

Franziska Granc, Arno Fiedler

Nationale und europäische Sicht auf eIDAS 2.0 – Aufwand und Nutzen

Der digitale Binnenmarkt bietet für Bürger:innen, Wirtschaft und Verwaltung einen großen Nutzen. Die 2014 in Kraft getretene eIDAS-Verordnung hat dafür den Grundbaustein gelegt und die Digitalisierung Europas gestärkt. Leider haben die Potentiale der Verordnung nur in wenigen Mitgliedsstaaten Anwendung gefunden. Die gestiegene Nachfrage für vertrauenswürdige Identifizierungen im Netz und die immer weiterwachsende Abhängigkeit von wenigen globalen Unternehmen erfordert eine Novellierung der bestehenden Verordnung. Die Kommission stellt mit ihrem Revisionsvorschlag eine souveräne Nutzung von digitalen Identitäten in den Vordergrund und ebnet den Weg für neue dezentrale Technologien.

1 Einleitung

Am 17. September 2014 trat die Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates vom 23. Juli 2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt (eIDAS) in Kraft. Damit wurde das bisher geltende Signaturgesetz, welches auf der Richtlinie 1999/93/EG aufbaute, aufgehoben. Die eIDAS Verordnung hat einen Grundbaustein für die Digitalisierung im europäischen Raum gelegt. Seit Mitte 2016 ist die Verordnung in allen Mitgliedsstaaten unmittelbar gültig und ermöglicht eine grenzüberschreitende Nutzung elektronischer Identifizierungen und Vertrauensdienste. Als Vertrauensdienste definiert eIDAS elektronische Signaturen, elektronische Siegel, elektronische Zeitstempel,

Zustelldienste und Webseitenzertifikate. Bürger:innen, Wirtschaft und Verwaltung können durch die Regelung verschiedenste Dienste und Anwendungen beanspruchen. Praktische Beispiele, die sich mit eIDAS sicher und einheitlich regeln lassen, sind medienbruchfreie Signaturen, beispielsweise im Gesundheitssystem, die Authentifizierung von Webseiten oder auch die Nachvollziehbarkeit und Revision elektronischer Dokumente mithilfe elektronischer Zeitstempel. Zusammenfassend können durch eIDAS Bürger:innen, Staat und Unternehmen verschiedenste elektronische Transaktionen im digitalen Binnenmarkt vertrauenswürdig durchführen.

2 Entwicklungsgeschichte – Warum braucht es eine europäische Verordnung?

Der Bedarf nach qualifizierten elektronischen Signaturen und einheitlichen europäischen Standards wurde bereits 1999 erkannt und durch die Einführung der Electronic Signatures Directive gedeckt. Die Verordnung schrieb vor, dass elektronische Signaturen gleichermaßen anzuerkennen sind wie Unterschriften auf dem Papier. Die Verordnung wurde 2014 durch eIDAS ersetzt. Ziel von eIDAS ist die Schaffung eines rechtlichen Rahmens, in dem Bürger:innen, Wirtschaft und Verwaltung digitale grenzüberschreitende Transaktionen ausüben können. Services aus verschiedenen Branchen, wie zum Beispiel dem Finanzsektor, dem Bildungssektor oder der öffentlichen Verwaltung sollen in allen Mitgliedsstaaten sicher und grenzüberschreitend beansprucht werden können. Digitalen Identitäten kommt dabei die Schlüsselfunktion zu. Hierfür schreibt eIDAS die Anerkennung der jeweils nationalen eID-Systeme vor. Dadurch soll das im *Single Digital Gateway* (SDG) vorgesehene Once-Only Prinzip verwirklicht werden können [6]. Nicht in allen Mitgliedsstaaten wurden die nach eIDAS definierten ID-Lösungen jedoch gleichermaßen umgesetzt. Laut einer PWC Studie deckt die bisherige



Arno Fiedler

Geschäftsführer, Nimbus Technologieberatung GmbH.

E-Mail: af@nimbus.berlin



Franziska Granc

Projektmanagerin, Nimbus Technologieberatung GmbH.

