

Warum die Akzeptanz der EU Digital Identity Wallet für SCA nach eIDAS2 verpflichtend wäre

Anmerkungen aus rechtlicher Sicht

Discussion Paper Version 1.0 (November 20, 2023)

Christian Lange-Hausstein,¹ Tim Kremer¹

Kontext

[1] In diesem Papier setzen wir uns mit der Frage auseinander, welche Pflicht die kommende eIDAS2 zur Akzeptanz der EU Digital Identity Wallet (nachfolgend: „EUDIW“) für europäische Zahlungsdienstleister enthält. Das halten viele für unklar (siehe Rn. 7 ff.). Investitionsentscheidungen der Europäischen Kreditwirtschaft müssten ohne eine Klarstellung (siehe Rn. 40 und 41) unter Unsicherheit getroffen werden.

[2] Am 8. November 2023 beendeten das Europäische Parlament und der Rat die Trilogverhandlungen über die eIDAS2-Verordnung.² Bis heute sind diverse gesellschaftlich relevante Aspekte umstritten.³ Unabhängig davon hat das

¹ Die Autoren sind Rechtsanwälte und Syndikusanwälte im Digitallabor des DSGVO. Das Digitallabor bewirbt sich beim Bundesministerium des Innern für die Umsetzung der EUDIW in Deutschland und ist in den eIDAS2 Large Scale Pilots NOBID und Potential sowie in der Testphase für den Digitalen Euro aktiv.

² https://ec.europa.eu/commission/presscorner/detail/en/IP_23_5651.

³ *Heeger*, Tagesspiegel Background zu eIDAS Trilog, 7. November 2023; zu den abgeschafften Unique Identifiern siehe: *Schroers*: A Unique Identification Number for Every European Citizen: The Proposal for a European Digital Identity Regulation and What it Entails, VerfBlog, 2023/2/24, <https://verfassungsblog.de/digital-id-eu/>, DOI: 10.17176/20230224-185228-0; zudem: *Breyer*, European Digital Identity: Permanent personal identification number is off the table!, 30. Juni 2023; <https://www.patrick-breyer.de/en/european-digital-identity-permanent-personal-identification-number-is-off-the-table/>; zu QWACS u.a. siehe: Joint statement of scientists and NGOs on the EU’s proposed eIDAS reform idF vom 2. November 2023, abrufbar unter: <https://nce.mpi-sp.org/index.php/s/cG88cptFdaDNyRr>.

Bundesministerium des Innern am selben Tag auf der Smart Country Convention die deutsche Version der EUDIW für das 1. Quartal 2027 angekündigt. Im Q&A der EU-Kommission zum Verhandlungsende heißt es in der Antwort auf die Frage, „What can users do with the new EU Digital Identity Wallet?“:

“Users will be able to use it to authenticate digitally when logging into both public and private online services across the EU, or authorise online transactions, in particular where strong user authentication is required. Examples of these could be accessing a bank account, initiating a payment (...)”⁴

Die EU-Kommission teilt auch in einer Pressemitteilung mit, „(...) the Wallet will allow users to open bank accounts, make payments (...)“.⁵

[3] Für Teile der Europäischen Kreditwirtschaft ist das allerdings nicht so eindeutig. Sie diskutieren eine Unklarheit des Verordnungstextes, die Investitionsentscheidungen erheblich erschwere. Die europäischen Bankenverbände haben sich noch einen Tag vor dem Ende der Verhandlungen – *im Ergebnis erfolglos* - an Parlament und Kommission gewendet, um eine Klarstellung im Verordnungstext zu erreichen.⁶

[4] Die Verbände legten dar, dass sich aus dem Verordnungstext der eIDAS2 nicht eindeutig ergebe, ob Zahlungsdienstleister verpflichtet sind, die EUDIW zum Zwecke der starken Kundenauthentifizierung (nachfolgend: „SCA“) bei Zahlungen und sonstigen SCA-relevanten Fällen zu akzeptieren.

