bitkom

Position Paper

December 2025

eIDAS Implementing Act: European Digital Identity Wallets – user onboarding

Summary

From Bitkom's perspective, clearer provisions are needed on wallet and device binding, closer alignment with established European standards, and a flexible identity proofing approach besides the eID as the reference method for identification that supports fully automated onboarding and hybrid onboarding when strict security requirement are not met in well-defined and secure scenarios.
Bitkom further considers a risk-based PID onboarding model, the involvement of independently accredited certification bodies, and proportionate conformity and testing requirements essential to ensure scalability and market readiness.
Overall, the Implementing Act should enable secure, interoperable and operationally feasible onboarding processes that support broad adoption of the EUDI Wallet throughout the EU.

Bitkom highlights that a key challenge in achieving a European level playing field lies in clarifying the technical specifications for assurance levels "high" and "substantial", as mandated by Article 8(3) of the eIDAS Regulation, and underlines the importance of developing the corresponding Implementing Act in a timely manner to ensure legal certainty and consistent application across Member States.

Specific comments on the implementing regulation

Nr.	Article	Action	Justification/Recommendation
1	**Recital (1)**	Specify	It is not specified in the CIR or its Annex how the EUDIW and device binding should be performed. We recommend describing the EUDIW and device binding according to the Wallet Unit Attestation

			(WUA) specification that is published by EC DG-CNCT as EUDIW TS03. For general information, WUA will also be described in CEN TS 18098 (PID on-boarding) and will be specified in ETSI TS 119 476-3 (WUA).
2	**Annex (5)**	Amend	It is stated that the identity proofing process for PID issuance must be fully automated. On that matter, we express serious security concerns and point out the need to take all the necessary measure to ensure a high and consistent level of trust, robustness, and resilience of identity proofing processes across the EU, in particular against fraud, impersonation, and emerging attack vectors. Hybrid identity proofing should also not be excluded if security requirements are not met with a fully automated process and recommendations of European cybersecurity agencies should be taken into account.
3	**Annex**	Amend	Using electronic signatures for PID on-boarding is implicitly allowed since this is specified in ETSI TS 119 461 v2.1.1 (identity proofing) clause 9.5.1 requirement USE-9.5.1-07. . PID on-boarding should be stricter and not rely upon identification based on electronic signatures as supplementary means. Hence, we recommend restricting the Annex so that ETSI TS 119 461 v2.1.1, requirement USE-9.5.1-07, which allows the use of electronic signatures as an identification method, is not permitted for PID on-boarding.
4	**Annex**	Amend	The Annex refers to ETSI TS 119 461 clauses (e.g., 9.2.3.4, 9.5.3) for identity proofing. In line with eIDAS 2.0 (Articles 6a and 12a), certification should be carried out by CABs accredited under Regulation (EC) No 765/2008 and the Cybersecurity Act, ensuring compliance with security and interoperability requirements. This approach guarantees harmonized trust and security across Member States.
5	**Regulation and/or annex**	Amend	The Commission proposal sets clear expectations for wallet onboarding: ▪ An existing eIDAS identity at Level of Assurance “high”, or ▪ by electronic identification means conforming to assurance level substantial in conjunction with additional remote onboarding procedures in order to meet LoA “high” (i.e. an ID document or reference image for

			verification and biometric - as long as security requirements are met for example through direct comparison with an official picture stored in the document's secure chip ▪ face matching, technology-neutral processes Including these elements explicitly in the Implementing Regulation ensures flexibility for Member States while maintaining strong security standards. It also supports innovation and prevents fragmentation in onboarding practices across the EU.
6	**Annex**	Amend	The Annex modifies the point 8.3.3 in this way: "*The effectiveness of the measures for complying with the requirements VAL-8.3.3-05X, VAL-8.3.3-05A, VAL-8.3.3-05B, VAL-8.3.3-05C, VAL-8.3.3-07A and VAL-8.3.3-07X, shall be tested by an accredited laboratory or a national competent authority, whenever they are designated, at the latest by 19 August 2027 and then be repeated every second year*." The Implementing Act requires accredited laboratory testing for the requirements VAL-8.3.3-07A and VAL-8.3.3-07X related to physical ID document validation. Such obligations are disproportionate, do not reflect the actual operational risk, and exceed the current capacity of accredited laboratories in Europe, creating the risk of market blockage, inability to complete testing cycles in time, and severe delays in onboarding processes relying on IDV systems. Proposal: Remove references to VAL-8.3.3-07A and VAL-8.3.3-07X from the Implementing Act. Limit the obligation of accredited laboratory testing to purely technical components (e.g., PAD/IAD mechanisms covered by VAL-8.3.3-05X/A/B/C), consistent with the proportionality principle and the existing conformity assessment framework for QTSPs.
7	**Annex**	Specify	The Annex modifies the point 9.5.3 in this way: "*An identity proofing process fulfilling the requirements for Extended LoIP from one of the use cases described in clauses 9.2.1, 9.2.2, or 9.2.3 of the present document, or it has been previously been peer reviewed or certified by an accredited conformity assessment body to comply with assurance level high in accordance with Regulation (EU) No 910/2014 [i.25] shall*

			be used to capture a reference face image and to bind the necessary identity attributes to this reference face image." This is aligned with the eIDAS ARt 5a(24) provision "by electronic identification means conforming to assurance level substantial in conjunction with additional remote onboarding procedures that together meet the requirements of assurance level high." We think that identity proofing solutions and applicant binding in case of Extended Level of Identity Proofing (LoIP) shall support both the following scenario in a fully automated way: (a) PACE unlocking through the use of the user PIN (PIN-CAN) where the electronic identity document implements such mechanism (if already notified as an eID scheme, this scenario is by default covered by clauses 8.2.4 and 9.2.4 and, therefore, in this case, Member States may directly leverage the electronic identity document for the onboarding process for the purposes of this Regulation, as also reiterated in recital 3), and (b) biometric verification of the applicant against the portrait stored in the document's secure chip where PIN-CAN is not applicable or chosen/known by the user. Since clause 9.5 of ETSI TS 119 461 includes Subclause 9.5.2, which allows the extension from a baseline Level of Identity Proofing (LoIP) to an extended LoIP through the use of an identity document and the applicant's facial image and requirement USE-9.5.2-01 specifies that the requirements defined for one of the use cases described in Clauses 9.2.1, 9.2.2, or 9.2.3 shall be applied. Clause 9.2.3 is precisely the use case that requires protection in this context, as it covers the scenario based on an NFC-enabled digital document combined with facial verification, without the use of a PIN. Security requirements should be met in order to avoid any fraud or similar cybersecurity issues. Proposal: since the objective is to ensure broad adoption of the wallet, we kindly request confirmation that both scenarios described can

			be implemented in a fully automated manner if strict security requirements are met, otherwise in a hybrid way, by the IPSP.
8	**Annex**	Amend	8.2.4 Use of existing eID means as evidence should reference to 8.2.4-02A instead of 8.2.4-02X

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)