

EU Business Wallet: Trust Requires Certification

A Key Building Block of the Single Market Requiring the Same Level of Security as the EU Digital Identity Wallet

The European Business Wallet is set to become a core component of the Single Market's digital infrastructure. It will enable companies to exchange official documents, prove representation rights and carry out legally binding transactions across borders.

It is also expected to be used alongside the European Digital Identity Wallet under Regulation EU No 910/2014, forming part of the same ecosystem of trusted digital services. In this context, the European Business Wallet will interact with identity data, credentials and trust services, and will therefore be exposed to similar risks and security requirements.

Recent developments already demonstrate the risks of deploying components within this ecosystem without prior certification. The age verification application promoted at Union level, intended to be integrated into or used in conjunction with the European Digital Identity Wallet, **was shown by independent security researchers to be compromisable in less than two minutes**¹. These findings were made in the absence of prior independent security evaluation, including penetration testing² and certification.

This example exposes a structural weakness of an approach relying on ex-post supervision. Introducing non-certified applications into the wallet ecosystem creates systemic vulnerabilities

¹ Politico, EU launched age-checking app, hackers say it took them 2 minutes to break it.
<https://www.politico.eu/article/eu-brussels-launched-age-checking-app-hackers-say-took-them-2-minutes-break-it/>

² Penetration testing is the act of locating weaknesses and vulnerabilities of devices and information systems by anticipating the intent, actions and skills of malicious hackers. Penetration testing is done for defensive purposes, with the objective to improve the security of devices and information systems, and to give assurance that they will resist attacks once deployed
Cybersecurity Act: Ethical Hacking does matter - <https://www.eurosmart.com/eurosmart-welcomes-the-european-commission-proposal-to-boost-the-eu-cybersecurity-industry-by-the-creation-of-a-cybersecurity-industrial-technology-and-research-competence-centre-2/>

and undermines trust in the entire infrastructure. Relying parties cannot be expected to distinguish between certified and non-certified components within the same system.

While the European Digital Identity Wallet is subject to a certification framework under Regulation EU No 910/2014, no equivalent mechanism is currently proposed for the European Business Wallet. This inconsistency creates a gap in the trust framework and risks undermining the security and credibility of the entire ecosystem.

There is therefore no justification for applying a lower level of security to the European Business Wallet. It must meet the same level of security as the European Digital Identity Wallet.

Trust requires verifiable security – Why Pentesting Matters

Trust cannot be achieved through the mere definition of technical requirements. It must be supported by mechanisms that demonstrate, in a verifiable and comparable manner, that those requirements are effectively implemented.

The EU Cybersecurity Certification Framework provides such a mechanism. It ensures independent validation of compliance, based on recognised standards, and guarantees that systems meet the required level of security and robustness.

A framework relying primarily on self-declaration or weak controls would not be sufficient for infrastructure enabling legally binding transactions.

Proposed amendment: mandatory certification of core components of the European Business Wallet by conformity assessment bodies designated by Member States.

Alignment with the European Digital Identity framework and existing Union instruments

The European Union has already established a robust and operational certification-based framework for the European Digital Identity Wallet under Regulation EU No 910/2014 as amended.

This framework relies on certification of core components by conformity assessment bodies designated by Member States and on European cybersecurity certification schemes established under Regulation EU 2019/881. It provides a coherent, harmonised and trusted approach that enables interoperability and mutual recognition across the Union.

Importantly, this framework is already being implemented. The European Union Agency for Cybersecurity is currently developing a European cybersecurity certification scheme for the European Digital Identity Wallet, which has been identified as a priority at Union level.

At the same time, Member States are required to establish certification mechanisms at national level to enable the deployment of the European Digital Identity Wallet ahead of the adoption of a

Union-wide certification scheme. This demonstrates that certification is an immediate operational requirement, not a future objective.

There is therefore no justification for developing a separate or weaker model for the European Business Wallet.

Proposed amendment: alignment of certification requirements with European cybersecurity certification schemes under Regulation EU 2019/881 and consistency with the framework established under Regulation EU No 910/2014.