[5] Für das Vorhaben des Gesetzgebers kann diese Unsicherheit zum Problem werden. Denn sein Ziel, die umfassende Marktdurchdringung der EUDIW in Europa, ist nach den bereits in Skandinavien gemachten Erfahrungen mit digitalen Identitäten ohne Banken deutlich schwerer zu erreichen.⁷

Zusammenfassung

[6] Der Verordnungstext enthält in seiner aktuellen Fassung viele Anhaltspunkte dafür, dass eine Pflicht der Zahlungsdienstleister geregelt werden soll, die EUDIW zum Zwecke der SCA bei Zahlungen und Online-Banking Logins zu akzeptieren.

⁴ https://ec.europa.eu/commission/presscorner/detail/en/QANDA_21_2664.

⁵ https://ec.europa.eu/commission/presscorner/detail/en/ip_23_5651.

⁶ <https://www.ebf.eu/ebf-media-centre/ecsas-call-for-clarity-on-the-application-of-sca-obligations-to-payments-under-eidas-2-0/>.

⁷ Podcast Lage der Nation, Folge 355 vom 2. November 2023, ab Minute 39.

Das ergibt sich aber nicht nur aus dem eIDAS2-Text, sondern auch aus dem PSR-Entwurf und aus dem Entwurf für eine Verordnung über den Digitalen Euro. Eine Präzisierung der eIDAS2 würde Restunsicherheit beseitigen. Je nachdem, was der Gesetzgeber anstrebt, genügt die Streichung von zwei Worten (siehe unten Rn. 40 und 41).

Unklar: Was ist “strong user authentication for online identification”?

[7] Die finale Fassung des Verordnungstextes der eIDAS2 wurde noch nicht veröffentlicht. In der Fassung, die dem „Provisional Agreement“ zur eIDAS2 vom 8. November 2023 zugrunde liegt (nachfolgend: „eIDAS2-PA“), heißt es unter der Überschrift „Cross-border reliance on European Digital Identity Wallets“⁸ in Art. 6 db:

“2. Where private relying parties providing services, with the exception of microenterprises and small enterprises as defined in Commission Recommendation 2003/361/EC, are required by national or Union law to use strong user authentication for online identification or where strong user authentication for online identification is required by contractual obligation, including in the areas of transport, energy, banking, financial services, social security, health, drinking water, postal services, digital infrastructure, education or telecommunications, private relying parties shall, no later than 36 months after the entry into force of the implementing acts referred to in [Article 6a] paragraph 11 and Article 6c(4)] and strictly upon voluntary request of the user, also accept the use of European Digital Identity Wallets provided in accordance with this Regulation.” (Hervorhebungen hinzugefügt)

[8] Zunächst gilt: Aus dem Standort der Regelung im Abschnitt „Cross-border reliance on European Digital Identity Wallets“ ergibt sich keine Beschränkung der Akzeptanzverpflichtung auf grenzüberschreitende Vorgänge. Der Regelungstext enthält kein Tatbestandsmerkmal, das das stützen würde. Es wäre – praktisch – auch dieselbe Wallet, mit der Personen Nutzungsvorgänge innerhalb von Mitgliedstaaten und zwischen ihnen durchführen würden.

⁸ Provisional Agreement vom 8. November 2023: <https://www.europarl.europa.eu/committees/en/european-digital-identity-provisional-ag/product-details/20231116CAN72103>.

[9] Zahlungsdienstleister, die „private relying parties“ sind, müssen die EUDIW akzeptieren, wenn sie nach europäischen oder nationalen Vorschriften zur „*strong user authentication for online identification*“ verpflichtet sind.

[10] Zahlungsdienstleister sind *private relying parties*, denn sie vertrauen auf die identitätsbezogenen Informationen. – Aber sind sie auch zur „*strong user authentication for online identification*“ verpflichtet?

