# DIGITALE IDENTITÄT IM ZAHLUNGSVERKEHR

Helgo Eberwein / Lejla Tuholjaković

Mag. Dr. Helgo Eberwein, Jurist, Bundesministerium für Inneres, Abteilung III/7 – Rechtsangelegenheiten und Datenschutz
Herrengasse 7, 1010 Wien, AT
helgo.eberwein@bmi.gv.at; https://www.bmi.gv.at

Mag. iur. Lejla Tuholjaković, Consultant mit Schwerpunkt Banking, Ernst & Young Management Consulting GmbH, Financial Services Consulting
Wagramer Straße 19, 1220 Wien, AT
lejla.tuholjakovic@at.ey.com; https://www.ey.com/de_at/people/lejla-tuholjakovic

***Schlagworte:*** ***Legitimationsprüfung, Zahlungsverkehr, Elektronische Identität, Digitale Identität, Geldwäsche, EUid, Know Your Customer (KYC)***

***Abstract:*** *Die EU-Kommission hat im Juni 2021 einen Rahmen für eine europäische digitale Identität (EUid) vorgeschlagen. Damit soll EU-Bürgern sowie Unternehmen ein Identitätsnachweis, die elektronische Dokumenten-Weitergabe mittels EUid-Brieftasche sowie die Nutzung europaweiter Online-Dienste ermöglicht werden. Die Autoren untersuchen die Entwicklung der Legitimationsprüfung und die Unterschiede zwischen derzeitiger und zukünftiger Rechtslage. Berücksichtigt werden die Einflüsse der Legitimationsprüfung auf die geldwäscherelevanten Transaktionen, die Rechtslage in den USA, Risken und Missbrauchsfälle.*

## 1. Digitale Strategie der EU und Nachhaltigkeitsziele der UN

Die digitale Technologie verändert unser Leben. Die Kommission ist entschlossen, das kommende Jahrzehnt zur „Digitalen Dekade Europas" zu machen und den Schwerpunkt dabei auf Daten, Technologie und Infrastruktur zu setzen: „Ein Europa für das digitale Zeitalter" wurde als eine von sechs Prioritäten der Kommission für 2019 – 2024 festgelegt. In der Umsetzung dieser Zielvorgaben stellte die Kommission am 3.6.2021 einen Rahmen für eine europäische digitale Identität (EUid) vor; die Umsetzung ist mit 2022 beabsichtigt.[1] Bei der digitalen Transformation gilt es – wie bei jedem gesellschaftlichen Wandel – die gewünschten Bevölkerungsgruppen an der neuen Entwicklung teilhaben zu lassen.[2] Eine legale Identität für alle Menschen ist auch eines der Nachhaltigkeitsziele, die die Vereinten Nationen bis 2030 erreichen wollen.[3] Das britische „Economic and Social Research Council" (ESRC) hat 2017 durch das Projekt „Building Digital Identities" den Einsatz digitaler Identitäten evaluiert und auch die Weltbank setzt auf digitale Identitäten, um das UN-Nachhaltigkeitsziel zu erreichen.[4]

Die europäische digitale Identität bringt viele Vorteile mit sich und zwar u. a.:

– EU-weit anerkannte digitale Identität,
– einfache und verlässliche Kontrolle sowie viele Informationen für Dienstleistungen, die einen Informationsaustausch erfordern, preisgegeben werden,
– digitale Brieftaschen, die per Handy-App und anderweitig verfügbar sind,

---

1 https://ec.europa.eu/info/strategy_de; https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age_de (abgerufen am 5.11.2021).

2 Eberwein/Martino, Digitale Identität für EU-Bürger, Öffentliche Sicherheit 9–10/21, S. 93 (93).

3 UN-Ziele und Zielvorgaben (aus der Agenda 2030 für nachhaltige Entwicklung) Punkt 16.9: „Bis 2030 insbesondere durch die Registrierung der Geburten dafür sorgen, dass alle Menschen eine rechtliche Identität haben." (abrufbar unter: https://unstats.un.org/sdgs/indicators/Global%20Indicator%20Framework%20after%202021%20refinem ent_Ger.pdf; abgerufen am 14.11.2021).

4 Hafen, Die prekäre Zukunft der digitalen Identität (abrufbar unter: https://computerwelt.at/news/die-prekaere-zukunft-der-digitalen-identitaet; abgerufen am 14.11.2021).