E-Mail: franziska.granc@nimbus.berlin

eIDAS Verordnung gerade einmal die Hälfte der EU-Bevölkerung ab, 41% haben laut der Studie keinen Zugang zu einem sicheren, vertrauenswürdigen und grenzüberschreitenden eID-System [2]. In Deutschland gibt es zwar bereits seit mehreren Jahren ein eID-System, jedoch haben die Anwendungen für den elektronischen Personalausweis bisher wenig Akzeptanz erfahren.

Die Einführung qualifizierter Webseitenzertifikate (QWACS) in der EU ist weltweit einzigartig und bietet eine sehr gute Möglichkeit der Webseitenauthentifizierung. Durch QWACS können Bürger:innen sicherstellen, dass die Identität eines Webseiteninhabers vertrauenswürdig und rechtsverbindlich geprüft werden kann. Leider hat die Akzeptanz von QWACS bisher nicht die kritische Masse erreicht, da eine Unterstützung durch die Browserhersteller nicht erfolgte. Auch wenn die eIDAS Verordnung so wie sie 2014 verabschiedet wurde einen wesentlichen Grundbaustein für die Digitalisierung in der EU gelegt hat, fehlt es also sowohl im ID-Bereich als auch bei den qualifizierten Siegeln und Webseitenzertifikaten noch an flächendeckendem Zugang und Akzeptanz. Es fehlt eine umfassende Regelung für die vertrauenswürdige Identifizierung im privaten Sektor und die Möglichkeit ausgewählte digitale Nachweise von Identitätsattributen auszutauschen [2]. Dabei könnten Unternehmen als qualifizierte Vertrauensdienste ebenfalls Identitätslösungen anbieten und den Markt und das Angebot innerhalb der EU erweitern. Tatsächlich gibt es im privaten Sektor immer mehr Identitätsanbieter (z.B. Banken, Online-Plattformen, Kommunikationsdienste) die anwendungsspezifisch für Kontoeröffnungen, Leasingverträge oder Telekommunikationsverträge Identitäten prüfen. Die steigende Nachfrage von öffentlichen und privaten Services sowie die steigende Abhängigkeit von wenigen globalen Unternehmen und steigende Cyberkriminalität machen eine Revision der eIDAS Verordnung notwendig. Zentrales Erfolgskriterium ist dabei die Zusammenarbeit zwischen der öffentlichen Verwaltung und Wirtschaft.

3 eIDAS 2.0 – was ist neu?

In diesem Jahr hat die Kommission einen Vorschlag zur Revision der eIDAS Verordnung vorgelegt. Mit diesem Vorschlag geht die für alle Mitgliedsstaaten verpflichtende Einführung einer sogenannten EUid einher. Konkret sollen Mitgliedsstaaten verpflichtet werden eine EU-Identity Wallet anzubieten. Dabei handelt es sich um eine digitale Brieftasche, in der die hoheitliche nationale Identität und weitere digitale Identitätsnachweise abgelegt werden können. Die Wallet soll nach europäisch standardisierten und definierten technischen Regeln von den jeweiligen Mitgliedsstaaten selbst bereitgestellt werden und anschließend EU-weit genutzt werden können. Dadurch sollen Bürger:innen der EU und Unternehmen grenzüberschreitend Online-Dienste nutzen können. Die digitalen Nachweise in dieser Wallet werden in eIDAS 2 als „Attribute Attestations“ definiert. Hierbei handelt es sich um digitale, identitätsbezogene Nachweise.

In dem novellierten eIDAS Vorschlag steht die Souveränität des Nutzers im Vordergrund. Dabei werden im Vorschlag verschiedene Technologien, darunter auch die Distributed Ledger Technologie (DLT) berücksichtigt.

Die „Attribute Attestations“ können in verschiedenen technologischen Ausprägungen vorkommen. Mögliche Formen sind beispielsweise Verifiable Credentials (VC). Von VCs spricht man oftmals im Kontext der Self-Sovereign-Identity (SSI). Beim SSI

Ansatz steht der Nutzende im Vordergrund. Konkret bedeutet dieser Ansatz, dass der User jederzeit über seine Identität verfügt und einzelne Nachweise seiner Identität selbstbestimmt und ausgewählt mit Dritten teilen kann. Neu an dem SSI-Ansatz ist also, dass es keinen zentralen Speicher mit Identitätsinformationen gibt, sondern der Inhaber einer Identität auch derjenige ist, der seine Daten auf beispielsweise einem mobilen Endgerät (Smartphone) besitzt.