“Strong user authentication” entspricht “strong customer authentication”

[11] Damit ist aus der Sicht von Zahlungsdienstleistern zunächst klärungsbedürftig, was unter „strong user authentication“ zu verstehen ist. Nach Art. 97 Abs. 1 PSD2 sind Zahlungsdienstleister nämlich nicht zur strong *user authentication* verpflichtet, sondern zur strong *customer authentication*. Das wird ab der künftig geltenden PSR auch so sein (Art. 85 Abs. 1 PSR-Entwurf).

[12] Die Definition der „strong user authentication“ im eIDAS2-PA entspricht allerdings ganz wesentlich der Definition der „strong customer authentication“ in der PSD2 bzw. künftig der PSR (Art. 3 lit. i (50) eIDAS2-PA; Art. 4 (30) PSD2 bzw. künftig Art. 3 Nr. 35 PSR-Entwurf). Beide Definitionen stellen darauf ab, dass mindestens zwei Elemente bzw. Faktoren der Kategorien Wissen, Besitz und Inhärenz genutzt werden, die insofern voneinander unabhängig sind, als die Nichterfüllung eines Kriteriums die Zuverlässigkeit der anderen nicht in Frage stellt. Deshalb kann davon ausgegangen werden, dass der eIDAS2-Gesetzgeber vergleichbare Vorgänge meinte.

[13] Das wird auch gestützt dadurch, dass der Begriff *user* kein Vertragsverhältnis erfordert und damit weiter ist als der Begriff *customer*, letzterer also mitgemeint ist.

[14] Die Begriffserweiterung gegenüber dem Zahlungsverkehrsrecht ist auch deshalb erforderlich, weil die eIDAS2 auch die Digitalisierung der Verwaltung unterstützen soll, in der regelmäßig keine Vertragsverhältnisse zwischen Bürger und Staat bestehen.

Hat „for online identification“ eine eigenständige Bedeutung?

[15] Auslegungsbedürftig ist allerdings, was unter dem Tatbestandsmerkmal „for online identification“ zu verstehen ist, das der Gesetzgeber anfügt („strong user authentication for online identification“). Drei Möglichkeiten sind erkennbar:

- [16] Enges Verständnis: Der Verordnungsgeber könnte mit „strong user authentication for online identification“ meinen, dass Zahlungsdienstleister nur dann zur Nutzung der EUDIW verpflichtet sein sollen, wenn sie eine SCA zur bloßen Identifizierung der Person einsetzen.

Folge: Dann wäre die Akzeptanzpflicht der EUDIW auf SCA-Vorgänge begrenzt, die der Identifizierung dienen – bspw. die Identifizierung nach geldwäsche-rechtlichen Vorschriften. Die Akzeptanzpflicht wäre damit auf eine Kernfunktion der EUDIW beschränkt. Eine Akzeptanzpflicht der EUDIW bei der Nutzung der SCA bei Zahlungen oder Online-Banking-Logins bestünde nach diesem Verständnis nicht.

- [17] Hybrid-Verständnis: Der Verordnungsgeber könnte mit „strong user authentication for online identification“ auch meinen, Zahlungsdienstleister sollen zur Akzeptanz der EUDIW verpflichtet sein in Fällen, in denen sie zur SCA verpflichtet sind und er könnte die Verpflichtung auf den Teil der SCA beschränken wollen, der die Identifizierung der Person betrifft.

Folge: Dann wäre für die Identifizierungskomponente einer SCA bei der Freigabe einer Zahlung oder bei dem Login in das Online-Banking auch die EUDIW zu akzeptieren und noch ein weiteres Instrument für die weiteren Komponenten hinzuziehen.

- [18] Weites Verständnis: Der Verordnungsgeber könnte mit „strong user authentication for online identification“ meinen, Zahlungsdienstleister sollen zur Akzeptanz der EUDIW verpflichtet sein in Fällen, in denen sie zur SCA verpflichtet sind – ohne die Akzeptanzpflicht auf einen Teil der SCA beschränken zu wollen.

Folge: Dann wäre für die vollständige SCA bei der Freigabe einer Zahlung oder bei dem Login in das Online-Banking auch die EUDIW zu akzeptieren.

