# Stellungnahme/Comments

Proposal for a
REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL amending Regulation (EU) No 910/2014 as regards establishing a framework for a European Digital Identity

Register of Interest Representatives
Identification number in the register: 52646912360-95

Our ref
Ref. DK: ES
Ref. DSGV:8528

Contact: Tim Kremer, Oliver Lauer
Telephone: +49 30 20225- 5314, - 5531
Telefax: +49 30 20225- 5345
E-Mail: tim.kremer@dsgv.de, oliver.lauer@dsgv.de

Berlin, September 2, 2021

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-sector 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 more than 1,700 banks.

Coordinator:
German Savings Banks Association
Charlottenstraße 47 | 10117 Berlin | Germany
Telephone: +49 30 20225-0
Telefax: +49 30 20225-250
www.die-deutsche-kreditwirtschaft.de

## Zusammenfassung

Die Deutsche Kreditwirtschaft unterstützt und begrüßt die Zielsetzung der Verordnung, notwendige Rahmenbedingungen für die weitere Digitalisierung von öffentlichen und privaten Dienstleistungen bzw. Geschäftsprozessen in der EU zu schaffen. Die Einführung von EUid-Wallets bietet die Chance, wettbewerbsfähige und regulatorisch anerkannte Identitäts-Ökosysteme in Europa zu etablieren, die auf breite Akzeptanz sowohl im öffentlichen, als auch im privaten Sektor hoffen lassen.

Zur Schaffung von Rechts- und Planungssicherheit und zum Erhalt der Innovationsfähigkeit der europäischen Wirtschaft besteht in Bezug auf nachfolgende Punkte des Verordnungsvorschlags weiterer Klärungsbedarf:

- Die Chancen, Rollen und Verantwortungen der Privatwirtschaft in einem neuen Identitäts-Ökosystem, insbesondere in Abgrenzung zur der öffentlichen Hand, bedürfen unseres Erachtens einer Präzisierung.
- Eine mögliche Akzeptanzpflicht der EUid-Wallet darf sich nur auf einen einzigen Schnittstellenstandard beziehen. Bei Vorliegen von mehreren Lösungen müssen diese schnittstellenkompatibel sein, um eine möglichst große Reichweite zu erzielen.
- Die mögliche Akzeptanzpflicht der EUid-Wallet darf nicht dazu führen, dass Sicherheitsrisiken oder Widersprüche zu anderen regulatorischen Vorgaben entstehen (wie z.B. PSD2, GDPR)
- Das Haftungsregime muss vor Inkrafttreten der Verordnung geregelt sein.
- Die Finanzierung der notwendigen Infrastruktur für eine EUid muss vor Inkrafttreten der Verordnung geregelt sein. Den Beteiligten muss ein Business Case ermöglicht werden.
- Die Meilensteine dürfen nicht allein auf das Inkrafttreten der eIDAs-Verordnung abstellen, sondern auf das Erreichen der dort enthaltenen und jeweils vorgelagerten Meilensteine. Nach unserer Erfahrung in der Finanzindustrie erscheinen die Fristen der Meilensteine als zu kurz. Die Fristen sollen auch nicht in der Verordnung selbst festgeschrieben werden.
- Alle wesentlichen Aspekte (z.B. Haftung und Governance) sollen in der eIDAS-Verordnung selbst geregelt und nicht in RTS oder Delegated Acts ausgelagert werden.

## Im Einzelnen

I. Zur Rolle von Kreditinstituten:

Es muss unseres Erachtens verpflichtend sein, dass bei Erfüllung der einheitlichen europäischen Zertifizierungskriterien auch privatwirtschaftliche ID Wallet Lösungen von den Mitgliedsstaaten anzuerkennen sind.

Um eine breite Akzeptanz des EUid-Ökosystems zu erreichen, müssen Kreditinstitute aktiv in die Entwicklung einer EUid eingebunden werden. Für die Integration der EUid in neue oder bestehende Kundenbeziehungen müssen wirtschaftliche Anreize ermöglicht werden. Dies können beispielsweise bepreisbare Mehrwertdienste sein.