– die Möglichkeit, sich online und offline auszuweisen,
– die Möglichkeit, die Informationen aus verlässlichen privaten Quellen zu speichern und weiterzugeben.[5]

Seit dem Inkrafttreten des Teils der eIDAS-Verordnung[6] betreffend die elektronische Identifizierung im September 2018 haben 14 Mitgliedstaaten mindestens ein elektronisches Identifizierungssystem (eID-System) notifiziert. Deshalb haben nur 59 % aller EU-Einwohner grenzübergreifenden Zugang zu vertrauenswürdigen und sicheren eID-Systemen.[7] Eine Vereinheitlichung auf EU-Ebene wird daher angestrebt. Digitale Identität ist ebenfalls im Zahlungsverkehr von großer Wichtigkeit. In immer schwieriger werdenden Zeiten muss die Zahlungsverkehrsbranche das Vertrauen bewahren, indem sie einen Weg findet, die Verbraucher vor der ständigen Bedrohung durch Zahlungsbetrug und -diebstahl zu schützen.

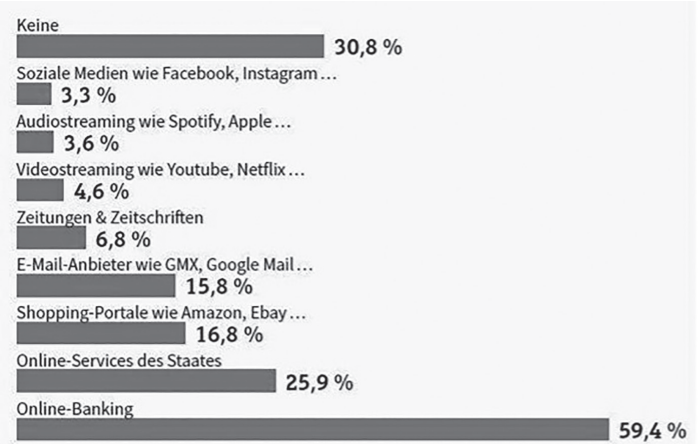


**Abbildung 1: „Welche dieser Plattformen gehen verantwortungsvoll mit ihren Identitäten um?“ (Quelle: Civey)[8]**

## 2. eIDAS-Verordnung vs. EUid

Im Juli 2014 wurde die Verordnung des Europäischen Parlaments und des Rates der WU über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt (eIDAS[9]-Verordnung) angenommen.[10] Die eIDAS-Verordnung regelt Vertrauensdienste[11], elektronische Signaturen[12], elektronische

5 https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/european-digital-identity_de (abgerufen am 5.11.2021).
6 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 und zur Aufhebung der Richtlinie 1999/93/EG.
7 Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zur Änderung der Verordnung (EU) Nr. 910/2014 im Hinblick auf die Schaffung eines Rahmens für eine europäische digitale Identität, COM/2021/281 final vom 3. Juni 2021, S. 1–2.
8 Hafen, Die prekäre Zukunft der digitalen Identität (abrufbar unter: https://computerwelt.at/news/die-prekaere-zukunft-der-digitalen-identitaet; abgerufen am 14.11.2021).
9 Vgl. Englisch: electronic IDentification, Authentication and trust Services.
10 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 und zur Aufhebung der Richtlinie 1999/93/EG.
11 Art 3 Z 16 eIDAS-Verordnung definiert „Vertrauensdienste“ als einen elektronischer Dienst, der in der Regel gegen Entgelt erbracht wird und aus Folgendem besteht: a) Erstellung, Überprüfung und Validierung von elektronischen Signaturen, elektronischen Siegeln oder elektronischen Zeitstempeln, von Diensten für die Zustellung elektronischer Einschreiben, elektronischer Attributsbescheinigungen sowie diese Dienste betreffende Zertifikate; b) Erstellung, Überprüfung und Validierung von Zertifikaten für die Website-Authentifizierung; c) Bewahrung von diese Dienste betreffenden elektronischen Signaturen, Siegeln oder Zertifikaten; d) elektronische Archivierung elektronischer Dokumente; e) Verwaltung elektronischer Fernsignatur- und -siegelerstellungseinheiten; f) Aufzeichnung elektronischer Daten in einem elektronischen Vorgangsregister.
12 Art 3 Z 12 eIDAS-Verordnung definiert „Elektronische Signatur“ als „Daten in elektronischer Form, die anderen elektronischen Daten beigefügt oder logisch mit ihnen verbunden werden und die der Unterzeichner zum Unterzeichnen verwendet“.

