not conduct a separate regulatory impact assessment, but instead relied on a staff working document, SWD(2025) 837, which includes an estimate of potential costs and benefits. This means that the overall cost burden for providers and SMEs, the readiness of national registers, and the interactions with the EUDI-Wallet, the SDG/OOTS, NOOTS, national registers and sector specific legislation have not been systematically assessed. These interactions should therefore be further specified, in particular with regard to the EUDI-Wallet, the SDG/OOTS, NOOTS, national registers and sector specific legislation. At national level, a concept for a coherent overall architecture should therefore be developed at an early stage. This concept should address the integration of registers, public authorities and relevant wallet infrastructures into the Germany Stack (Deutschland-Stack). The role of the QERD service should also be taken into account, as it may become highly relevant for secure and legally binding communication processes within the EBW ecosystem.

f) High security without disproportionate barriers to market access

The EBW will serve as the central technical authority for the entire ecosystem. This role must be taken into account by applying the highest standards when it comes to security. Potential attacks on this technical authority must be prevented, as they would immediately undermine trust in the ecosystem. At the same time, particular attention must be paid to ensure that security and certification requirements remain proportionate and practicable. Excessive or overly complex requirements could lead to smaller and innovative providers in particular being excluded from the market, slowing the overall development of the ecosystem. Such excessive technical requirements risk effectively acting as barriers to market entry. In parallel, regulatory requirements should focus on effective oversight, operational manageability, and EU-wide enforcement, rather than being applied across the board to ownership structures, in order to avoid unnecessary overregulation.

A balanced relationship between security, user-friendliness, and economic feasibility is therefore essential. Otherwise, there is a risk that innovation potential will be stifled and the development of a competitive, diverse wallet ecosystem in Europe will be limited. The goal should be to combine high security standards with practical requirements that enable broad market participation and continuous innovation.

g) Market Awareness and Promotion of Adoption

The current low market awareness and lack of awareness pose a significant hurdle to the success of the EBW. Many companies are not yet aware of the existing opportunities and initiatives in the field of digital identities; both the EUDI-Wallet and the European Business Wallet are currently known only on a limited user base. Without targeted measures to increase visibility, understanding, and trust, there is a risk that usage will fall short of expectations. Active promotion of adoption – for example, through information campaigns, concrete use cases, and integration into existing business processes—is therefore essential.

h) Restriction of Issuance Functionality for EBW Owners (Art. 5 EBW Regulation)

A critical point is that, following the current amendments to Art. 5(1)(f) of the EBW Regulation, EBW owners would no longer be able to issue electronic attribute certificates independently but would instead be reliant on the EBW provider for this purpose. At the same time, the independent «issue» functionality in Art. 5(1)(a) is no longer designated as a core functionality. This would restrict the central function of the EBW and create an additional dependency on intermediaries.

This jeopardizes acceptance in the business community, particularly about data sovereignty, the confidentiality of business relationships, and scalability. Wallet providers could use metadata to draw conclusions about sensitive customer and supplier relationships. Furthermore, fast, automated, and mass-market applications—such as in KYS and KYC processes or in product-related wallet implementations—could be made significantly more difficult.

The EBW should therefore be designed in such a way that EBW owners can issue electronic attribute certificates independently and without unnecessary reliance on intermediaries.

4. Are the security requirements imposed on EBW providers and the EBW itself sufficient, and is the authorization procedure suitable for ensuring compliance?

The security requirements for the EBW and its providers are fundamentally sufficient, provided they are risk-based and built upon the already very robust eIDAS and NIS2 regulatory frameworks.

At the same time, businesses have a lower need for protection than natural people, so a less stringent yet still secure framework is appropriate. Furthermore, both providers and users have a strong vested interest in secure solutions, as the wallets support business-critical processes and trust is an immediate market requirement.

The proposed notification procedure is considered a suitable authorization procedure to ensure compliance, provided it is based on an established approach and can offer legal certainty through clear, uniform, and objective criteria.

The conformity assessment procedures should be published simultaneously with the implementing acts. The assessment methodology should be risk-based and

proportionate. Conformity assessments should be subject to mutual recognition among Member States to avoid duplicate national testing requirements. QTSPs that are already subject to conformity assessment under eIDAS should benefit from a simplified EBW conformity procedure.

Ultimately, it is crucial that the provision of the wallet be market-driven and that additional regulatory requirements do not create unnecessary barriers that hinder the development of a dynamic market.