Ex-ante certification as a prerequisite - not ex-post supervision

For systems enabling legally binding transactions and the exchange of sensitive business data, security cannot rely on ex-post supervision alone.

An approach based primarily on ex-post controls assumes that non-compliance or vulnerabilities can be addressed after deployment. This assumption is flawed. Once deployed, insecure components may already have been exploited, leading to legal uncertainty, financial losses and a loss of trust that is difficult to restore.

For this reason, **certification must take place before deployment. Ex-ante certification ensures that core components have been independently verified and comply with the applicable requirements before they are used. It prevents risks from materialising rather than attempting to mitigate them after the fact.**

The approach adopted for the European Digital Identity Wallet reflects this reality by placing certification at the core of the framework. The European Business Wallet should follow the same logic.

Proposed amendment: introduction of an ex-ante certification requirement, prohibiting the use of non-certified components for the European Business Wallet.

A balanced governance model supporting European Digital Sovereignty

The certification framework for the European Business Wallet preserves a balanced distribution of responsibilities between Member States and the Union. Member States designate conformity assessment bodies and supervise certification, while the Commission ensures coordination, harmonisation and the publication of certified wallets.

At the same time, the European Business Wallet has direct implications for digital sovereignty. A certification-based approach strengthens European control over critical components, including hosting and operational infrastructure, by ensuring that they comply with Union requirements and remain subject to Union law.

Alignment with the framework established under Regulation EU No 910/2014 and Regulation EU 2019/881 supports a coherent European ecosystem and reduces exposure to risks linked to third-country legal or technical frameworks.

Proposed amendment: preservation of Member State responsibilities combined with Union-level coordination and certification requirements ensuring that critical components, including hosting and infrastructure, are subject to Union law and protected from third-country access or control.

Conclusion

The European Business Wallet will only deliver its full potential if it is trusted across the Union. Trust cannot be assumed. It must be ensured through a robust and enforceable certification framework.

The European Union has already established such a model for the European Digital Identity Wallet under Regulation EU No 910/2014. There is no justification for applying a weaker approach to the European Business Wallet.

Failure to introduce mandatory certification would create fragmentation, weaken security and undermine confidence in the system from the outset. **Only a certification-based framework can ensure a high level of protection, enable interoperability and guarantee a level playing field across the Single Market.**

For these reasons, the proposed amendments introduce mandatory certification, alignment with Regulation EU 2019/881 and a transparent publication mechanism. They are necessary to ensure the security, resilience and credibility of the European Business Wallet and should be fully supported.

Proposed Amendments

Text Proposed by the Commission	Proposed Amendment	Rationale
	Recital (32a) NEW In order to ensure a high level of trust, security and interoperability across the Union, European Business Wallets should be designed in a manner consistent with the approach applicable to European Digital Identity Wallets under Regulation (EU) No 910/2014. In particular, the framework established in Article 5c of Regulation (EU) No 910/2014 provides for certification of conformity, a high level of cybersecurity assurance and interoperability across Member States. European Business Wallets should follow an equivalent approach, adapted to their specific use cases. Given that European Business Wallets enable legally binding transactions, the exchange of official documents and the management of representation rights across borders, their core components should	European Business Wallets will enable legally binding transactions, including the exchange of official documents and the management of representation rights across borders. They therefore require a high level of trust, security and interoperability. This recital clarifies that the proposal should be consistent with the approach established for European Digital Identity Wallets under Regulation (EU) No 910/2014, in particular the certification-based framework set out in Article 5c, in order to avoid fragmentation and ensure mutual recognition across Member States.