Kreditinstitute müssen als vertrauende Partei (Relying Party) auch aktiv eine EUid-Wallet-Funktion in ihre bestehenden Banking Apps integrieren und mit diesen herausgeben dürfen. Ob die im Entwurf der Verordnung enthaltene verpflichtende physikalische und logische Trennung dies erlaubt, ist uns bisher

unklar und sollte konkretisiert werden. Zudem müssen Kreditinstitute sich unter Berücksichtigung der für Banken bestehenden Regulatorik als qualifizierter Vertrauensdienst anerkennen lassen können, um Credentials und Attribute in der Wallet qualifiziert bescheinigen zu dürfen.

II. Zur verpflichtenden Akzeptanz der EUid-Wallet für den privaten Sektor:

Die verpflichtende Akzeptanz der EUid-Wallet, z.B. für die PSD II-konforme Authentifizierung, erachten wir dann als kritisch, wenn Kreditinstitute Sicherheitsrisiken der Software- und Hardwareumgebung in Kauf nehmen müssen, auf die sie keinen Einfluss nehmen können. Ein Kreditinstitut darf beispielsweise nicht verpflichtet werden, Authentifizierungen über die EUid-Wallet auf einem Betriebssystem durchzuführen, welches nach eigenen Richtlinien als risikobehaftet gilt.

Aus dem aktuellen Entwurf wird nicht ersichtlich. wer im Fall unzureichender Sicherheit für resultierende Schäden haften muss. Eine Haftung besteht nach unserem Verständnis nur für notifizierte eID-Systeme in einem grenzüberschreitenden Kontext zwischen den Mitgliedsstaaten; vgl. Art. 11. Es fehlt jedoch ein nationales Haftungsregime für Schäden im Zusammenhang mit der EUid-Wallet. Es besteht das Bedürfnis für eine **klare Regelung der Haftung für alle involvierten Parteien**.

Es muss im Weiteren sichergestellt sein, dass die Kreditinstitute durch die Nutzung des EUid-Ökosystems **nicht in Widerspruch zu anderen geltenden Regularien** stehen. Falls die EUid-Wallet beispielsweise im Rahmen der Prozesse einer starken Kundenauthentifizierung genutzt werden soll, muss sichergestellt werden, dass dann bei diesem EUid-Wallet basierten SCA-Verfahren alle Anforderungen der Delegierten Verordnung (EU) 2018/389 (RTS zur PSD2) erfüllt werden können. Insbesondere die für die Sicherheit elementaren dynamischen Sicherheitselemente müssten damit als Grundvoraussetzung auch in der Wallet zur Verfügung gestellt werden.

Soweit privatwirtschaftliche Anbieter zum Angebot ihrer Services in EUid-Wallets, z.B. im Rahmen der starken Kundenauthentifizierung, verpflichtet sind, muss auch gewährleistet sein, dass sie ihre **ID-Merkmale kostenlos einbringen und validieren** können. Die Anbieter müssen dabei wählen können, wie sie die Wallet unterstützen, etwa durch Auswahl der auszugebenden eigenen Credentials.

Die Anforderungen an eine physische und logische Trennung von Daten im Kontext der Anwendung einer neuen eIDAS (6a und 45f). im Bankenumfeld bedarf einer Präzisierung. Die aktuellen Formulierungen können zu Auslegungsproblemen führen. Eine Orientierung an der PDS2 erscheint auch hier vorteilhaft (vgl. Art. 9 RTS PSD2).

Die Regelungen der Verordnung sollten sich ausschließlich auf die in der vorliegenden Verordnung definierten, qualifizierten ID-Services beziehen. Hierzu ist eine Klarstellung zum Anwendungsbereich wünschenswert, um eine unbeabsichtigte Ausstrahlung auf andere Transaktionen, z. B. im Zahlungsverkehr, auszuschließen.

Dieses gilt insbesondere auch für die Gleichstellung von Offline-Authentifizierungen mit Online-Authentifizierungen. Insbesondere im Payment im Präsenzgeschäft ist eine solche Verpflichtung mit massiven Auswirkungen und Investitionen auf die gesamte Akzeptanzstruktur für Kartenzahlungen verbunden. Zusätzlich steigen die Anforderungen an das ID-Wallet-System exponentiell, da seit Einführung der Chips alle Karten dynamische Sicherheitsmerkmale aufweisen, die in den bekannten Wallet-basierten ID-Systemen bisher nicht vorgesehen bzw. realisiert sind und zunächst spezifiziert und entwickelt werden müssten. Ferner würde eine Ausweitung auf offline-Autorisierungen sämtliche stationären SB-Komponenten der Logistik- (z.B. Paketstationen), Mineralöl- (Tankkarten, Kundenkarten), Finanzbranche (SB-Geräte in Bankstellen, Zutritt außerhalb Öffnungszeiten), etc. betreffen.