Neben der hoheitlichen, nationalen Identität sollen auch weitere Nachweise, wie zum Beispiel der Führerschein, Hochschulzeugnisse, anderweitige Zertifikate und Bescheinigungen in die Wallet abgelegt werden können. Die Bereitstellung der Wallet selbst obliegt dem Mitgliedsstaat und kann, wenn von dem jeweiligen Mitgliedsstaat vorgesehen, auch von Privatunternehmen angeboten werden. So wie die Mitgliedsstaaten verpflichtet werden sowohl die Bereitstellung der Wallet als auch die entsprechenden Nachweise zu organisieren, so werden juristische Personen, also Unternehmen und Behörden verpflichtet die hoheitliche eID und Nachweise als Identifikationslösung zu akzeptieren. Artikel 12b (2) erwähnt explizit die Anwendungsfelder Verkehr, Energie, Bank- und Finanzdienstleistungen, soziale Sicherheit, Gesundheit, Trinkwasser, Postdienste, digitale Infrastrukturen, Bildung oder Telekommunikation. Wichtige neue Anwendungsfelder werden auch dadurch erschlossen, dass die großen Online-Plattformanbieter dazu verpflichtet werden, für den Zugang zu ihren Online-Diensten die EUid für die Nutzer-Authentifizierung zu akzeptieren.

Für Bürgerinnen ergeben sich dadurch neue Anwendungsmöglichkeiten ihre Identität selbstbestimmt und souverän nachzuweisen. Durch die genannten Attribute Attestations können nun ausgewählte zusätzliche Eigenschaften, Qualifikationen und Rechte von natürlichen und juristischen Personen geteilt werden, ohne dass dabei die gesamte Identität, also alle zu einer Person oder Organisation gehörenden Identitätsinformationen preisgegeben werden müssen. Folglich könnten unter eIDAS 2.0 mit den „Attribute Attestations“ pseudonyme Identifizierung und Authentifizierung dort wo es möglich ist gewahrt werden. Dies gilt insbesondere für Anwendungen im nicht-hoheitlichen Bereich. Muss beispielsweise nachgewiesen werden, dass es sich bei einer Person um eine Volljährige handelt, so ist lediglich der Nachweis darüber, dass die Person älter als 18 Jahre alt ist, erforderlich. Der Name und das genaue Geburtsdatum werden nicht benötigt.

Wenn auch die Etablierung eines EU-Identity Frameworks im Vordergrund der eIDAS Revision steht, so wurden von der Kommission auch die verbindliche Einführung von Normen für vertrauenswürdige Systeme und Produkte vorgeschlagen.

Qualifizierte Archivierungsdienste

Neben der Einführung eines EU-Identity Frameworks sieht der Vorschlag der EU-Kommission zur eIDAS-Novellierung die Einführung qualifizierter Archivierungsdienste als neuartige Vertrauensdienste vor. Somit wird der bisher definierte Rahmen der qualifizierten Bewahrungsdienste um die langfristig unveränderbare Aufbewahrung von Dokumenten erweitert. Hieraus ergibt sich ein neuartiges Geschäftsfeld für Vertrauensdiensteanbieter, welches bisher nur von Bibliotheken und Notaren rechtsverbindlich angeboten werden konnte.