Siegel[13], elektronische Zeitstempel[14], Dienste für elektronische Einschreiben und Zertifikate für die Webseite-Authentifizierung[15]. Die Kommission baut auf einem bereits bestehenden rechtlichen Rahmen auf und muss nicht bei null beginnen. Die eIDAS-Verordnung bildet die Grundlage für den neuen Vorschlag der Europäischen Kommission hinsichtlich einer Verordnung bezogen auf die Schaffung eines Rahmens für eine einheitliche europäische digitale Identität.[16] Dieser Vorschlag soll die geltende eIDAS-Verordnung ändern. Der neue Verordnungsvorschlag soll nach den Plänen der Europäischen Kommission ein harmonisiertes Sicherheitskonzept für Unionsbürger bieten, die einer EUid im Online-Bereich vertrauen. Es soll auch eine gemeinsame technische Architektur entwickelt werden.[17]

## 3. Identitätsprüfung im Rahmen des Online-Bankings

Jede Banking-Innovation beginnt beim Zahlungsverkehr.[18] Die Identifikation von Kunden im Ferngeschäft stellt aufgrund einer fortgeschrittenen Digitalisierung eine große Herausforderung für Kredit- und Finanzinstitute dar. Die Kredit- und Finanzinstitute sind aufgrund ihrer kundenbezogenen Sorgfaltspflichten verpflichtet, bestimmte Dokumente, Daten und Informationen, die von einer glaubwürdigen und unabhängigen Quelle stammen, einschließlich elektronischer Mittel für die Identitätsfeststellung, betreffend ihrer Kunden einzuholen und aufzubewahren.[19] Der Zweck der Identitätsprüfung ist die Verhinderung der Geldwäsche und Terrorismusfinanzierung. Diese kundenbezogenen Sorgfaltspflichten werden als KYC-Verfahren („know your customer“) bezeichnet. Sie werden in FM-GwG[20], das auf Kredit- und Finanzinstitute sowie auf Dienstleister in Bezug auf virtuelle Währungen (Verpflichtete) anzuwenden ist, geregelt (§ 1 Abs 1 FM-GwG). Die Sorgfaltspflichten gegenüber Kunden[21] umfassen u. a. „Feststellung der Identität des Kunden und Überprüfung der Identität auf Grundlage von Dokumenten, Daten oder Informationen, die von einer glaubwürdigen und unabhängigen Quelle stammen, einschließlich elektronischer Mittel für die Identitätsfeststellung und einschlägiger Vertrauensdienste gemäß der Verordnung (EU) Nr. 910/2014 und anderer sicherer Verfahren zur

---

13 Art 3 Z 29 eIDAS-Verordnung definiert „Elektronische Siegel“ als „eine elektronische Bescheinigung oder ein Satz elektronischer Bescheinigungen, die bzw. der elektronische Siegelvalidierungsdaten mit einer juristischen Person verknüpft und den Namen dieser Person bestätigt.“

14 Bestätigung, dass ein Dokument zu einem bestimmten Zeitpunkt in der gegebenen Form vorlag. Vgl. dazu Bundesnetzagentur (abrufbar unter: https://www.bundesnetzagentur.de/EVD/DE/Verbraucher/Vertrauensdienste/Zeitst empel/Zeitstempel.html; abgerufen am 15.11.2021).

15 Die Zustellung elektronischer Einschreiben ermöglicht die Übermittlung von Daten zwischen Dritten auf elektronischem Weg und weist dabei nach, dass die Daten versandt und empfangen wurden (abrufbar unter: https://www.bitkom.org/Themen/Datenschutz-Sicherheit/Datenschutz/Bitkom-Trusted-List/Elektronische-Einschreib-und-Zustelldienste.html; abgerufen am 15.11.2021).

16 Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zur Änderung der Verordnung (EU) Nr. 910/2014 im Hinblick auf die Schaffung eines Rahmens für eine europäische digitale Identität, COM/2021/281 final vom 3. Juni 2021.

17 Eberwein/Martino, Digitale Identität für EU-Bürger, Öffentliche Sicherheit 9–10/21, S. 93 (93).

18 In einer Umfrage der Trustly Group AG gaben gerade einmal 36 % der befragten niederländischen Bankkunden, beim Onlinebanking Log-in zur Authentifikation ihren Benutzernamen und Passwort anzugeben. 25 % der Kunden bevorzugen einmalig generierte Tokens, 22 % das chipTAN-Verfahren (bei dem der Chip der Bankkarte von einem Kartenlesergerät geprüft wird), 19 % bevorzugen mTAN (über einen SMS-Code), 12 % pushTAN (ebenfalls einmalig generierter Code), 5 % den Zugang über eine Codekarte mit einmaligem Code, 3 % Anrufverifizierung und lediglich 9 % nutzen andere Methoden oder sind sich nicht sicher. Vgl. dazu Mühl, Bank 4.0, S. 192. Im Banking gibt es aktuell neun gängige TAN-Verfahren, wobei „TAN“ für eine einmal gültige Transaktionsnummer steht. Diese sind detailliert in Mühl, Bank 4.0, S. 192ff aufgezählt.