Enges Verständnis ist fernliegend

[19] Gegen das enge Verständnis spricht zunächst, dass es keine isolierte “strong user authentication for online identification” gibt. Die Gründe, aus denen SCA durchzuführen ist, nennt der Gesetzgeber in Art. 97 Abs. 1 PSD2 (bzw. Art. 85 Abs. 1 PSR). Die bloße Identifizierung gehört nicht dazu. Wenn der Gesetzgeber nur Zahlungsdienstleister erfassen wollte, die SCA für Identifizierungen benutzen,

würde er im Ergebnis niemanden verpflichten. Bestandteil der SCA ist mit der Authentisierung zwar stets ein identifizierendes Element.⁹ Die Identifizierung ist aber nicht Selbstzweck, sondern wird benötigt im Zusammenhang mit einem weiteren Vorgang, etwa der Zustimmung zu einer Zahlung (Autorisierung) oder dem Login.¹⁰ Die „reine“ Identifizierung, z.B. aus geldwäscherechtlichen Gründen, richtet sich nicht nach den Vorgaben für eine SCA, sondern nach jenen des Geldwäscherechts für die Identifizierung einer Person, so dass bei einem engen Verständnis kein praktischer Anwendungsfall mehr denkbar wäre.

Hybrid-Verständnis ist fernliegend

[20] Gegen das Hybrid-Verständnis spricht die Grammatik der Formulierung „strong user authentication *for online identification*“. Nach dem reinen Textverständnis spricht der Satz von einer SCA für Identifizierungen. Es gibt aber keine Identifizierung, die eine SCA-Komponente hat (siehe zuvor). Es gibt vielmehr nur SCA-Vorgänge, die eine Komponente der Identifizierung haben. Es ist anzunehmen, dass der Ordnungsgeber deutlicher zum Ausdruck gebracht hätte, wenn er nur die identifizierende Komponente der SCA meinen würde.

Erwägungsgrund 31 stützt weites Verständnis

[21] Die Erwägungsgründe (EG) sprechen für ein weites Verständnis.¹¹ In EG 31 des eIDAS2-PA heißt es:

„Secure electronic identification and the provision of attestation of attributes should offer additional flexibility and solutions for the financial services sector to allow identification of customers and the exchange of specific attributes necessary to comply with, for example, customer due diligence requirements under the Anti Money Laundering Regulation, [reference to be added after the adoption of the proposal], with suitability requirements stemming from investor protection legislation, or to support the fulfilment of strong customer authentication requirements for online identification for the purpose of account login and initiation of transactions in the field of payment services.“ Hervorhebungen hinzugefügt.

[22] EG 31 stützt ein weites Verständnis der Verpflichtung zur Akzeptanz der EUDIW sowohl zu Identifizierungs-, als auch zu den SCA-Zwecken Login und Transaktionsfreigabe.

⁹ Im Einzelnen: Casper/Terlau/Zahrte, 3. Aufl. 2023, ZAG § 55 Rn. 2, 3.

¹⁰ Zur künftigen Rechtslage: Art. 3 Nr. 34 PSR-Entwurf. Identisch mit Art. 4 (29) PSD2

¹¹ Provisional Agreement vom 8. November 2023:

<https://www.europarl.europa.eu/committees/en/european-digital-identity-provisional-ag/product-details/20231116CAN72103>.

[23] Denn der Verordnungsgeber füllt das Tatbestandsmerkmal „for online identification“ konkret aus, indem er die Beispiele „account login“ und „transactions“ als Zwecke („purpose“) der Vorgänge nennt.

[24] Zudem zählt er „customer due dilligence“ und „the fulfilment of strong customer authentication requirements for online identification for the purpose of account login and initiation of transactions“ gleichrangig hintereinander auf. Das wäre nicht schlüssig, wenn er das Verständnis zugrunde legen würde, dass mit SCA „for online identification“ nur Vorgänge der Identifizierung gemeint wären. Denn unter „customer due dilligence“ ist die geldwäscherechtliche Identifizierung gemeint, sodass der Verordnungsgeber zweimal das gleiche aufzählen würde.