Zwar muss der Vorschlag der Kommission im Rahmen des Gesetzgebungsprozesses der EU im Trilog-Verfahren mit dem Euro-

päischen Parlament und dem Europäischen Rat noch weiter ausverhandelt werden, parallel wird aber während dieses Prozesses bereits an den technischen Anforderungen gearbeitet. Speziell gegründete Working Groups arbeiten an der Ausarbeitung einer sogenannten Toolbox, um die neuen Vorgaben aus der eIDAS Revision technisch zu konkretisieren. Dies bestätigt auch der bereits veröffentlichte Zeitplan der Kommission für die technische Ausgestaltung von eIDAS 2.0: Bis Dezember 2021 soll bereits ein erster Entwurf für die Vereinbarung der technischen Architektur für die Wallet vorliegen. Bis Juni 2022 sollen die technischen Details und jeweiligen Standards sowie Best Practices für die Bereitstellung und den Austausch von Attributen sowie für die Funktionalität der Wallet definiert werden. Bis September 2022 soll schließlich die Vereinbarung der Toolbox von allen Mitgliedsstaaten beschlossen werden, sodass diese dann Oktober 2022 von der Kommission veröffentlicht werden könnte. Dieser Zeitplan ist sehr ambitioniert und erfordert schnelle Einigungen über technische Details. Gleichzeitig verdeutlicht dieses Bestreben die Dringlichkeit, die eID-Landschaft in Europa zeitnah zu harmonisieren und somit weitere Abhängigkeiten von wenigen globalen Unternehmen zu reduzieren und stattdessen europäische Lösungen auf dem Markt zu etablieren.

4 Bürger, Verwaltung und Wirtschaft – Aufwand und Nutzen

Die Covid-19 Pandemie hat die Nachfrage nach sicheren digitalen Identitäten nochmals stark unterstrichen. Im Folgenden soll deshalb erläutert werden, welcher Aufwand und Nutzen sich für Bürger:innen, Verwaltung und Wirtschaft durch eIDAS 2.0 ergibt. Wichtig zu erwähnen ist, dass die Verordnung sowohl für natürliche als auch juristische Personen gilt. Die Bereitstellung der genannten „Attribute Attestations“ erfordert in einem ersten Schritt zunächst die Digitalisierung der relevanten Behördenprozesse. Abgesehen von den finanziellen Kosten, erfordert dies auch einen immensen administrativen Aufwand. Aus deutscher Perspektive ist in dem 2017 beschlossenen Online-Zugangsgesetz (OZG) eine solche Digitalisierung ohnehin vorgesehen und muss unabhängig von eIDAS bis 2025 umgesetzt werden. Dennoch ergeben sich neue Herausforderungen zumindest aus deutscher Sicht, die gesetzlichen Anforderungen zu erfüllen. Neben dem OZG sind in Deutschland auch das Registermodernisierungsgesetz und die Einführung der Smart-eID bereits laufende Projekte. Der Aufwand besteht also darin, die neuen europäischen Vorgaben von Anfang an zu berücksichtigen und in die nationalen Initiativen und Vorhaben zu integrieren.

Abhilfe bei der Bereitstellung aller in eIDAS 2.0 vorgeschriebenen Attribute können die Unternehmen bzw. die Wirtschaft schaffen. Insbesondere im nicht-hoheitlichen Bereich ist es nicht immer erforderlich, dass der Staat als Provider bestimmter ID-Nachweise fungiert. Umgekehrt profitieren viele Unternehmen von der eIDAS Revision. Langwierige Identifizierungsprozesse können maßgeblich verkürzt werden. Beispielsweise im Bankensektor bei der Eröffnung eines Bankkontos oder bei der Beantragung eines Kredits. Um der Komplexität gerecht zu werden ist eine enge Zusammenarbeit zwischen Staat und Wirtschaft unbedingt erforderlich. Hier kann Deutschland EU-weit eine Vorbildfunktion übernehmen. Laufende Projekte wie zum Beispiel das Schaufensterprogramm „Sichere Digitale Identitäten“