19 Gorzala, Online-Identifikation von Bankkunden, ÖBA 2019, S. 120 (120); Koch in Zankl, Rechtshandbuch der Digitalisierung Kap 21 Rz 21–29.

20 Bundesgesetz zur Verhinderung der Geldwäscherei und Terrorismusfinanzierung im Finanzmarkt (Finanzmarkt-Geldwäschegesetz – FM-GwG), BGBl I 2018/118.

21 Die Sorgfaltspflichten gegenüber Kunden sind in folgenden Fällen anzuwenden: i) Begründung einer Geschäftsbeziehung, ii) bei Durchführung von allen nicht in den Rahmen einer Geschäftsbeziehung fallenden Transaktionen (gelegentliche Transaktionen), iii) bei jeder Einzahlung auf Spareinlagen und bei jeder Auszahlung von Spareinlagen, wenn der ein- oder auszuzahlende Betrag mindestens 15 000 EUR oder EUR-Gegenwert beträgt, iv) wenn der Verdacht oder der berechtigte Grund zu der Annahme besteht, dass der Kunde einer terroristischen Vereinigung (§ 278b StGB) angehört oder dass der Kunde objektiv an Transaktionen mitwirkt, die der Geldwäscherei (§ 165 StGB – unter Einbeziehung von Vermögensbestandteilen, die aus einer strafbaren Handlung des Täters selbst herrühren) oder der Terrorismusfinanzierung (§ 278d StGB) dienen; v) bei Zweifeln an der Echtheit oder der Angemessenheit zuvor erhaltener Kundenidentifikationsdaten (§ 5 FM-GwG).

Identifizierung aus der Ferne oder auf elektronischem Weg [...]" (§ 6 Abs 1 Z 1 FM-GwG). Die Überprüfung der Identität gemäß § 6 Abs 1 Z 1 FM-GwG hat bei einer natürlichen Person durch die Vorlage eines amtlichen Lichtbildausweises zu erfolgen.[22]

Neben der Identifizierung bei einer Bank, welche derzeit über die Zwei-Faktoren-Authentifizierung und Social-Media-Identitäten[23] läuft, welche teilweise auch zur Abwicklung von Zahlungen (insbesondere Micro-Payment) dienen, steht derzeit die digitale Identität als Gegenpol im Raum.[24] Bei der Eröffnung eines Bankkontos wird künstliche Intelligenz eine Rolle bei der Erkennung des Personalausweises, insb. bei der Erkennung des darauf befindlichen Hologramms, spielen. Während sich die Mehrheit der Gesellschaft noch daran gewöhnt, für Identifikationsverfahren nicht persönlich zur Bank gehen zu müssen, ist die Identifizierung via Webcam oder PostIdent-Verfahren vielen Innovator und Early Adopters zu aufwendig. Es bieten sich deshalb neue Authentifikationsverfahren an. Die FMA-konforme Verifizierung der eigenen Identität für Kunden sollte vereinfacht werden, indem auf voll-automatisierte Hologrammüberprüfung abgestellt und zukünftig das veraltete PostIdent-Verfahren ersetzt wird.[25] Mit dem neuen Verfahren werden die Kunden angesprochen, die für die Verifizierung ihrer Person komplett auf menschlichen Kontakt verzichten möchten.[26]

## 4. Etablierung von Ökosystemen und Vorteile der EUid

Digitale Identität spielt auch im Rahmen von „Banking-as-a-Platform"-Lösungen eine Rolle. Das einheitliche Ökosystem stellt den Bankkunden alle gewünschten und relevanten Anwendungen und Dienstleistungen bereit; die Finanzdienstleistungen sind darin eingebettet. Mobile Payments, selbstverwaltete digitale Identitäten, Machine-to-Machine-Payments, Digitale Zwillinge, Tokenisierung und digitale Währungen erfordern solche Ökosysteme. Jede Person sowie jedes Objekt besitzt de facto eine digitale Identität, weil sowohl die Menschen als auch die Maschinen im Netz Datenspuren hinterlassen.[27]