Erwägungsgrund 28 stützt weites Verständnis

[25] EG 28 der Entwurfsfassung aus November 2023 wiederholt im Wesentlichen den Wortlaut von Art. 6 db Abs. 2 eIDAS2-PA, setzt diesen aber vorweg in einen konkreten Kontext:

„The wide availability and usability of EDIWs should rely on their acceptance and trust by both private individuals and private service providers. Therefore, private relying parties providing services such as in the areas of transport, energy, banking and financial services, social security, health, drinking water, postal services, digital infrastructure, telecommunications or education should accept the use of EDIWs for the provision of services where strong user authentication for online identification is required by Union or national law or by contractual obligation.“
(Hervorhebungen hinzugefügt)

[26] Es wäre geradezu widersinnig, wenn die Abwicklung von Zahlungen als die mit großem Abstand am häufigsten genutzte Dienstleistung im Finanzsektor nicht erfasst würde. Das Bezahlen hat in besonderer Weise das Potential, die EUDIW zu einem Teil des täglichen Lebens der europäischen Bürgerinnen und Bürger zu machen.

Weites Verständnis genügt methodischen Anforderungen des EuGH an Hinzuziehung der Erwägungsgründe

[27] Ein weites, auf die Erwägungsgründe gestütztes Verständnis der Akzeptanzpflicht der EUDIW muss den methodischen Anforderungen des EuGH an die Hinzuziehung von Erwägungsgründen zur Auslegung genügen.

[28] Erwägungsgründe haben keine rechtliche Bindungswirkung. Wörtlich führte der EuGH¹² aus, es

“...should be borne in mind that the preamble to a Community act has no binding legal force and cannot be relied on either as a ground for derogating from the actual provisions of the act in question or for interpreting those provisions in a manner clearly contrary to their wording“ (Hervorhebung hinzugefügt).

[29] Gleichwohl können die Erwägungsgründe herangezogen werden, um die eigentlichen Bestimmungen eines Rechtsakts zu ermitteln.¹³

[30] Es ist also danach zu fragen, ob ein weites Verständnis des Begriffs „online identification“ auf der Grundlage der Erwägungsgründe eine (noch zulässige) Ermittlung der eigentlichen Bestimmung von Artikel 6 db darstellt, oder ob es sich bei einem solchen Verständnis schon um eine (unzulässige) Abweichung („derogating“) oder gar einen offensichtlichen Widerspruch („clearly contrary“) handelt.

[31] Ein offensichtlicher Widerspruch kann verneint werden, denn Art. 6 db eIDAS2-PA schließt eine Pflicht zur Akzeptanz der Wallet für über die Identifizierung hinausgehende Zwecke nicht aus, sondern formuliert lediglich uneindeutig.

[32] Ob ein weites Verständnis der Akzeptanzpflicht eine unzulässige Abweichung im Sinne der EuGH-Rechtsprechung von Art. 6 db eIDAS2-PA darstellt, ist allerdings schwer zu beantworten, weil Art. 6 db nicht eindeutig und die Identifizierung ein wesentlicher Aspekt der SCA ist. Das weite Verständnis wird allerdings auch von zwei systematischen Argumenten gestützt, sodass das weite Verständnis keine Abweichung von Art. 6 db eIDAS2-PA darstellen dürfte.

Erwägungsgrund 111 PSR-Entwurf stützt weites Verständnis

[33] Bislang hat der Europäische Gesetzgeber nicht vorgegeben, mit welchem konkreten Mittel die SCA durchgeführt werden soll. Stattdessen ergibt sich aus der PSD2 (Art. 97 Abs. 1) und künftig aus der PSR (Art. 85 Abs. 1) lediglich, in welchen Fällen eine SCA durchzuführen ist. Welche Anforderungen eine SCA erfüllen muss, wann auf sie verzichtet werden kann: hier arbeiten Gesetzgeber und

¹² EuGH, Urt. vom 19.6.2014, Rs. C 345/13, ECLI:EU:C:2014:2013 – Karen Millen Fashions, Rn. 31; auch: EuGH, Urt. vom 13.9.2018, Rs. C-287/17, ECLI:EU:2018:707 (Ceska pojistovna a.s./WCZ, spol. S r. o., Rn. 33.

