Bundesverband der Deutschen Volksbanken und Raiffeisenbanken e. V.
Bundesverband deutscher Banken e. V.
Bundesverband Öffentlicher Banken Deutschlands e. V.
Deutscher Sparkassen- und Giroverband e. V.
Verband deutscher Pfandbriefbanken e. V.

Die Deutsche Kreditwirtschaft

Comments

on the draft implementing act for the onboarding of users to the European Digital Identity Wallet (EUDIW) under eIDAS 2.0

Lobby Register No R001459
EU Transparency Register No 52646912360-95

Contact:
Diana Campar
Associate Director
Telephone: +49 30 1663-1546
E-Mail: diana.campar@bdb.de

Berlin, 30 December 2025

The **German Banking Industry Committee** is the joint committee operated by the central associations of the German banking industry. These associations are the Bundesverband der Deutschen Volksbanken und Raiffeisenbanken (BVR), for the cooperative banks, the Bundesverband deutscher Banken (BdB), for the private commercial banks, the Bundesverband Öffentlicher Banken Deutschlands (VÖB), for the public banks, the Deutscher Sparkassen- und Giroverband (DSGV),
for the savings banks finance group, and the Verband deutscher Pfandbriefbanken (vdp), for the Pfandbrief banks. Collectively, they represent approximately 1,700 banks.

Coordinator:
Bundesverband deutscher Banken e. V.
Burgstraße 28 | 10178 Berlin | Germany
Telephone: +49 30 1663-0
www.die-deutsche-kreditwirtschaft.de
www.german-banking-industry.org

Comments on the draft implementing act for the onboarding of users to the European Digital Identity Wallet (EUDIW) under eIDAS 2.0

I. General comments

A) Draft implementing regulation - Ares(2025)10575642

Paragraph 3 of the Draft Implementing Regulation highlights the importance of leveraging electronic identification means for onboarding users into European Digital Identity Wallets ("Wallets") and underscores the need for harmonised standards that align with established practices and evolving security requirements. We offer the following feedback regarding the application of assurance levels within the financial industry, specifically in the context of the forthcoming European Digital Identity Wallet (EDIW) and the principles established by the eIDAS Regulation (EU No 910/2014) and the Implementing Regulation (EU) 2015/1502.

The eIDAS Regulation (EU No 910/2014) established three distinct levels of assurance for electronic identification schemes: "low", "substantial", and "high". The core distinction between these levels lies in the stringency of the identity proofing processes and the robustness of security measures applied throughout the lifecycle of the identity. The amended eIDAS Regulation (commonly referred to as eIDAS 2.0) retains these levels and further clarifies their application, particularly with the introduction of the European Digital Identity Wallet (EUDIW).

In essence, while an eID at the "substantial" assurance level offers a robust and widely applicable degree of security and certainty, the "high" assurance level represents the gold standard. It is reserved for situations where the potential impact of identity fraud is so severe that it necessitates the absolute maximum level of confidence and protection. The EUDIW itself is designed to accommodate identity attributes issued at both "substantial" and "high" assurance levels.

From a financial industry perspective, a staggered, risk-based approach to applying these eIDAS assurance levels is not only sensible, but also highly beneficial. This approach aligns seamlessly with existing financial regulations and best practices, notably those governing Anti-Money Laundering (AML) and Know Your Client (KYC) obligations.

Applying eIDAS assurance levels in a staggered manner directly supports and enhances the established risk-based approach to client due diligence. We recognise that not all business relationships, products, and services carry the same inherent level of risk concerning fraud, money laundering, or terrorist financing.

For lower-risk products or services, a "low" or "substantial" assurance level can be sufficient to meet the inherent risk profile. This enables a streamlined and accelerated identification process, significantly improving the customer experience and reducing potential onboarding friction.

Conversely, for products and services that entail higher levels of fraud, money laundering, or terrorist financing risk, robust identification processes requiring "high" assurance are entirely justified. By reserving the most rigorous (and typically more expensive) identity proofing, advanced security measures, and potentially manual verification steps for where they are truly needed, financial institutions can significantly reduce operational costs for lower-risk offerings.