	meet harmonised certification and assurance requirements.	
Article 6 Technical features	Article 6 Technical features and certification of European Business Wallets	The amendment updates the title to reflect that Article 6 not only defines technical features but also establishes certification and conformity assessment requirements, thereby improving legal clarity and coherence.
Article 5 Core functionalities of European Business Wallets	Article 5(6) (new) European Business Wallets shall be designed, implemented and operated in a manner that ensures that critical components, including hosting and operational infrastructure, are subject to Union law and protected against access or control by third-country jurisdictions that may compromise security or confidentiality.	This paragraph introduces a general requirement ensuring that critical components of European Business Wallets are subject to Union law and protected against access or control by third-country jurisdictions. Given the use of European Business Wallets for legally binding transactions and sensitive business data, this safeguard is necessary to prevent external legal or technical interference that could undermine security and trust. It complements the technical and certification requirements set out in Articles 6 and 7 and contributes to a consistent level of protection across the wallet ecosystem.
Article 6(5) The Commission shall, by means of implementing acts, establish a list of reference standards and, where necessary, establish specifications and procedures for	Article 6(5) The Commission shall, by means of implementing acts, establish a list of reference standards and, where necessary, establish specifications and procedures for the	This amendment extends the scope of the Commission's implementing powers to include certification-related elements, namely the applicable certification schemes,

the technical features of European Business Wallets provided for in paragraphs 1, 2 and 3 of this Article. Those implementing acts shall be adopted in accordance with the procedure referred to in Article 19.	technical features of European Business Wallets provided for in paragraphs 1, 2 and 3 of this Article. Those implementing acts shall also specify, where relevant: (a) the European cybersecurity certification schemes applicable to the core components of European Business Wallets, in accordance with Regulation (EU) 2019/881; (b) the conformity assessment procedures to be applied; (c) the assurance levels required, taking into account the risks associated with the use of European Business Wallets; (d) the conditions for ensuring consistency with the approach applicable to European Digital Identity Wallets under Regulation (EU) No 910/2014. (e) the hosting and operation of core components of European Business Wallets, including infrastructure supporting cryptographic key generation, management and validation mechanisms, shall be considered critical components.	conformity assessment procedures and assurance levels. This is necessary to ensure that the certification framework introduced in paragraphs 6 to 9 can be effectively operationalised and applied consistently across the Union. Without such provisions, the certification requirement would remain insufficiently defined and could lead to divergent national approaches. By explicitly referring to European cybersecurity certification schemes established pursuant to Regulation (EU) 2019/881, the amendment ensures that the framework builds on existing Union mechanisms and avoids duplication. It also enables the Commission to define, through implementing acts subject to Member State control, the detailed technical and procedural requirements necessary for interoperability and security. Moreover, (e) clarifies that hosting and infrastructure are critical components, ensuring they fall within the scope of technical and certification requirements. This approach is consistent with the governance model applied to European Digital Identity Wallets and ensures that certification
---	---	--

	Those implementing acts shall be adopted in accordance with the procedure referred to in Article 19.	is both harmonised and adaptable to technological developments.
	Article 6(6) new The conformity of the core components of European Business Wallets, including wallet units, secure cryptographic devices and applications, cryptographic key generation and management, and validation mechanisms, with the requirements laid down in this Article and, where applicable, with the standards and technical specifications referred to in paragraph 5, shall be certified by conformity assessment bodies designated by Member States.	This paragraph establishes that the conformity of the core components of European Business Wallets must be certified by conformity assessment bodies designated by Member States. This approach is fully aligned with the certification framework established under Regulation EU No 910/2014, in particular Article 5c on the certification of European Digital Identity Wallets, which requires certification by conformity assessment bodies designated by Member States. The introduction of a certification requirement, rather than a simple assessment, reflects the critical nature of European Business Wallets, which will be used for legally binding transactions and the exchange of sensitive business information. Certification provides a higher level of assurance and creates a clear, enforceable standard for compliance. By entrusting conformity assessment bodies designated by Member States, the provision ensures independence, technical competence and alignment with existing Union conformity assessment frameworks. It also reinforces

