bitkom

Position Paper

June 2025

Bitkom on the European Business Wallet

Summary

The European Commission has launched a consultation on the European Business Wallet (EUBW) to gather concrete insights into the challenges businesses may face around identification, authentication, and data exchange – particularly in the context of digital transactions, regulatory compliance, and cross-border operations. In this position paper, Bitkom highlights the key challenges organizations face in B2B and B2G contexts – and to some extent in B2C, B2M and B2E – and outlines essential use cases alongside technical and legal requirements to be integrated into the forthcoming EU legislation on the EUBW.

The term EUDI-Wallet initially covers digital identity wallets for both natural and legal persons under the revised eIDAS Regulation. Recently, the term European Business Wallet (EUBW) was introduced specifically for legal entities. In this document, we use EUDI-Wallet to refer exclusively to wallets for natural persons (citizens), and EUBW for wallets related to legal persons and organisational contexts including identities for employees and machines.

If designed effectively, the EUBW could serve as a foundational tool for secure, seamless, and cross-border data exchange between businesses and public authorities by simplifying administrative workflows, reducing redundant data submissions, enhancing data quality, and improving compliance across both regulatory and commercial contexts. In a broad B2B context, the EUBW could support a variety of use cases, such as including Know-Your-Customer (KYC) and Know-Your-Business (KYB) procedures, the execution of digital contracts, supply chain documentation, and digital product passports. By linking verifiable credentials to legal entities and their representatives, it could help automate complex workflows, strengthen trust, and enable secure, cross-border data sharing.

However, the success of the EUBW would depend on its integration with a broader modernization of administrative and legal frameworks. Existing legislation would need to be reviewed for digital compatibility, and procedural requirements harmonized across sectors and Member States. The EUBW should not be focused on government-

to-government or purely administrative processes, as the Single Digital Gateway Regulation already offers some suitable mechanisms for such interactions. Instead, the wallet should focus on supporting economic actors, particularly in the private sector. Ultimately, it could serve as a foundation to rethink and enhance digital processes across both public administrations and businesses.

Current technical and structural barriers affecting public and private organizations

A major obstacle to digital transformation across public administrations and private organizations lies in the absence of seamless and interoperable mechanisms for identifying and exchanging verifiable, auditable and non-repudiable company-related data. Legal, procedural, and technical discrepancies across Member States and organization types contribute to the fragmentation of document requirements and attribute structures. As a result, businesses and administrations are forced to engage in time-consuming, manual upload and review processes that rely heavily on paper-based or non-standardized formats. These inefficiencies place a significant administrative burden on both B2G and B2B interactions and hamper the emergence of harmonized, user-friendly digital services across the EU.

Technical barriers

We observe that current digital workflows are often interrupted by media discontinuities. Many administrative processes continue to depend on scanned documents or file formats that are not machine-readable, such as JPEG images or metadata-free PDFs. These formats not only break the continuity of digital exchanges but also require additional parallel handling steps that reduce process efficiency and legal reliability.

Moreover, back-end systems across the EU remain fragmented and heterogeneous. Most are not capable of automatically processing or validating digitally verifiable proofs. For example, registry data or UBO (Ultimate Beneficial Owner) information often cannot be retrieved or validated automatically and instead rely on manual procedures that are error-prone and time-intensive.

At a more structural level, there is currently no comprehensive technical framework that supports complex organizational use cases. The existing EUDI-Wallet architecture primarily focuses on natural persons and smartphone-based solutions and lacks native support for scenarios such as digital product passports, documentation of physical or technical assets, or Europass-based qualifications in the context of corporate processes.

The lack of interoperability between national infrastructures further exacerbates the issue. At present, there is no EU-wide mechanism to verify and trust digital proofs across borders. Formats for KYC/KYB verification are neither standardized nor supported by trusted validation mechanisms. The absence of harmonized attribute sets and digital identity schemes across Member States – and beyond the European

Economic Area – severely limits the usability and scalability of potential solutions like the EUBW.

Legal and structural barriers

From a legal perspective, the identification requirements imposed on companies and their representatives used to be highly fragmented across Member States. Rules and expectations used to vary widely regarding which documents are accepted, which data points must be provided (such as nationality, place of residence, or date of birth), and how representation rights and beneficial ownership must be demonstrated. While significant progress has been made in addressing the initial lack of harmonization, further efforts are still needed as remaining inconsistencies continue to undermine legal certainty, slows down data exchange, and contradicts the goals of the eIDAS Regulation and the ambition of a truly digital single market.