¹³ Wegener, in: Calliess/Ruffert, AEUV/EUV, 4. Aufl. 2011, Art. 19 EUV, Rn. 15.

Aufsicht zusammen. Die Akzeptanz konkreter Mittel, die für eine SCA verwendet werden können, wäre neu.

[34] Aus dem Entwurf der PSR lassen sich allerdings Argumente dafür ableiten, dass der Gesetzgeber jetzt so weit gehen will.¹⁴ In EG 111 PSR-Entwurf heißt es konkret, dass die EUDIWs grenzüberschreitende Identifizierung und auch Authentifizierung ermöglichen:

“European Digital Identity Wallets implemented under Regulation (EU) No 910/201452 of the European Parliament and of the Council, as amended by Regulation [XXX], are electronic identification means that offer identification and authentication tools for accessing financial services across borders, including payment services. The introduction of the European Digital Identity Wallet would further facilitate crossborder digital identification and authentication for secure digital payments and facilitate the development of a pan-European digital payments landscape.” (Hervorhebungen hinzugefügt)

Klare Positionierung der EU-Kommission für weites Verständnis im digital euro proposal

[35] Die EU-Kommission bringt auch im Explanatory Memorandum¹⁵ zu ihrem Regulierungsvorschlag für die Einrichtung eines Digitalen Euro deutlich zum Ausdruck, dass sie ein weites Verständnis von der Akzeptanzpflicht zugrunde legt. Dort¹⁶ heißt es,

“The EU-wide interoperable European Digital Identity Wallet allows users, on a voluntary basis, to on-board and perform strong customer authentication when making payments, as required by Article 97 of the PSD2. The same functionalities should be offered to digital euro users.”

[36] Nach Art. 97 Abs. 1 PSD2 sind es gerade die Zahlungsfreigabe und der Login, die von einer SCA abhängen. In dem Memorandum spricht die EU-Kommission auch nur von dem *user*, der die Möglichkeit haben soll, die EUDIW zu wählen. Sie setzt damit die Auswahlmöglichkeit und mit ihr die technische Bereitstellung durch den Zahlungsdienstleister voraus.

¹⁴ Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über Zahlungsdienste im Binnenmarkt und zur Änderung der Verordnung (EU) Nr. 1093/2010, COM(2023) 367 final.

¹⁵ Proposal for a Regulation of the European Parliament and of the Council on the establishment of the digital euro, COM(2023) 369 final.

¹⁶ Proposal for a Regulation of the European Parliament and of the Council on the establishment of the digital euro, COM(2023) 369 final, S.5.

[37] Zahlungen mit dem Digitalen Euro sollen nach dem Verordnungsentwurf auch über die EUDIW autorisiert¹⁷ werden:

„Payment service providers should also accept the use of European Digital Identity Wallets if the payer wishes to use the wallet for payment authorisation of digital euro payment transactions.”

Ergebnis

[38] Der Verordnungstext enthält in seiner aktuellen Fassung viele Anhaltspunkte dafür, dass eine Pflicht der Zahlungsdienstleister geregelt werden soll, die EUDIW zum Zwecke der SCA bei Zahlungen zu akzeptieren. Das ergibt sich aber nicht nur aus dem eIDAS2-PA, sondern auch aus dem PSR-Entwurf und aus dem Entwurf für eine Verordnung über den Digitalen Euro. Eine Präzisierung der eIDAS2 würde Restunsicherheit beseitigen. Je nachdem, was der Gesetzgeber anstrebt, genügt die Streichung von zwei Worten (siehe unten 39).