des Bundeswirtschaftsministeriums arbeiten an der Etablierung sicherer digitaler Identitätslösungen im Alltag. Die von den Schaufensterprojekten erprobten Lösungen zeigen, wie das Zusammenspiel zwischen Staat und Wirtschaft praktisch aussehen kann. Während die Einführung der deutschen Smart-eID in den hoheitlichen Bereich fällt, arbeiten die Schaufensterprojekte in über 100 Use Cases an der Bereitstellung digitaler Nachweise. Diese Nachweise könnten nach Inkrafttreten von eIDAS 2.0 in die Liste der „Attribute Attestations“ mitaufgenommen werden. Wenngleich also in Deutschland die Smart-eID den Grundbaustein für eine sichere, vom Staat bereitgestellte digitale Identität legt, ist diese hoheitliche Identifizierung nach eIDAS „hoch“ nicht unbedingt in jedem Anwendungsfall notwendig. In eIDAS werden drei Sicherheitsniveaus (Level of Assurance) vorgegeben: niedrig, substanziell und hoch. Diese Unterscheidung spielt bei der Zusammenarbeit zwischen Staat und Wirtschaft eine wichtige Rolle. Um das Sicherheitsniveau „hoch“ zu erreichen ist fast immer eine hoheitliche eID erforderlich. Das kann in Deutschland die Wirtschaft bisher kaum oder gar nicht leisten. In anderen Ländern hingegen, wie zum Beispiel in Norwegen und Italien, ist der Einsatz von privat ausgestellten Identitäten auch bei hoheitlichen Anwendungsfällen möglich.¹ Bei Anwendungen mit niedrigem oder substanziellen Sicherheitsniveau kann die Privatwirtschaft jedoch die Verwaltung entlasten und selbst Identitätsnachweise ausstellen.

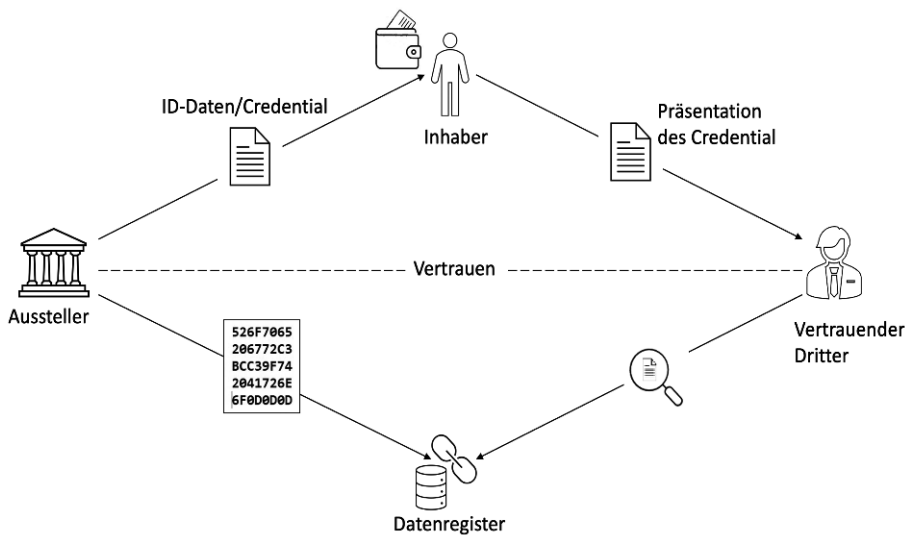
Für Bürger:innen schafft die novellierte eIDAS Verordnung potenziell den größten Nutzen, da die EUid branchenübergreifend Anwendung finden könnte. Sie könnte Abhilfe bei der aufwändigen und oftmals unsicheren Nutzernamen-Passwort Identifizierung schaffen, da sich Bürger:innen mit einem vereinheitlichten und global anerkannten Instrumentarium bei Online-Services authentisieren könnten.

Single-Sign-Ons von großen globalen Unternehmen bringen Bürger:innen in eine Abhängigkeit, bei der die Kontrolle darüber, welche Daten wann und mit wem geteilt werden, nicht gewährleistet ist. Dem wird durch die novellierte eIDAS Verordnung Abhilfe geschaffen. Dies hat nicht nur Vorteile für die Bürger:innen, sondern ermöglicht auch Unternehmen sichere und vertrauenswürdige Identifizierungsvorgänge[2]. Die Rollenverteilung nach eIDAS 2.0 unterteilt sich in drei Akteure: Inhaber, Aussteller und Vertrauender Dritter (Relying Party). Bürger:innen, Verwaltung und Wirtschaft können dabei jede der drei Rollen einnehmen. Diese Flexibilität schafft die Voraussetzung für ein selbstsouveränes ID-Ökosystem und bietet einen Mehrwert gegenüber dem bisherigen Ansatz. Die folgende Graphik stellt die Rollenverteilung beispielhaft dar.