Es sollte klargestellt werden, dass die Anforderungen der eIDAS sich ausschließlich auf **qualifizierte** Services beziehen, um eine unterschiedliche Auslegung in den Mitgliedstaaten zu verhindern.

Für die Dienstleistungen, die nicht unmittelbar mit der digitalen Identität verbunden sind, sollten keine neuen Anforderungen durch die Verordnung geschaffen werden, um eine ungewollte Anwendbarkeit anderer Regularien wie z.B. BaIT, GOBs, etc. zu vermeiden. Eine Ausweitung auf alle elektronischen Archivierungssysteme hätte weitere unnötige Auswirkungen auf IT-Dienstleister, die Steuerberatenden Berufe, Krankenhäuser usw. da dort überall Archivierungsservices unterhalten und den Mandanten entweder im Rahmen von Zusammenarbeitsmodellen oder gegen Entgelt angeboten werden.

III. Interoperabilität:

Alle Mitgliedsstaaten sollen verpflichtet werden, innerhalb von 12 Monaten nach Inkrafttreten der Verordnung ihren Bürgern und Unternehmen mindestens eine nationale EUid-Wallet zur Verfügung zu stellen. In den einzelnen Mitgliedsstaaten werden hierfür aktuell unterschiedliche technischen Lösungsansätze verfolgt.

Es sollte gewährleistet werden, dass vertrauende Parteien für jede nationale EUid-Wallet nur eine gemeinsame, standardisierte Schnittstelle implementieren müssen, insbesondere dann, wenn eine Pflicht zur Anerkennung besteht. Die Akzeptanzpflicht der EUid-Wallet sollte sich daher nur auf diese eine einzige Schnittstelle beziehen.

Vor diesem Hintergrund und dem Grad des aktuellen Detailswissens erscheint der vorgelegte Zeitplan, wonach die Mitgliedsstaaten EUid-Wallets innerhalb von zwölf Monaten auf Basis eines noch zu erarbeitenden Standards anbieten müssen, sehr herausfordernd. Diese neuen Standards sollen zudem erst in einer Konsultationsphase mit den Marktteilnehmern abgestimmt werden. Erst nach Vorliegen der Spezifikationen für die wallet kann aus Sicht der Finanzwirtschaft eine realistische Schätzung des für die Umsetzung erforderlichen Zeitrahmens vorgenommen werden.

IV. Finanzierung des Ökosystems:

Der Entwurf äußert sich nicht dazu, wie Investitions- und Betriebskosten der notwendigen Infrastruktur finanziert werden. So wird nicht erwähnt, wie bzw. durch wen die Umsetzungsarbeiten finanziell getragen werden sollen.

Ein innovationsfördernder Rahmen, welcher auch tragfähige Geschäftsmodelle erlaubt, sollte beschrieben und definiert werden. Die Verordnung sieht bisher lediglich vor, dass Verbraucher für die Nutzung der EUid-Wallet keine Entgelte zahlen sollen. Es ist jedoch unklar, inwieweit einzelne Dienstleistungen im Zusammenhang mit einer Wallet monetarisiert werden können. Hierfür wären ggf. frühzeitig Möglichkeiten zur Umsetzung von positiven Business Cases zu schaffen. Ferner ist die Formulierung zu breit gewählt. Die Übernahme von Credentials in die Wallet ist ein Teil der Nutzung. Mit dem Ziel, heutige papierhafte Credentials im vollständig zu digitalisieren, würden damit sowohl Preise für Bankprodukte (Beispiel Karten), Bescheinigungen (Beispiel Bankauskunft / Bonität) mit einem Mehrwert für den Kunden, als auch Entgelte/Gebühren (Ausgabe Personalausweis) verboten sein.