One of the structural challenges was the establishment of a consistent and interoperable legal entity identifier at the EU level. While the revised eIDAS Regulation mandates a EUDI-Wallet for legal persons, many critical implementation details – particularly those concerning the Legal Person Identification Data (LPID) – remain undefined. This situation is particularly problematic in some European countries like Germany, where there is no unified registry covering all types of organizations, including public authorities and certain categories of professionals. Without such a unified infrastructure, the definition, issuance, and management of a consistent LPID become exceedingly difficult, hindering the seamless use of verifiable credentials across different types of legal entities. We advocate for the definition and adoption of a harmonized LPID that is interoperable across the EU. We particularly note that a gap remains for legal entities that are not currently covered by national company registers. This includes, depending on the EU membership country, a range of organizations such as public entities (e.g., universities), governmental authorities, churches, and other institutional actors that play critical roles in cross-border service provision and funding programs. These entities often lack a unified and verifiable registration basis, particularly in Member States without a comprehensive register. We see the LPID issuance process as a strategic opportunity to close this registration gap. Issuing LPIDs for legal entities not currently registered, based on a harmonized set of minimum criteria, could effectively address this issue. Moreover, closing this registration gap will significantly enhance other legal and administrative processes beyond just LPID issuance.

Finally, it remains unclear how the EUBW will relate to existing frameworks such as eIDAS Regulation and the Single Digital Gateway Regulation.

We therefore call on the European Commission to address these foundational issues as a matter of priority. The success of the EUBW depends on resolving both the technical interoperability barriers and the underlying legal fragmentation that currently constrain cross-border digital transactions.

Use cases and key requirements for the European Business Wallet

Use Cases

We call for the EUBW to be purposefully designed to address critical challenges in both B2G and B2B interactions. To achieve meaningful impact, the EUBW must enable the exchange of machine-readable, verifiable, and identity-bound credentials that support automated, cross-border, and seamless processes. The following use cases are provided as recommendations and do not constitute an exhaustive list.

In public sector contexts, the EUBW must help to simplify administrative processes such as registering, permits, and licensing workflows by enabling once-only data submission and allowing verified information to be reused across different authorities. This would significantly reduce the administrative burden on companies, improve data quality, and ease compliance with regulatory requirements.

For the private sector, the wallet should support a broad range of practical use cases. It ought to facilitate critical procedures like KYC and KYB in finance, including when verifying beneficial ownership, which remains a complex and costly process today. The EUBW should also support the documentation needs arising from digital product passports and supply chain compliance under emerging European regulations. Additionally, it should enable efficient master data management, facilitate data sharing under the Data Act, and be applicable in sectors such as healthcare, HR, and technical asset management. More broadly, it must allow for legally binding digital contracts, secure authorization credentials, and clear digital representation of both persons and objects within companies.

Key requirements

Technical requirements

To realize this vision, we demand that the EUBW be built on a robust technical framework that is cloud-native and API-first, ensuring compatibility with existing ERP and legacy systems. Data should be hosted on a sovereign EU-based cloud infrastructure, which must coexist with a secure mobile solution. Machine-to-machine communication should also be an integral part of the EUBW architecture, although access to such interfaces should be tailored to the specific use cases. The EUBW should support server-to-server communication to integrate smoothly with the heterogeneous IT landscapes (ERP, KYC systems, etc.) of both public administrations and private enterprises. This interoperability is crucial to avoid media breaks and foster widespread acceptance.

It should be possible that the EUBW supports the binding of identity attributes and transactional data. This capability is fundamental for representing complex business scenarios involving legal delegation and authority. We advocate for the establishment of a harmonized and interoperable, EU-wide LPID within the EUDI framework, along

with integrated role and mandate management. The wallet should allow legal entities to link verified representatives with clear scopes of authority – without depending on external mandate registers—ensuring legal certainty in digital interaction, for instance by connecting signatures and seals with representation credentials. Additionally, the unlinkability principle – developed for the EUDI-Wallet to preserve the privacy of natural persons – should not be applied to the EUBW. In the business context, traceability, accountability, and auditability are essential. Applying unlinkability would conflict with these requirements and hinder the transparent attribution of actions to legal representatives, complicating business operations and contractual frameworks that rely on this.

Moreover, the EUBW should offer full wallet functionality, including the issuance, storage, presentation, and validation of (qualified) electronic attestations and identity data. It must be interoperable with the EUDI-Wallet ecosystem and support public and private sector relying party functionalities. As the eIDAS trust services ecosystem already provides mature, legally recognized, and technologically integrated trust services, the EUBW should be built on those existing eIDAS trust services such as (Qualified) Electronic Registered delivery services (Q-ERDSs) for notification in order to meet the objectives stated in the call for evidence. The appropriate level of assurance – whether substantial or high – should be determined based on use cases.

Legal and structural requirements

From a regulatory standpoint, the development of the EUBW must be fully aligned with existing applicable EU legislation. This includes both eIDAS-Regulation (EU) No. 910/2014, amended by the regulation (EU) 2024/1183, as well as the provisions on legal entity identification as laid out in Annex 1, No. 3 of the Implementing Acts. The wallet should also be built to support AML compliance, simplifying the verification of beneficial owners and streamlining KYC processes across Member States using the EUDI-Wallet infrastructure.