Eine Herausforderung von der bestehenden eIDAS-Verordnung ist die bisher noch uneinheitliche eID Landschaft in Europa. Die verpflichtende Einführung bei eIDAS 2.0 in allen Mitgliedsstaaten ist daher ein wichtiger Schritt in die richtige Richtung, wird aber einen großen Aufwand gerade von Mitgliedsstaaten, welche sich noch am Anfang einer solchen Einführung befinden, erfordern. Deutschland kann aus europäischer Sicht hier unterstützen und bei der Interoperabilität der Lösungen eine aktive Rolle einnehmen. Ein weiterer Nutzen von eIDAS 2.0 wäre aus Sicht der EU, dass Anbieter von Online-Diensten dadurch auch konform mit bereits geltenden Gesetzen und Regelungen

¹ Bank-ID

Abbildung 1 | Mögliche Rollenverteilung gemäß eIDAS 2.0



wie zum Beispiel der DSGVO werden würden, da sie die eIDAS Standards und Vorgaben implementieren müssen [6].

5 Internationales Feedback zur eIDAS Revision

Die Kommission strebt mit ihrem Vorschlag der eIDAS Revision in erster Linie an, die europäische Souveränität zu stärken und die Abhängigkeit von wenigen globalen Playern zu reduzieren. Letztere haben sich in offiziellen Stellungnahmen zu dem Vorschlag der eIDAS Novellierung geäußert.² Während der Ansatz der Etablierung eines EU-Identity Frameworks begrüßt wurde, wurden ebenfalls Bedenken, Kritik und Wünsche geäußert. Unter anderem besteht der Wunsch, insbesondere bei der Ausgestaltung der eIDAS Toolbox auf internationale Standards, wie den ISO-Normen zu setzen. Des Weiteren wurde von den Unternehmen der in Teilen bereits in eIDAS vorgesehene Ansatz der „Datenminimierung“ nochmals unterstrichen. Im vorherigen Kapitel dieses Artikels wurde bereits der Ansatz der Self-Sovereign-Identity beschrieben. Dieser bietet zumindest in der Theorie die Möglichkeit, dass der User selbstbestimmt ausgewählte Attribute teilt und nicht bei jedem Identifizierungsprozess die gesamte Identität preisgeben muss. Folglich würde eine eIDAS 2.0 Umsetzung nach SSI Prinzipien den von Unternehmen angesprochenen Aspekt der Datenminimierung erfüllen.

Ein wesentlicher Kritikpunkt, der von den globalen Playern geäußert wurde, ist die Verpflichtung der Unternehmen oder Relying Parties die EUid-Wallet als Identifizierungsmittel zu akzeptieren. Dies sei insbesondere eine Herausforderung für Unternehmen, welche bisher keine hoheitlichen Identifizierungsprozesse innerhalb ihrer Services vorsehen. Insbesondere im privatwirtschaftlichen Bereich erfordern viele Identifizierungsprozesse nicht das von eIDAS definierte Sicherheitsniveau „hoch“. Die-

se Umstellung wäre für Unternehmen mit einem hohen Kostenaufwand verbunden, der durch den Nutzen nicht gerechtfertigt werden könne, weil sich um Anwendungen oder Services mit niedrigem Sicherheitsniveau handle. Diese Kritik ist durchaus in Teilen berechtigt. Auch wenn in eIDAS die Unternehmen, die die EUid akzeptieren müssen, von dem Umsatz des Unternehmens abhängt, sollte eine Überregulierung vermieden werden. Andernfalls könnte ein Wettbewerbsnachteil gegenüber globalen Playern insbesondere für KMUs und Startups entstehen. Wenn auch dies aus Sicht einiger Unternehmen mit einem potenziell größeren Aufwand verbunden wäre, so hätte der User (Bürger:innen) durch eine solche Verpflichtung den Nutzen, dass seine vertrauens-

würdige europäische digitale Identität jederzeit bei öffentlichen und privaten Services genutzt werden kann. Dies verbessert die Kontrolle über die eigenen Daten und vermindert durch einen fehlenden zentralen Speicher aller User-Daten die Wahrscheinlichkeit für Hackerangriffe.