This allows for more effective resource allocation and optimized security spending, maximising prevention effectiveness against genuine threats.

A staggered, risk-based application of eIDAS assurance levels is not merely beneficial but essential for financial institutions. It provides financial institutions with greater granularity and flexibility in designing their client journeys and risk controls. They can tailor the identity verification process precisely to the specific risks associated with the product or service type, transaction value, and client segment. It enables them to effectively navigate the complex landscape of digital identity, enhance security, optimise operational costs, significantly improve customer experience, and ensure robust regulatory compliance in an increasingly digital world.

Further, we advocate for the principle that once an electronic identification means at the "high" assurance level has been successfully used for identification and considering the robust measures against changes in personal identification data, it should generally not be required to repeat the comprehensive identity proofing and verification processes. The initial identity proofing and verification procedures for "high" assurance are exceptionally stringent, often involving rigorous in-person verification or highly secure remote methods, comprehensive document verification, and cross-referencing with authoritative data sources. Once this meticulous process is completed and the eID means is issued, the identity is considered reliably established. A fundamental objective of the eIDAS framework is to facilitate the seamless, cross-border re-use of eID means. If a "high" assurance eID were subject to repeated full re-verification by every relying party (such as a financial institution) for each transaction, it would undermine the very purpose of the framework and introduce significant friction, negating the benefits of digital identity. Therefore, the high initial assurance should allow for subsequent reliance without necessitating a complete re-run of the complex identification process, provided the relying party trusts the notified eID scheme and the accompanying strong authentication mechanisms.

Considering this, we propose that upon the successful rollout and widespread availability of the European Digital Identity Wallet (EUDIW), and where identity attributes within the EUDIW are secured with credentials and an assurance level of "high", specific redundant verification steps during the onboarding process should be reconsidered. For instance, an additional separate verification of client data by comparing it with corresponding entries in the German transparency register (Transparenzregister) could be dispensed with. Instead, clients should be able to rely exclusively on the identity data provided through the EUDIW at a "high" assurance level. An additional, separate verification process in such cases would be redundant and, given the high level of security provided by the EUDIW framework, no longer justifiable. This approach would realise the full potential of the EUDIW for efficient and secure digital onboarding in the financial sector.

B) Annex - Ares(2025)10575642

Section 8.2.4 "Use of existing eID means as evidence" reads: "If the Baseline LoIP is targeted, the eID means shall have been notified at least at eIDAS LoA substantial or shall have been assessed by an independent conformity assessment body to fulfil the requirements for an

Comments on the draft implementing act for the onboarding of users to the European Digital Identity Wallet (EUDIW) under eIDAS 2.0

eIDAS substantial eID or eIDAS high eID. The independent conformity assessment body shall be accredited as per Article 3 (18) of Regulation (EU) No 910/2014 [i.25], and, if all applicable requirements are fulfilled, the assessment shall result in a certificate of compliance based on a certification audit…."

We kindly request clarification as to whether this passage is to be understood as introducing a potential opening for entities to participate, through the possibility of certification by independent conformity assessment bodies (and not exclusively by bodies notified by Member States), that go beyond the traditional eID providers designated by Member States. Specifically, the question arises whether private companies, such as credit bureaus (like Schufa), could under certain conditions act as independent conformity assessment bodies or have their eID means certified by such bodies for a substantial or high level of security to participate in the onboarding process.

This interpretation raises important questions regarding the uniformity of security and certification processes, as well as the accountability of the entities involved. Ensuring that only certified and responsible actors are involved in this sensitive area is crucial for trust in the European Digital Identity Wallets. As Financial Institutions, we are, and must be, able to rely on the eID/PID stored in the Wallet. While an opening for additional actors (potentially not certified by Member States) who integrate eID into the Wallet may improve accessibility and facilitate low-threshold access to the initiation and use of the EUDI-Wallets for EU citizens, the eID/PID in the Wallet remains the core element for its functionality. Therefore, it must be adequately protected and should not be entrusted to additional actors who are potentially not certified by Member States. Additionally, liability issues must be addressed, as such an opening could create new complexities regarding the accountability of the involved parties.