5. Do you consider a mandatory acceptance requirement for the business sector to be sensible? For which sectors?

A general mandatory acceptance requirement for the business sector is not considered necessary. Rather, a high adoption rate depends on appropriate legal frameworks and the creation of relevant use cases that facilitate usage and reduce bureaucratic hurdles, rather than imposing additional regulatory obligations on economic operators. Mandatory use of the EBW, on the other hand, would undermine existing, efficient processes and could create disproportionate bureaucratic hurdles for economic operators.

Adoption should stem from the tangible added value of the EBW, particularly through user-friendly applications and high-quality use cases, as well as from a sustainable and balanced cost model. Incentives are particularly useful in areas where standardized digital credentials lead to significant efficiency gains, such as in regulated B2B processes, KYC and onboarding procedures, and in cross-border verification and procurement processes.

Furthermore, it is crucial that government agencies allocate targeted budgets for piloting, building a functioning ecosystem, and for accompanying marketing and awareness-raising measures. Experience with the European Digital Identity Wallet shows that cooperative approaches in the form of EU-funded consortia—such as those within initiatives like WeBuild or Aptitude—contribute significantly to successful development and testing. Comparable programs should therefore also be established for the European Business Wallet at the European and national levels. Such initiatives make it possible to work with the business community, and technology providers to develop practical solutions, define standards, and ensure that these are both regulatory-compliant and operationally feasible. Only through an actively supported, collaborative ecosystem can broad and sustainable acceptance be achieved.

In certain cases, however, we see that companies can contractually agree to use the EBW in their bilateral business relationships—a sensible, market-oriented mechanism that enables gradual and needs-based adoption. Furthermore, it remains possible for national or European legislators to mandate use in specific areas, such as in the draft EU Inc. Regulation. This combination of voluntary use, contractual agreements, and targeted legally mandated areas represents, in our view, a balanced and proportionate approach that both fosters innovation and provides legal certainty. If the legislator deems an acceptance obligation for economic operators necessary, it should regulate this obligation in accordance with Article 5f(2) and (3) of the eIDAS Regulation.

We recommend evaluating the EBW Regulation in this regard five years after the introduction of the EBW.

6. How do you assess the acceptance obligations of the public sector?

The acceptance obligation for public authorities (Art. 16 EBW Regulation) is crucial to the success of the EBW. Only with public authorities serving as early adopters can the EBW provide real benefits to businesses, given that businesses have approximately 200 administrative interactions per year. Voluntary use by public bodies or incomplete coverage of the public sector would lead to inconsistent offerings and thus significantly reduce the attractiveness and adoption of the EBW. Without mandatory involvement of the administration, the EBW lacks the necessary market pressure and reach. Previous experiences—such as with the new ID cards show that voluntary approaches often fail due to low integration and a lack of opportunities for use. The idea of exempting municipalities with fewer than 10,000 residents from the obligations under Article 16 of the EBW Regulation should not be pursued further. Such an implementation would result in a significant portion of the public administration not being obligated to support the EBW. In Germany, around 80% of municipalities have fewer than 10,000 residents. The importance of the municipal level must be particularly emphasized: 75% of all interactions with the administration take place at this level.

In Germany, support from central bodies such as the IT Planning Council can significantly promote the integration of the wallet.

7. Do you consider it necessary for public agencies to have their own EBW?

In our view, it makes sense for public agencies to have their own EBW to enable digital, interoperable, and seamless processes. Their need for efficient digital workflows largely aligns with that of the private sector. Without their own EBW, the implementation of core functions would be limited. What might at first glance appear to be a relief for public agencies would quickly prove to be an inadequate stopgap solution that would later require significant effort to correct. Therefore, the administration should be fully integrated from the outset to ensure a functional and future-proof system.

In accordance with the concept of self-sovereign identities and the principle of the trust triangle, it is necessary for the trusting party (verifier) to also clearly authenticate themselves when querying identity data or other verified credentials. Otherwise, the holder cannot independently decide whether and to whom they are currently making the data available. This requirement must also be ensured during data retrieval by an EBW (EBW-to-EBW communication).

Furthermore, legal entities under public law also participate in the digital economy. To do so, they may need to identify and authenticate themselves to economic actors. In order to «identify» themselves to economic actors, legal entities require their own

identification record. Legal entities also act through various authorized representatives. In the case of municipalities, for example, this is the mayor. This body may, in turn, delegate the power of representation to municipal employees under certain circumstances.