Weiter wurde kritisiert, dass im eIDAS 2.0-Vorschlag bereits Bezug zum Digital Markets Acts (DMA) genommen wird, obwohl dieser noch nicht final beschlossen ist. Dieser Kritikpunkt ist nur in Teilen berechtigt, da es sich bei eIDAS 2.0 ebenfalls um einen ersten Entwurf und keinen finalen Beschluss handelt. Der DMA könnte potenziell eine wichtige Rolle bei der Umsetzung von eIDAS 2.0 spielen, insbesondere im Hinblick auf eine mögliche Überprüfung und gegebenenfalls Sanktion fehlender Unternehmen bei der Einhaltung von der Verordnung.

Die novellierte eIDAS Verordnung sieht vor, dass qualifizierte Webseitenauthentifizierungszertifikate automatisch von Webbrowsern anerkannt und der Vertrauensstatus visualisiert dargestellt werden muss. Von den globalen Playern wurden Bedenken geäußert, dass dies die Sicherheit der Browser maßgeblich beeinträchtigen könnte. Die Unabhängigkeit von Webbrowsern und die vom Unternehmen entwickelten Sicherheitsvorkehrungen würden durch eIDAS 2.0 beeinträchtigt. Deshalb wird gefordert den Artikel 45³ der eIDAS Novellierung ersatzlos zu streichen.

Bei den genannten Äußerungen muss berücksichtigt werden, dass wirtschaftliche Interessen der globalen Unternehmen ebenfalls eine Rolle spielen. Beispielsweise wurde von Apple die Adaption der ISO 18013-5 (mobile Driving licence „mDL“) angeregt, nachdem in Teilen der USA der Führerschein künftig in der Wallet des Unternehmens abgelegt werden kann. Somit ist zu erwarten, dass Apple sich im Bereich der hoheitlichen Credentials stärker engagiert⁴ und somit die Souveränität staatlicher eID-Systeme in Frage stellt.

Zuletzt wurde der Wunsch geäußert, die internationale Experten-Community aktiv mit in die Ausgestaltung der eIDAS Tool-

² Mozilla Feedback (November 2021) <https://blog.mozilla.org/netpolicy/files/2021/11/eIDAS-Position-paper-Mozilla-.pdf>; Apple Feedback (September 2021) https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12528-EU-digital-ID-scheme-for-online-transactions-across-Europe/F2669161_en

³ eIDAS 2.0 Art. 45 (2): „Die in Absatz 1 genannten qualifizierten Zertifikate für die WebsiteAuthentifizierung werden von Webbrowsern anerkannt.“

⁴ So soll beispielsweise der Covid-19 Impfnachweis künftig auch in der Apple Wallet abgelegt werden können.

box miteinzubeziehen. Eine internationale Kooperation ist sicherlich sinnvoll im Hinblick auf eine globale Interoperabilität.

6 Fazit

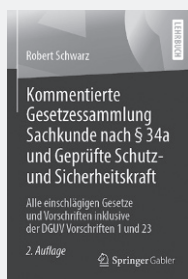
Zusammenfassend ist festzustellen, dass die Revision der eIDAS Verordnung ein essenzieller Schritt ist für die sichere Digitalisierung der EU, da sie eine rechtliche Grundlage für vertrauenswürdige Identifizierungsdienste schafft und somit sowohl öffentliche als auch private Services digital angeboten werden können, die sicher, interoperabel und vertrauenswürdig gemäß eIDAS sind. Das stärkt den europäischen Markt und ermöglicht europäisch souveräne Lösungen. Die Covid-19 Pandemie hat gezeigt, dass eine sichere und nachhaltige Digitalisierung ohne sichere digitale Identitäten und qualifizierte Vertrauensdienste nicht möglich ist. Die bestehende eIDAS Verordnung hat zwar eine gute Grundlage geschaffen, die derzeit bestehende Fragmentierung hinsichtlich eID-Lösungen im europäischen Markt hat aber zur Folge, dass sich ID-Lösungen weniger großer Unternehmen zumindest im privaten Sektor immer weiter ausbreiten. Eine Einführung einer EUid sollte deshalb zügig erfolgen und für natürliche und juristische Personen sicher und breitflächig nutzbar sein. Dies würde durch gemeinsame Standards und die Verpflichtung der Mitgliedsstaaten eine Identity Wallet und digitale Nachweise bereitzustellen, erreicht werden.