We therefore ask for confirmation or a more precise explanation of this point to fully understand the potential impact on market participation and the assurance of the required security level.

II. Comments on particular points

A) Draft implementing regulation - Ares(2025)10575642

It is stated: "The onboarding of users to the European Digital Identity Wallets ('wallets') is a crucial step as regards the verification of the identity of the wallet users, the binding of the personal identification data of the users to their wallets and to the user device in which the wallet units are installed."

It is, however, not specified in the CIR or its Annex how the EUDIW and device binding should be performed.

Proposed change: Describe the EUDIW and device binding according to the Wallet Unit Attestation (WUA) specification that is published by EC DG-CNCT as EUDIW TS03. The EUDIW

Comments on the draft implementing act for the onboarding of users to the European Digital Identity Wallet (EUDIW) under eIDAS 2.0

TS03 technical specification is in turn based on OpenID For Verifiable Credentials Issuance (OID4VCI).

WUA will also be specified in ETSI TS 119 476-3 (WUA). When ETSI TS 119 476-3 has been published, this standard could also be referenced by the CIR Annex.

B) Annex - Ares(2025)10575642

1) 5 Operational risk assessment: The draft implementing act frequently refers to external standards without summarising the applicable requirements (e.g. OVR-5-01 referring to ETSI EN 319 401, clause 5). We note that the multiplicity of cross-references makes it difficult to identify and understand the concrete obligations applicable to Wallet onboarding. Clarification or a more explicit indication of the relevant requirements would support consistent implementation.

2) 7.10 Collection of evidence and 7.12 Termination and termination plans: The notes to OVR-7.10-01 and OVR-7.12-01 allow for multiple possible distributions of roles between IPSPs, PID Providers, and Wallet Providers. This openness may lead Member States to introduce different operational models, which could impair interoperability and auditability.

We therefore recommend a binding and unambiguous clarification of responsibilities. For each task within the onboarding and identity-proofing process, a clear and nationally consistent allocation of roles between PID Providers, IPSPs, and Wallet Providers should be defined to avoid fragmentation and divergent interpretations.

3) 9.2.3.4 Use case for automated operation, 9.5.3 Use case for enhancing identity proofing to Extended LoIP by use of a previously captured reference face image and 8.3.3 validation of physical identity document: The technical requirements in USE-9.2.3.4-04, USE-9.5.3-01 and VAL-8.3.3-21 relate to automated, biometric and AI-supported identity verification processes, which are likely to qualify as high-risk AI systems within the meaning of the AI Act, depending on their concrete use. While the applicability of the AI Act follows directly from Union law, the draft Implementing Act does not explicitly clarify the relationship between these technical requirements and the obligations laid down for high-risk AI systems in Articles 10 to 15 of the AI Act. This may create legal and technical uncertainty and may lead to divergent interpretations and fragmentation across Member States. We therefore recommend including an explicit reference, preferably in a recital, clarifying that AI-supported identity verification processes covered by this Implementing Act remain subject, where applicable, to the requirements for high-risk AI systems set out in the AI Act.

Regarding USE-9.5.3-01, we note that the operational feasibility and security of identity proofing based on the reuse of a previously captured reference face image depend on the quality of both the historical and newly captured images. Insufficient image quality may increase the risk of false negatives and negatively affect onboarding outcomes.

Moreover, the reuse of historical images may introduce specific fraud risks, including the injection of outdated images and exposure to spoofing or deepfake attacks. Clear safeguards regarding image quality, liveness detection, and the secure capture, conservation and reuse of

reference face images from the initial receipt onwards would support secure and consistent implementation.