Die Ausgabe einer EUid-Wallet durch Kreditinstitute muss vom jeweiligen Mitgliedsstaat anerkannt werden; vgl. Art. 6a. Daher darf es nicht zu Wettbewerbsverzerrungen aufgrund des Unternehmenssitzes kommen, z. B. in Abhängigkeit von einer staatlichen oder privaten Lösung.

Die bisher schon am Markt existierenden kommerziellen Identifizierungslösungen dürfen im Wettbewerb nicht behindert werden. Sie müssen in der eIDAS-VO als gleichberechtigt gelten, sofern sie entsprechende Kriterien erfüllen.

Alle Anbieter, die Anwendungen in der Wallet betreiben, müssen **nach europaweit einheitlichen Maßstäben zertifiziert** werden. Privatwirtschaftliche Anbieter und staatliche Stellen müssen in ganz Europa gleichbehandelt und nach denselben Maßstäben zertifiziert werden, gleich in welchem Land die Zertifizierungsstelle ihren Sitz hat. Dieses kann unseres Erachtens am besten durch eine zentrale, für die gesamte EU zuständige Zertifizierungsstelle erreicht werden.

CONVENIENCE TRANSLATION

Summary

The German banking industry supports and welcomes the objective of the regulation to create the necessary framework conditions for the further digitalisation of public and private services and business processes in the EU. The introduction of EUid wallets offers the opportunity to establish competitive and regulatory-recognised identity ecosystems in Europe, which are expected to be widely accepted in both the public and the private sector.

In order to create legal and planning certainty and to maintain the innovative capacity of the European economy, there is a need for further clarification with regard to the following points of the proposed regulation:

- In our opinion, the opportunities, roles and responsibilities of the private sector in a new identity ecosystem, especially in contrast to the public sector, need to be specified.
- A possible obligation to accept the EUid wallet must only refer to a single interface standard. If several solutions are available, they must be interface-compatible in order to achieve the widest possible reach.
- The possible acceptance obligation of the EUid wallet must not lead to security risks or contradictions with other regulatory requirements (such as PSD2, GDPR).
- The liability regime must be established before the regulation enters into force.
- The financing of the necessary infrastructure for an EUid must be adressed before the regulation enters into force. The stakeholders must be enabled to develop a business case.
- The milestones must not be based solely on the entry into force of the eIDAs Regulation, but on the achievement of the milestones contained therein and the respective upstream milestones. In our experience in the financial industry, the deadlines for the milestones appear to be too short. The deadlines should also not specified in the regulation itself.
- All essential aspects (e.g. liability and governance) should be regulated in the eIDAS Regulation itself and not be outsourced to RTS or Delegated Acts.

## In detail

I. On the role of credit institutions:

In our opinion, it must be obligatory for private-sector ID wallet solutions to be recognised by the member states if the uniform European certification criteria are met.

In order to achieve broad acceptance of the EUid ecosystem, credit institutions must be actively involved in the development of an EUid. Economic incentives must be made possible for the integration of the EUid into new or existing customer relationships. These can be, for example, value-added services that can be monetarized.

Credit institutions must also be allowed to actively integrate an EUid wallet function into their existing banking apps as a relying party and issue it with them. Whether the mandatory physical and logical separation contained in the draft regulation allows this is unclear to us so far and should be specified. In addition, credit institutions must be able to be recognised as a qualified trust service, taking into account the existing regulatory framework for banks, in order to be allowed to certify credentials and attributes in the wallet in a qualified manner.

II. on the mandatory acceptance of the EUid wallet for the private sector:

We consider the mandatory acceptance of the EUid wallet, e.g. for PSD II-compliant authentication, to be problematic if credit institutions have to accept security risks of the software and hardware environment over which they have no influence. For example, a credit institution must not be obliged to carry out authentications via the EUid wallet on an operating system that is considered risky according to its own guidelines.

It is not clear from the current draft who is liable for any resulting damage in the event of insufficient security. As we understand it, liability only exists for notified eID systems in a cross-border context between member states; cf. Art. 11. However, there is no national liability regime for damages in connection with the EUid wallet. There is a need for a clear regulation of liability for all parties involved.

Furthermore, it must be ensured that credit institutions do not contradict other applicable regulations by using the EUid ecosystem. If, for example, the EUid wallet is to be used as part of the processes of strong customer authentication, it must be ensured that all requirements of Delegated Acts (EU) 2018/389 (RTS on PSD2) can then be fulfilled in this EUid wallet-based SCA process. In particular, the dynamic security elements that are elementary for security would also have to be made available in the wallet as a basic requirement.