Mögliche Klarstellung

[39] Trotzdem gute Gründe dafürsprechen, dass die Verordnungsentwürfe eine weite Akzeptanzpflicht enthalten bzw. eine solche zugrunde legen, besteht Klarstellungsbedarf – und zwar sowohl dann, wenn der Gesetzgeber tatsächlich eine weite Akzeptanzpflicht regeln wollte, als auch dann, wenn er eigentlich das Gegenteil im Sinn hatte.

- [40] Gesetzgeber wollte weite Akzeptanzpflicht regeln: In diesem Fall läge es nahe, die Ergänzung „for online identification“, die die Unklarheiten verursacht, zu streichen.
- [41] Gesetzgeber wollte keine weite Akzeptanzpflicht regeln: In diesem Fall läge es nahe, eine Definition in den Verordnungstext aufzunehmen, aus der sich ergibt, was mit “strong user authentication for online identification” gemeint ist.

Technische Aspekte

[42] Die mögliche Pflicht der Zahlungsdienstleister, nach Art. 6 db eIDAS2-PA die EUDIW für SCA zu akzeptieren, fällt zeitlich zusammen mit Überlegungen der

¹⁷ Wir haben nicht genauer untersucht, ob der Gesetzgeber hier mit „autorisiert“ die Autorisierung im Sinne der Zustimmung der zahlenden Person zur Ausführung des Zahlungsvorgangs oder die Authentisierung gemeint ist. Beides ist für die Zahlung relevant und kann zusammenfallen. Zur Abgrenzung: Casper/Terlau/Zahrte, 3. Aufl. 2023, ZAG § 55 Rn. 2, 3.

EU-Kommission, die Haftung für autorisierte betrügerische Zahlungsvorgänge zu verschärfen (Art. 59 Abs. 1 PSR-Entwurf). Wenn die EU-Kommission mit der IT-Architektur der EUDIW dafür sorgt, dass SCA mit der EUDIW die Sicherheit erhöht, löst das möglicherweise einen faktischen Anreiz für Zahlungsdienstleister aus, die EUDIW zu akzeptieren. In technischer Hinsicht wäre es jedenfalls möglich, mit der EUDIW die gesamte SCA abzuwickeln. Das konnte mit Prototypen von Technikern des Digitallabors schon nachgewiesen werden.

Contact

Digitallabor c/o Deutscher Sparkassen- und Giroverband e.V.
Charlottenstraße 47
10117 Berlin
0049177 4803 413 (Oliver Lauer)
<https://www.digitallabor.berlin>

Das Digitallabor ist eine Organisationseinheit im Deutschen Sparkassen- und Giroverband e.V. (DSGV). Der DSGV vertritt die Interessen der 353 Sparkassen, der Landesbankengruppen und der DekaBank sowie von acht Landesbausparkassen, neun Erstversicherungsgruppen der Sparkassen und zahlreichen weiteren Finanzdienstleistungsunternehmen.

Die Diskussionspapiere des Digitallabors dienen dazu, die Ergebnisse der laufenden Arbeiten vor der Veröffentlichung zu verbreiten, um den Gedankenaustausch und die politische, ökonomische und wissenschaftliche Diskussion zu fördern. Die vom Digitallabor veröffentlichten Diskussionspapiere geben die Meinung der jeweiligen Autoren wieder und spiegeln nicht unbedingt die Meinung des Digitallabors oder des DSGV insgesamt wider.

Alle Digitallabor Discussion Papers können hier heruntergeladen werden:
<https://www.digitallabor.berlin/papers/>

Suggested Citation: Lange-Hausstein/Kremer, Warum die Akzeptanz der EU Digital Identity Wallet für SCA nach eIDAS2 verpflichtend wäre, Nov. 23, Digitallabor Discussion Paper, <https://www.digitallabor.berlin/papers/>.

Schreiben Sie uns

Dr. Christian Lange-Hausstein
christian.lange-hausstein@dsgv.de

Tim Kremer
tim.kremer@dsgv.de