Finally, we note that the automated identity proofing requirements in USE-9.2.3.4-04 appear to assume digital-identity-document-based processes. This may necessitate substantial changes to existing onboarding models relying on alternative identification methods. Further clarification on the scope of application and acceptable equivalent approaches would support proportionate implementation.

4) It is stated: "9.2.3.4 Use case for automated operation – USE-9.2.3.4-04: The IPSP shall establish target values for the FAR and FRR, based on a risk analysis and its threats intelligence procedure, by following the methodology established in the ENISA report 'Methodology for sectoral cybersecurity assessments' [i.28] or an equivalent methodology, in fully automated identity proofing processes."

The identity proofing process for PID issuance is recommended to be a hybrid process, i.e. a combination of automated identity proofing with manual inspections.

Proposed change: Require the identity proofing process at LoIP Extended to be hybrid for PID on-boarding, i.e. a combination of automated identity proofing with manual inspections.

Hybrid identity proofing is also required by CEN TS 18098 (PID on-boarding) section 8.3.3.9.4. When the CEN TS 18098 (PID on-boarding) has been published, this standard could also be referenced by the CIR Annex.

5) 8.3.3 Validation of physical identity document: VAL-8.3.3-21 requires that the effectiveness of document validation measures be tested by an accredited laboratory or, where designated, by a national competent authority by 19 August 2027 and subsequently every two years. However, at present, many Member States do not have ISO/IEC 17025-accredited facilities in the relevant domains, nor have all designated competent authorities with equivalent testing capabilities. Given that establishing and accrediting such laboratories typically takes 18-36 months, compliance with the proposed deadline may prove unrealistic and could lead to capacity bottlenecks, delays in implementation and uneven security levels across Member States.

In addition, compliance with this requirement may necessitate the deployment of advanced document fraud detection technologies, often provided by specialised third-party vendors, combined with regular external testing. This may result in a significant operational and financial burden for providers, particularly in the context of limited testing capacity. Excessive or duplicative validation requirements could also negatively affect user experience, increasing the risk of client drop-off or rejection during onboarding, which may ultimately undermine the uptake of the EUDIWs.

Furthermore, the Annex introduces a biennial testing obligation but does not clarify whether this applies per provider, per system or software version, or per validation method, which creates operational uncertainty and risks fragmentation.

We therefore recommend aligning the implementation timeline with the actual availability of accredited laboratories, including by enabling temporary cross-border testing arrangements and harmonised test methods. We also suggest clarifying the exact scope of the biennial

testing requirement and considering its alignment with existing eIDAS certification and reassessment cycles to avoid unnecessary duplication.

6) The use case of using electronic signatures for PID on-boarding is implicitly allowed since this is specified in ETSI TS 119 461 v2.1.1 (identity proofing) clauses 8.2.5 and 8.3.5.

This may open a security breach, if the QES is created with QCs issued under eIDAS1 using eID LoA Substantial or under eIDAS2 with fully automated identity proofing.

Proposed change: Restrict the CIR Annex such that ETSI TS 119 461 v2.1.1 clauses 8.2.5 and 8.3.5 on electronic signatures are not allowed for PID on-boarding.

CEN TS 18098 (PID on-boarding) does not allow for electronic signatures for PID on-boarding. When the CEN TS 18098 has been published, this standard could also be referenced by the CIR Annex.

7) For security reasons, it is recommended to use a different IPSP (Identity Proofing Service Provider) for the additional remote identity proofing, than was initially used when issuing the eID means at LoA Substantial.

If the same IPSP is used twice at LoA Substantial, this will not increase the security for the PID on-boarding. However, if a different IPSP at LoIP Extended is used, this can be used to increase the security to LoA High for the PID on-boarding.

Proposed change: Update the CIR Annex with a requirement that a different IPSP at LoIP Extended must be used for the additional remote identity proofing, than was initially used when issuing the eID means at LoA Substantial.

CEN TS 18098 (PID on-boarding) requires a different IPSP at LoIP Extended to be used than the initial identification for eID at LoA Substantial. When the CEN TS 18098 has been published, this standard could also be referenced by the CIR Annex.