Datensicherheit ist eine der wesentlichen Herausforderung des digitalen Zeitalters. Mehrere Zugänge zu Accounts zu haben und diese auf dem PC/Mac abzuspeichern ist nicht unbedingt sicher. Die Lösung dafür sind sogenannte Passwort-Manager, aber sie haben eine Schwachstelle: Man braucht ein Hauptpasswort als Zugang. Ist dieses geknackt, liegen alle Zugänge offen. Für Finanzanliegen sind Passwort-Manager nicht sicher. Neue Formen der Identifizierung und Authentifikation sollen hier Abhilfe schaffen. Sicher sind die Daten, wenn Unternehmen auch sicherstellen können, dass die Identität authentisch ist (also von der Person stammend für die sie sich ausgibt).[28]

Die digitale Identität könnte im Bereich von automatisierten Wertetransfers in DLT-Systemen zur Anwendung kommen. Zum Beispiel könnte die digitale Identität die Voraussetzung für den Zugriff auf Plattformen, die den Kauf und Verkauf von neuen Finanzprodukten („Digital Assets") anbieten, sein. Das würde die Gefahr der Geldwäsche und Terrorismusfinanzierung verringern und mehr Sicherheit für alle Beteiligten und Regulierung auf diesem neuen Markt anbieten. Die Praxis hat ebenfalls gezeigt, dass Banken Sicherheitslücken

---

22 Als amtlicher Lichtbildausweis in diesem Sinn gelten von einer staatlichen Behörde ausgestellte Dokumente, die mit einem nicht austauschbaren erkennbaren Kopfbild der betreffenden Person versehen sind und den Namen, das Geburtsdatum und die Unterschrift der Person sowie die ausstellende Behörde enthalten (§ 6 Abs 2 Z 1 FM-GwG). Bei juristischen Personen erfolgt die Überprüfung der Identität gemäß § 6 Abs 1 Z 1 FM-GwG anhand von beweiskräftigen Urkunden, die gemäß dem am Sitz der juristischen Personen landesüblichen Rechtsstandard verfügbar sind. Jedenfalls zu überprüfen sind der aufrechte Bestand, der Name, die Rechtsform, die Vertretungsbefugnis und der Sitz der juristischen Person (§ 6 Abs 2 Z 2 FM-GwG).

23 zB Apple Pay.

24 Eberwein, Digitalisierung vorantreiben, Öffentliche Sicherheit 5–6/21, S. 83 (84).

25 Die Identifizierung per Post ist für viele Nutzer nicht mehr zeitgemäß.

26 Steinschaden, Wie Europas Fintechs digitale Identität in den Mainstream bringen (abrufbar unter: https://www.trendingtopics.eu/wie-europas-fintechs-digitale-identitaet-in-den-mainstream-bringen/; abgerufen am 10.12.2021); Mühl, Bank 4.0, S. 200; IT Finanzmagazin (2018H): Nect startet Selfie-Ident für Banken & Versicherer: Identitätsfeststellung in 2 Minuten – per KI-Analyse! In: IT Finanzmagazin (16.11.2018), https://www.it-finanzmagazin.de/nect-selfie-ident-2-minuten-ki-80951/ (abgerufen am 13.11.2021).

27 Andrae, Digitale Kompetenzen im Corporate Banking, S. 12.

28 Mühl, Bank 4.0, S. 192.

in Bezug auf Erkennung von Kunden mit gleichem Namen haben. Beispielsweise ist bei Datenzwillingen schwer ersichtlich, ob es sich tatsächlich um mehrere Personen handelt. EUid könnte da Verbesserungen bringen, indem die Identität eines Kunden an die digitale Identität geknüpft wird.

## 5. Beispiel: Beantragung eines Bankkredits nach bisheriger und zukünftiger Rechtslage

Die europäische digitale Identität kann in unterschiedlichen Fällen zur Anwendung kommen und zwar u. a. bei der Nutzung aller öffentlichen Dienste wie z. B. Beantragung von Geburtsurkunden, Eröffnung eines Bankkontos, Einreichung der Steuererklärung, Bewerbung an einer Hochschule, Speicherung eines ärztlichen Rezepts, Altersnachweis, Anmietung eines Autos mit digitalem Führerschein, Check-in in einem Hotel usw.[29]