Das Potential von eIDAS 2.0 aus europäischer Sicht besteht also in erster Linie darin, die fragmentierte eID-Landschaft in der EU zu vereinheitlichen und dadurch neue Geschäftsfelder und Marktzugänge zu ermöglichen. Die Ausweitung der eIDAS Verordnung auf den privaten Sektor steigert die Effektivität der Verordnung und den Einsatz qualifizierter Vertrauensdienste. Es er-

geben sich neue Geschäftsmodelle, die zunächst zwar mit einem finanziellen und administrativen Aufwand verbunden sind, langfristig aber technologische Innovationen und somit den Wohlstand in der EU vorantreiben. Deutschland ist durch die nationalen Initiativen der Etablierung einer Smart-eID sowie der Erprobung weiterer dezentraler Identitätslösungen auf einem guten Weg innerhalb Europas eine Vorbildfunktion zu übernehmen und bei der Entwicklung der Standards und Toolbox für eIDAS 2.0 eine zentrale Rolle zu spielen.

Literatur

- [1] PWC (2018): Study on a marketing plan to stimulate to take-up of eID and trust service for the Digital Single Market. Im Auftrag der Europäischen Kommission durchgeführte Studie.
- [2] PWC, DLA Piper (2020): Study to support the impact assessment for the revision of the eIDAS regulation. Im Auftrag der Europäischen Kommission durchgeführte Studie.
- [3] Bauer, Armin; Ehneß Susanne: Die Digitalisierung der Brieftasche: Identity Wallets. eGovernment Computing. 2.11.2021. Link: <https://www.egovernment-computing.de/die-digitalisierung-der-brieftasche-identity-wallets-a-1071395/?cmp=nl-127&uuid=> letzter Zugriff: 24.11.2021.
- [4] BSI: eIDAS-Verordnung über elektronische Identifizierung und Vertrauensdienste. Link: https://www.bsi.bund.de/DE/Themen/Oeffentliche-Verwaltung/eIDAS-Verordnung/eidas-verordnung_node.html letzter Zugriff: 24.11.2021.
- [5] Bundesdruckerei: Drei Thesen zur eIDAS Novelle. 14.10.2021. Link: https://www.bundesdruckerei.de/de/Fokusthemen/Magazin/Drei-Thesen-zur-eIDAS-Novelle?etcc_cmp=NL-Gruppe-Nov-2021&etcc_med=Newsletter letzter Zugriff: 24.11.2021
- [6] Europäische Kommission, DG CNECT H4: Inception Impact Assessment. Revision of the eIDAS Regulation – European Digital Identity (EUid).



Datenschutz

R. Schwarz
Kommentierte Gesetzessammlung Sachkunde nach § 34a und Geprüfte Schutz- und Sicherheitskraft

Alle einschlägigen Gesetze und Vorschriften inklusive der DGUV Vorschriften 1 und 23

2. Aufl. 2019, aktualisierte, XI, 227 S. 1 Abb. Brosch.

€ (D) 14,99 | € (A) 15,41 | *sFr 17,00

ISBN 978-3-658-24546-7

€ 9,99 | *sFr 13,50

ISBN 978-3-658-24546-7 (eBook)

Ihre Vorteile in unserem Online Shop:

Über 280.000 Titel aus allen Fachgebieten | eBooks sind auf allen Endgeräten nutzbar | Kostenloser Versand für Printbücher weltweit

Jetzt bestellen auf springer.com/DGUV1 oder in der Buchhandlung

Part of **SPRINGER NATURE**