8. How do you assess the transition periods, particularly in light of the extensive acceptance requirements?

The benefits of the EBW will only be fully realized if it is rolled out quickly and widely in the market. Against this backdrop, the transition periods provided for in the draft regulation appear insufficiently ambitious. Shorter deadlines would not only reduce regulatory and technical uncertainties (for example, in conjunction with the EUDI-Wallet, see Art. 20 of the EBW Regulation) but also strengthen the willingness of market actors to invest early on. Furthermore, it should be noted that, pursuant to Article 5a (1) of the eIDAS Regulation, an EUDI-Wallet must be made available to legal entities by December 24, 2026, at the latest. Against this legal backdrop, Member States have already had to carry out extensive preparatory work, which can now be incorporated into the development and implementation of the European Business Wallet.

Specifically, we advocate shortening the general acceptance period to 18 months and the QERDS transition period to 24 months following the entry into force of the relevant implementing acts. All implementation deadlines should be linked to the entry into force of the implementing acts (Art. 5(5), Art. 9(4), Art. 10(6), and Art. 18 of the EBW Regulation) rather than to the entry into force of the Regulation itself, in order to provide clarity and avoid uncertainties regarding technical implementation. Specifically, we advocate for a mandatory six-month deadline for the adoption of all essential implementing acts.

However, the transition periods should be realistic and tailored to specific cases so that companies and authorities have sufficient time to make necessary adjustments and existing infrastructure can be meaningfully integrated.

9. Based on the Commission's proposal: What key changes would you like to see?

a) Definition of the economic operator pursuant to Art. 3(4) of the EBW Regulation

The prerequisite is that all economically active people regardless of whether they are natural or legal people receive an identification record and thus have access to the European Business Wallet. It is also necessary for economically active natural people to receive a separate identification record for each economic activity they perform. For example, a tax advisor who also practices as a lawyer and manages multiple law firms can be registered separately for each activity. In addition, legal entities that are not economically active, such as non-profit associations (e. V.), should also be able to use a European Business Wallet. Otherwise, they would be unable to use either the EUDI-

Wallet (natural people only) or the European Business Wallet (economically active people only).

b) Functional scope and technical requirements of the European Business Wallet (Art. 5 and Art. 6 of the EBW Regulation)

The European Business Wallet must be capable of meeting all the requirements of economic operators and public authorities. This includes the minimum set of functions for the European Business Wallet as specified in the EBW Regulation (Art. 5 EBW Regulation). It should be noted that the holder of a European Business Wallet typically acts through authorized representatives. In this context, it is crucial that the EBW provides clear and always traceable information regarding legal representation: which natural person is acting, on behalf of which legal entity, based on which mandate, and with what scope and duration of validity (structured, interoperable, and verifiable management of roles, mandates, and authorizations). These may include both internal company members (such as employees) and external parties (for example, tax advisors). This functionality is of crucial importance for economic use. It should be noted that different wallet categories are used by different groups of people. An employee could use their personal EUDI-Wallet for professional purposes, while alternatively they could also use an instance of the European Business Wallet on their business smartphone, provided they do not wish to use their private wallet for work-related activities. These cases must be taken into account accordingly. Furthermore, it is conceivable in the future that, in addition to natural people, machines or AI- agents will also be empowered to perform legal acts. This application scenario must also be taken into account in the regulatory requirements.

c) Principle of Equivalence (Art. 4 EBW Regulation)

The European Business Wallet will only be accepted and used by the business community if it can also be used to carry out legal transactions or administrative procedures that require specific formalities. It is therefore essential that users be assured of legal certainty that all actions performed via the European Business Wallet possess full legal validity. The basis for this should be the trust anchors already established in the eIDAS Regulation, in particular qualified trust services that already enable cross-border actions with full legal validity today. Economic operators in the European Single Market should not have to verify whether the use of the European Business Wallet is possible in a specific Member State. This verification burden must be eliminated by economic operators. Furthermore, the requirements for the digital procedure using the EBW must not be increased compared to the analog procedure. Current considerations by the European Union's legislative bodies provide that the principle of equivalence should apply only when qualified trust services are used. This could potentially prevent the use of non-qualified electronic attribute certificates from no longer being sufficient, even though in the analog procedure the submission of a printed copy would meet the requirements. The principle of equivalence must therefore ensure equivalence both in terms of the factual requirements (no higher or lower requirements, particularly regarding evidence) and in terms of legal consequences (identical legal effect). This would also support the considerations of the Federal Ministry for Digital Affairs and State Modernization: For according to Section 16(2) of the EBDIG-RefE, all forms of

electronic attribute certificates (unqualified, qualified within the meaning of Article 3(45) of the eIDAS Regulation, and administrative within the meaning of Article 3(46) of the eIDAS Regulation) should be able to replace a legally required written form within the scope of the application of federal law. The Federal Ministry has thereby made it clear that an exclusion of non-qualified electronic attribute certificates is not desired. Such an exclusion should therefore not be required at the European level either.