		Member States' role in supervising certification activities. This approach mirrors the certification-based model established for European Digital Identity Wallets and contributes to a consistent level of trust across the Union.
	Article 6(7) new Certification of the conformity of the core components of European Business Wallets referred to in paragraph 6 that are relevant for cybersecurity shall be carried out in accordance with European cybersecurity certification schemes adopted pursuant to Regulation (EU) 2019/881 and referred to in the implementing acts adopted under paragraph 5, ensuring at least a high level of assurance commensurate with the risks associated with their use.	This provision specifies that certification of components relevant for cybersecurity is to be carried out under European cybersecurity certification schemes adopted pursuant to Regulation (EU) 2019/881. It ensures that certification is based on harmonised Union schemes and that a high level of cybersecurity assurance is achieved across all Member States. By relying on the Cybersecurity Act, the amendment avoids the creation of parallel or overlapping certification frameworks and ensures coherence with existing Union legislation. The reference to assurance levels ensures that certification is proportionate to the risks associated with the use of European Business Wallets, while maintaining a high level of protection. This provision complements paragraph 6 by specifying the applicable framework for

		certification and contributes to a structured and coherent certification system.
	Article 6(8) NEW For requirements referred to in paragraph 6 that are not covered, or only partially covered, by European cybersecurity certification schemes, Member States may establish national certification or conformity assessment schemes, taking into account the specifications adopted pursuant to paragraph 5.	This paragraph provides for the possibility for Member States to establish national certification or conformity assessment schemes where European cybersecurity certification schemes do not yet fully cover all relevant requirements. (As European cybersecurity certification schemes under Regulation (EU) 2019/881 are still being deployed) This is necessary to ensure that all components of European Business Wallets can be subject to certification, even in areas where Union-level schemes are still under development. It avoids regulatory gaps and ensures continuity of the certification framework. At the same time, the provision ensures that national schemes are aligned with the specifications adopted at Union level, thereby limiting fragmentation and ensuring a gradual convergence towards harmonised certification.
	Article 6(9) NEW The core components referred to in paragraph 6 shall not be used for the provision of European Business Wallets	This provision introduces a clear ex-ante requirement that core components of European Business Wallets may not be used unless the applicable certification or

	unless the applicable certification or conformity assessment requirements have been fulfilled.	conformity assessment requirements have been fulfilled. This is a key element of the certification-based approach, ensuring that compliance is verified prior to deployment rather than after the fact. It prevents the use of non-compliant or insecure components and strengthens trust in the system. By establishing certification as a condition for use, the provision enhances legal certainty and enforceability and aligns the proposal with the approach applied to European Digital Identity Wallets.
Article 7 Requirements and obligations for providers of European Business Wallets 6. Providers of European Business Wallets shall: (a) ensure security-by-design; (b) provide validation mechanisms; (c) ensure revocation; ...	Article 7 Requirements and obligations for providers of European Business Wallets 6. Providers of European Business Wallets shall: (a) ensure security-by-design; (b) provide validation mechanisms; (c) ensure revocation; ... (h) ensure that the core components of the European Business Wallet comply with the	This amendment introduces an explicit obligation for providers to ensure that the core components of European Business Wallets comply with the certification requirements set out in Article 6. It ensures that certification is not merely a formal requirement but is effectively implemented and maintained by providers. It also clarifies the allocation of responsibilities, making providers accountable for ensuring that certified components are used and remain compliant throughout the lifecycle of the wallet.

	conformity assessment and certification requirements set out in Article 6(6) to (9). (i) ensure that critical components of the European Business Wallet, including hosting and operational infrastructure, are hosted and operated in the Union by entities established in the Union and subject to Union law, in a manner that ensures protection against access or control by third-country jurisdictions.	This strengthens enforcement and complements the certification framework by linking it directly to provider obligations. Moreover (i) ensures that critical components remain under Union jurisdiction and are protected from third-country interference, reinforcing the security of the wallet ecosystem.
	Article 7(7) NEW Where the provision of European Business Wallets relies on qualified trust services, such services shall comply with Regulation (EU) No 910/2014.	This provision clarifies that, where European Business Wallets rely on qualified trust services, those services must comply with Regulation (EU) No 910/2014. It ensures consistency with the existing Union framework for trust services, which already provides a high level of assurance for services such as electronic signatures, seals and time stamps. By explicitly linking Business Wallets to this framework, the amendment avoids duplication of requirements and ensures that existing trust infrastructures can be reused in a coherent and legally sound manner.