Moreover, the EUBW must comply with the Data Act and the Data Governance Act to ensure trusted, lawful, and reusable exchange of public and private sector data. Its development should build on insights from EBSI VECTOR and the ongoing and new EUDI-Wallet Large-Scale Pilots (POTENTIAL, NOBID, DC4EU, EWC, APTITUDE and WEBUILD) – for instance for the LPID definition and business wallet concepts – as well as on the standards created under those deliverables.

A further structural requirement concerns the legal representation. The principle of legal representation through a duly empowered natural person is essential, especially for basic functionalities such as those in B2G context. Accordingly, it is necessary to ensure interoperability between the EUDI-Wallet and the EUBW, especially with regard to role and mandate management. For more advanced use cases, mechanisms must be established to ensure traceability.

According to Article 5a, paragraph 15, sentence 1 of the eIDAS Regulation, the use of EUDI-Wallet is voluntary. While this voluntary nature is appropriate for individuals, it presents a significant obstacle to the digitalization of organizations, as alternative authentication methods must be maintained. To enable streamlined and uniform

digital processes, the EUBW should be exempt from this principle of voluntariness. This should also go hand in hand with a sustainable cost model that supports high adoption and helps ensure that the EUDI ecosystem remains inclusive, enabling broad participation and interaction across stakeholders. The financial situation of small businesses and sole proprietors should be duly taken into account when establishing this model, especially when such businesses make use of basic functionalities only.

As far as the implementation and deployment of the EUBW are concerned, it should not be reserved to or monopolized by the public entities. Unlike the EUDI-Wallet, where the public sector plays a key role in safeguarding citizens' rights, the EUBW operates in the economic domain in which private actors, including for instance QTSPs and identity providers, bring essential expertise, agility, and investment capacity. The role of the state should primarily be limited to oversight and standard-setting, not direct operation, and it shouldn't be the only entity to provide EUBW.

Additionally, in order to close the aforementioned registration gap, we recommend the European Commission to develop and publish clear operational and legal guidelines for LPID issuance and registration beyond today's BRIS-registered entities. The Commission should actively engage with Member States and the European Business Register Association (EBRA) to assess, and where necessary, extend the legal mandate of national business registries to include LPID issuance for currently non-registered legal persons. It is crucial to foster a trusted, interoperable, and inclusive identity infrastructure serving the full spectrum of legal entities operating within the European Union. An option would be to leverage national business registries as they are already integrated into BRIS, have strong capabilities in verifying identities, performing authentication, issuing verifiable Know Your Business (KYB) credentials—including Ultimate Beneficial Owner (UBO) data—monitoring changes, and revoking credentials as necessary. Such KYB credentials are crucial for onboarding processes in financial services, professional service industries, Industry 4.0 scenarios, and supply chain management. Additionally, KYB records provide foundational support for eGovernment procedures, onboarding into data spaces, and the implementation of export controls. In this sense, business registries can effectively act as a one-stop-shop, offering both LPID and verifiable KYB records, thus greatly contributing to the robustness, efficiency, and legal certainty of the European digital identity ecosystem. Moreover, existing global infrastructures, such as GLEIF, which has successfully established a standardized ecosystem for organizational identities, should also be taken into account in future developments

To ensure interoperability, we demand that all credentials issued or stored in the EUBW follow standardized, semantically aligned formats. Only through qualified and standardized digital proofs and mapping of attributes can the EUBW integrate seamlessly into existing IT systems, including for digital authorization mechanisms in the form of Electronic Attribute Attestations (EAA).

Finally, we emphasize the need for a transparent and efficient certification and conformity assessment process. Accredited bodies must ensure that the wallet meets legal, technical, and operational standards – building trust across stakeholders and enabling its cross-border use at scale.

Bitkom represents more than 2,200 companies from the digital economy. They generate an annual turnover of 200 billion euros in Germany and employ more than 2 million people. Among the members are 1,000 small and medium-sized businesses, over 500 start-ups and almost all global players. These companies provide services in software, IT, telecommunications or the internet, produce hardware and consumer electronics, work in digital media, create content, operate platforms or are in other ways affiliated with the digital economy. 82 percent of the members' headquarters are in Germany, 8 percent in the rest of the EU and 7 percent in the US. 3 percent are from other regions of the world. Bitkom promotes and drives the digital transformation of the German economy and advocates for citizens to participate in and benefit from digitalisation. At the heart of Bitkom's concerns are ensuring a strong European digital policy and a fully integrated digital single market, as well as making Germany a key driver of digital change in Europe and the world.

Published by

Bitkom e.V.

Albrechtstr. 10 | 10117 Berlin

Contact person

Lorène Slous | Policy Officer Trust Services & Digital Identity

T +49 30 27576-157 | l.slous@bitkom.org

Responsible Bitkom committee

AK Digitale Identitäten (Digital Identity)

AK Anwendung elektronischer Vertrauensdienste (Trust Services)

AK Digitale Verwaltung (Public Administration)