d) Obligations for Public Authorities (Art. 16 EBW Regulation)

The new ID card illustrates that well-intentioned concepts often fail to achieve the desired effect without binding requirements. The requirements for public authorities take this insight into account. It is therefore necessary for economic operators to be able to reach all public authorities via the European Business Wallet and to carry out all necessary measures through it.

e) Minimum requirements for the digital maturity of authentic sources (national registers) and explicit anchoring of OOTS integration

f) Clear, harmonized allocation of liability among EBW providers, operators of authentic sources, and certificate issuers; limitation of provider liability to matters within operational control

g) Risk-based, proportionate, and mutually recognized conformity assessment procedure; simplified procedure for QTSPs

h) Replacement of «control» with «operational control» in Article 7(2) of the EBW Regulation regarding provider eligibility

10. Do you think that every company should automatically receive a European Unique Identifier (EUID)?

The European legislative bodies' current deliberations on the EBW Regulation partially provide that a uniform identifier shall be assigned exclusively upon application by the economic operator. This means that the identifier is not automatically assigned to the economic operator in the register, but only after a corresponding application has been submitted. This process creates additional administrative burdens in the Member States and can lead to significant delays in the timely issuance of identification data. It is therefore recommended that the application requirement be reviewed and that the assignment of an identifier be provided as a standard practice and free of charge. The European Union and the Member States are encouraged to gain an overview of the various identification numbers and to examine possibilities for consolidating or federating existing national identification numbers. The assignment should take place within six months of the Regulation's entry into force for all existing companies and be linked to existing national registry identifiers.

However, this is contingent upon the assignment being seamlessly integrated into existing registration and incorporation processes and implemented uniformly across the

EU. This will ensure that the identifiers are immediately usable and realize their full value, particularly in cross-border contexts.

It should also be taken into account that the EUID—for example, in Germany—can change due to a relocation of the company's registered office and judicial district and thus does not constitute a permanent identifier. This issue should also be addressed to ensure that every economic operator, including self-employed individuals and other entities not subject to registration, can be assigned a permanently unique identifier. In addition, complex corporate structures (subsidiaries, branches) should be taken into account.

11. The proposal excludes providers that are under any form of control by companies from third countries. However, many EU companies have shareholders from third countries and would thus be excluded as providers. Do you see this as a problem?

The goal of digital sovereignty is of fundamental importance to the success of the EBW. For us, digital sovereignty means that we, as Europe, remain capable of acting, possess our own cutting-edge technological capabilities, and can decide for ourselves which trustworthy partners we work with.

Given the geopolitical situation and the sensitivity of business-critical identity data, it is essential to protect the trust infrastructure from undue influence by third countries. Nevertheless, careful consideration should be given to whether a blanket exclusion based on ownership structures is the appropriate measure. An overly restrictive approach carries the risk of unnecessarily limiting the market in this capital-intensive sector, deterring investment, and jeopardizing the ecosystem's scalability.

We therefore recommend a differentiated approach that combines security and competitiveness:

- From ownership to operational control: Instead of a blanket rejection of providers with third-country shareholders, the focus should be on operational control. We support the proposal to define «control» as the ability to exert decisive influence over key management or operational decisions. Mere minority stakes or foreign investments should not in themselves be grounds for exclusion, provided that European governance is maintained.
- Risk-based security approach: Digital sovereignty is most effectively ensured through strict, verifiable requirements for security, data protection, and interoperability. Compliance with European standards and the auditability of systems are crucial—regardless of where shareholders are headquartered.
- Autonomy through excellence: True digital sovereignty does not arise from market isolation, but from the ability to choose between high-performing alternatives from a position of strength. Criteria-based market access promotes innovation and ensures that the EBW operates at a world-leading level.