	Article 8a NEW Publication of certified European Business Wallets 1. Member States shall inform the Commission without undue delay of European Business Wallets provided in accordance with this Regulation whose core components have been certified by the conformity assessment bodies referred to in Article 6(6). They shall inform the Commission without undue delay where a certification is cancelled and shall state the reasons for the cancellation. 2. The information provided by Member States pursuant to paragraph 1 shall include at least: (a) the certificate and certification assessment report relating to the core components of the European Business Wallet; (b) a description of the European Business Wallet and its main functionalities; (c) information on the provider of the European Business Wallet and the applicable supervisory and liability regime;	Paragraph 1 requires Member States to notify the Commission of European Business Wallets whose core components have been certified. • It ensures that Member States retain a central role in the certification and supervision process, consistent with the overall governance model of the proposal. • The obligation to notify cancellations of certification ensures that the system remains up to date and responsive to security or compliance issues. Paragraph 2 defines the minimum information to be provided in the notification. • It ensures transparency and enables the Commission, other Member States and users to understand the scope and level of certification. The inclusion of certification reports, supervisory information and liability arrangements enhances trust and accountability. Paragraph 3 requires the Commission to establish, publish and maintain a list of certified European Business Wallets, including publication in the Official Journal of the European Union and in a machine-readable format.
--	---	---

	(d) the authority or authorities responsible for the supervision of the provider; (e) arrangements for suspension or withdrawal of certification or of compromised components. 3. On the basis of the information received pursuant to paragraph 1, the Commission shall establish, publish in the Official Journal of the European Union and maintain in a machine-readable form a list of certified European Business Wallets. 4. A Member State may submit a request to the Commission to remove a European Business Wallet from the list referred to in paragraph 3. 5. Where there are changes to the information provided pursuant to paragraph 1, the Member State shall provide the Commission with updated information. 6. The Commission shall keep the list referred to in paragraph 3 updated by publishing in the Official Journal of the European Union the corresponding	Paragraph 4 allows Member States to request the removal of a European Business Wallet from the list. • It provides a mechanism to address cases where certification is withdrawn or where compliance issues arise, ensuring that the list remains reliable and up to date. Paragraph 5 ensures that any changes to the information provided are communicated to the Commission. It guarantees that the list reflects the current certification status. Paragraph 6 requires the Commission to keep the list updated and to publish amendments without undue delay. Paragraph 7 empowers the Commission to adopt implementing acts to define the formats and procedures for notification, updates and removal. • It ensures harmonised implementation across the Union and allows for technical standardisation, while maintaining Member State oversight through the applicable committee procedure.
--	---	--

	amendments to the list without undue delay. 7. The Commission shall, by means of implementing acts, establish the formats and procedures applicable for the purposes of paragraphs 1, 4 and 5. Those implementing acts shall be adopted in accordance with the procedure referred to in Article 19.	
Article 10 European Digital Directory	Article 10(7) (new) The European Digital Directory, including its machine-readable interface, secure web-based platform and any security-critical or trust-critical supporting infrastructure, shall be hosted and operated in the Union by entities established in the Union and subject to Union law, in a manner that ensures protection against access or control by third-country jurisdictions that may compromise security or confidentiality.	Ensures that the European Digital Directory, as a core component of the European Business Wallet framework, is hosted and operated within the Union and remains subject to Union jurisdiction. Given its role as a trusted source of information and as a key enabler of communication between European Business Wallet owners, providers and public sector bodies, the Directory should not depend on hosting or operational arrangements that could expose it to extraterritorial risks or undermine the objectives of trust, resilience and digital sovereignty pursued by the Regulation.

About us

Eurosmart, the Voice of the Digital Security Industry, is a **European non-profit association located in Brussels**, representing the **Digital Security Industry** for multisector applications. **Founded in 1995**, the association is committed to expanding the world's Digital secure devices market, developing smart security standards and continuously improving the quality of security applications.