Insofar as private sector providers are obliged to offer their services in EUid wallets, e.g. within the framework of strong customer authentication, it must also be ensured that they can introduce and validate their ID features free of charge. In doing so, providers must be able to choose how they support the wallet, for example by selecting their own credentials to be issued.

The requirements for a physical and logical separation of data in the context of the application of a new eIDAS (6a and 45f) in the banking environment require clarification. The current wording can lead to interpretation problems. Orientation towards PDS2 seems advantageous here, too (cf. Art. 9 RTS PSD2).

The provisions of the regulation should refer exclusively to the qualified ID services defined in the present regulation. A clarification of the scope of application is desirable in order to exclude an unintended impact on other transactions, e.g. payment transactions.

This also applies in particular to the equivalence of offline authentications with online authentications. Such an obligation would have a massive impact on the entire acceptance structure for card payments

and require large investments, especially with regard to payments at the Point of Sale. In addition, the requirements for the ID wallet system increase exponentially, as, since the introduction of chips, all cards include dynamic security features that are not yet provided or realised in the known wallet-based ID systems and would first have to be specified and developed. Furthermore, an extension to offline authorisation would affect all stationary self-service components in the logistics (e.g. parcel stations), petroleum (fuel cards, customer cards), financial (self-service devices in bank branches, access outside opening hours), etc. sectors.

It should be clarified that the requirements of the eIDAS refer exclusively to qualified services in order to prevent different interpretations in the Member States.

For services not directly related to digital identity, no new requirements should be created by the regulation in order to avoid unintended applicability of other regulations such as BaIT (German Prudential Guidelines on IT, implementing the EBA Guidelines on ICT and Security Risk Management), GOBs (Principles of proper computerised accounting systems), etc. An extension to all electronic archiving systems would have further unnecessary effects on IT service providers, the tax advisory professions, hospitals, etc., as archiving services are maintained everywhere and are partly offered either against payment to clients or within the framework of cooperation models.

III. Interoperability:

All member states are to be obliged to make at least one national EUid wallet available to their citizens and businesses within 12 months of the regulation coming into force. Different technical approaches are currently being pursued in the individual member states.

It should be ensured that relying parties only have to implement a common, standardised interface for each national EUid wallet, especially if there is an obligation to accept it. The EUid wallet acceptance obligation should therefore only relate to this single interface.

Against this background and the level of current detailed knowledge, the timetable presented, according to which the member states must offer EUid wallets within twelve months on the basis of a standard yet to be developed, seems very challenging. Moreover, these new standards are to be agreed with the market participants only in a consultation phase. In our view, a realistic estimate of the time frame required for implementation can only bemade after the specifications for the wallet are available.

IV. Financing of the ecosystem:

The draft does not comment on how the investment in and operating costs of the necessary infrastructure will be financed. It is not mentioned how or by whom the implementation work is to be financed.

An innovation-promoting framework, which also allows for sustainable business models, should be described and defined. So far, the regulation only stipulates that consumers should not pay any fees for the use of the EUid wallet. However, it is unclear to what extent individual services in connection with a wallet can be monetarised. If necessary, opportunities for the implementation of positive business cases would have to be created at an early stage. In this regard, the wording is too broad. The transfer of credentials to the wallet is part of the use. With the goal of completely digitising today's paper-based credentials, this would prohibit prices for bank products (e.g. cards), certificates (e.g. bank information/creditworthiness) with added value for the customer, as well as fees (issuing ID cards).

The issuance of an EUid wallet by credit institutions must be recognised by the respective member state; cf. Art. 6a. Therefore, there must be no distortion of competition based on the location of the company, e.g. depending on a governmental or private solution.

The commercial identification solutions already existing on the market must not be hindered in competition. They must be considered as equal in the eIDAS Regulation, provided they fulfil the corresponding criteria.

All providers who operate applications in the wallet must be certified according to uniform standards throughout Europe. Private providers and government bodies must be treated equally throughout Europe and certified according to the same standards, regardless of the country in which the certification body is based. In our opinion, this can best be achieved by a central certification body responsible for the entire EU.