Overall, we advocate for a model that protects strategic security interests without blocking economic dynamism and the necessary integration of global capital flows. Only in this way can we create an infrastructure that is both secure and internationally competitive.

12. Do you believe that all Business Wallet data should be stored on infrastructure located within the EU?

The European Business Wallet serves as a central trust infrastructure and processes sensitive business-related data. Accordingly, the security, control, access protection, and resilience of the underlying infrastructure must meet the highest standards. From a sovereignty perspective, it is crucial that the services used reliably meet the specific protection needs of the respective use cases, particularly with regard to control, access, security, and supply chain resilience. A risk-based assessment should ensure that high security requirements, as well as flexibility and technological openness, are given equal consideration. At the same time, the legal framework should be designed in such a way that scalability and fair competition are maintained. Requirements for infrastructure, hosting, and cloud services should therefore be clear, proportionate, and verifiable, without indiscriminately excluding providers or unnecessarily hindering the emergence of a high-performing and diverse EBW ecosystem. The focus should be on common security standards, interoperability, auditability, and effective control mechanisms.

13. Do you see any potential overlaps that need to be addressed, for example with the digital product passport?

The «principle of the default use of European Business Wallets» («Business Wallet by Default») (see Recital 57) also implies that all existing regulations regarding the integration of the European Business Wallet and the EUDI-Wallet should be reviewed. This applies, for example, to the amended Company Law Directive, which currently only provides for compatibility with the EUDI-Wallet for the EU Company Certificate and the digital EU power of attorney and must be adapted accordingly. European and national legislators are therefore called upon to align the entire legal framework with wallet solutions and to create practical, seamless use cases. The digital product passport, such as the digital battery passport pursuant to Art. 77 et seq. of the EU Battery Regulation, is merely one example of an application in this context. As DPPs become mandatory for an increasing number of product categories, economic operators must be able to manage sustainability and compliance data via the wallet. To this end, it is recommended that a new Recital 21a be inserted to ensure EBW-DPP interoperability based on common interfaces and standardized technical protocols. Without this interoperability, there is a risk of parallel digital structures and increased administrative burdens. Furthermore, the EBW should be designed to be compatible with the EU-Inc. framework from the outset.

14. Do you think there should be a deadline for the Commission to present the technical standards, and would you support linking the implementation of the Regulation to the publication of the implementing acts?

A fixed deadline for implementing acts is essential, particularly to provide public authorities with the necessary planning certainty for detailed planning. We therefore propose a binding deadline of six months after the regulation enters into force, as the significant delays with eIDAS 2.0 have highlighted the need for clear timelines.

At the same time, it must be taken into account that rigid deadlines alone carry the risk of raising false expectations in the event of non-compliance. The deadlines must therefore also be strictly adhered to by the European Commission. A compromise could be to link the start of the implementation period strictly to the actual entry into force of the implementing acts. This is the only way to ensure that delays in the legislative process do not hinder technical implementation and that stakeholders are afforded the full preparation time.

15. How do you assess the ITRE rapporteur's proposal to repeal the privilege currently provided for qualified trust service providers in Article 11(3) of the EBW Regulation, under which they have so far been exempt from a review and verification procedure?

The removal of the privilege for qualified trust service providers (QTSPs) is viewed critically. QTSPs are already subject to strict conformity assessments under Regulation (EU) No. 910/2014 (eIDAS). An additional review and verification requirement would create an unnecessary double burden without increasing security.

Bitkom represents more than 2,300 member companies from the digital economy. In Germany, they generate over 200 billion euros in revenue with digital technologies and solutions and employ more than 2 million people. Its members include more than 1,000 small and medium-sized enterprises, over 500 startups, and virtually all global players. They offer software, IT services, telecommunications or internet services, manufacture devices and components, operate in the digital media sector, create content, provide platforms, or are otherwise part of the digital economy. 82 percent of the companies involved in Bitkom have their headquarters in Germany, another 8 percent come from the rest of Europe, and 7 percent from the U.S. 3 percent are from other regions of the world. Bitkom promotes and drives the digital transformation of the German economy and advocates for broad societal participation in digital developments. The goal is to make Germany a high-performing and sovereign digital hub.

Publisher

Bitkom e.V.
Albrechtstr. 10 | 10117 Berlin

Contact

Lorène Slous | Specialist for Trust Services & Digital Identities
T 030 27576-157 | l.slous@bitkom.org

Responsible Bitkom Committee

Working Group on the Application of Electronic Trust Services
Working Group on Digital Identities