Die Beantragung eines Bankkredits ist für die Kreditnehmer aufgrund zahlreicher (persönlicher) Termine sehr aufwendig. Die Kreditnehmer müssen grundsätzlich nach der Vorbesprechung bei der Bank die Dokumente (persönlich) einreichen. Die EUid bringt die Neuerungen dadurch, dass die für das Bankgeschäft benötigten Dokumente (vom nationalen Personalausweis bis zum Einkommensnachweis) direkt aus der digitalen Brieftasche ausgewählt und der Bank übermittelt werden können. Der Kreditnehmer entscheidet selber, welche Dokumente er der Bank zur Verfügung stellen möchte. Die überprüfbaren digitalen Dokumente werden somit erstellt und sicher zur Überprüfung an die Bank gesandt, die dann das Antragsverfahren fortsetzen kann.[30]

EUid könnte der erste große Schritt in der völligen end-to-end-Digitalisierung des Kreditprozesses sein. EUid bringt die Neuerung, dass ein Kredit ohne physische Anwesenheit der Kunden beantragt werden kann. Es stellt sich aber die Frage was nach der Beantragung des Kredits passiert. Eine völlige end-to-end-Digitalisierung des Kreditprozesses ist insbesondere im Hinblick auf die Wohnraum-Finanzierung zukunftsrelevant. Immobilien-Transaktionen können heute bereits vollständig digital abgewickelt werden. Dementsprechend könnten die Kunden rein mit der Verwendung der EUid von zuhause einen Wohnraum-Kredit beantragen und die gesamte Dokumentation und die notarielle Abwicklung digital durchführen.


**Abbildung 2: Beantragung eines Bankkredits mit EUid (Quelle: Europäische Kommission)[31]**

[29] https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/european-digital-identity_de (abgerufen am 14.11.2021).
[30] https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/european-digital-identity_de (abgerufen am 14.11.2021).
[31] https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/european-digital-identity_de (abgerufen am 14.11.2021).

## 6. Die Rechtslage in den USA

Laut einer im August 2020 von der „National Retail Federation und Forrester“ veröffentlichten Studie hat in den USA jeder fünfte Käufer während der Pandemie zum ersten Mal kontaktlos bezahlt.[32] Dies hat dazu geführt, dass sich die Finanzbranche mit verbesserter Sicherheit beschäftigen muss.[33] Während die Notwendigkeit einer digitalen ID feststeht, ist die Form, die sie annehmen wird, weniger klar. Es gibt zwei Hauptherausforderungen, die Zahlungsanbieter mit einer potenziellen neuen Identitätslösung bewältigen müssen: Das Onboarding neuer Benutzer und die Sicherstellung, dass die digitale ID mit allen Transaktionen kompatibel ist.[34]

Den USA fehlt eine umfassende Strategie für digitale IDs. Präsident Obama hat im April 2011 die Nationale Strategie für vertrauenswürdige Identitäten im Cyberspace veröffentlicht. Diese Strategie hat darauf abgezielt, die Sicherheit im Cyberspace und im E-Commerce zu verbessern.[35] Diese wurde von den Dienstleistern allerdings nie national angenommen. Der Kongress-Abgeordnete Foster hat im September 2020 den „Improving Digital Identity Act of 2020“ eingeführt.[36] Der Gesetzesentwurf zielt darauf ab, einen regierungsweiten Ansatz zur Verbesserung der digitalen Identität zu etablieren. Mit diesem Gesetzentwurf wäre die „Improving Digital Identity Task Force“ eingerichtet worden. Damit sollte eine regierungsweite Anstrengung zur Entwicklung sicherer Methoden für Regierungsbehörden zur Validierung von Identitätsattributen zum Schutz der Privatsphäre und Sicherheit von Einzelpersonen starten und eine zuverlässige, interoperable digitale Identitätsprüfung im öffentlichen und privaten Sektor unterstützen.[37] Forster hat im Juni 2021 erneut einen Gesetzesentwurf zur Entwicklung von Rechtsvorschriften rund um die digitale Identität „Improving Digital Identity Act of 2021“ vorgelegt.[38] Es bleibt abzuwarten, ob und in welcher Form das Gesetz in Kraft treten wird.

## 7. Risken – Missbrauchsfälle – Ausblick

Es bleibt abzuwarten, wie sich mögliche Missbrauchsfälle rund um die EUid entwickeln werden: Einerseits sind Fälle denkbar, bei denen die EUid selbst gefälscht wird oder die den Missbrauch der Benutzerdaten betreffen.[39] Globale Banken, die ein mehrschichtiges Sicherheitsprogramm betreffend Cybersicherheit und moderne – auf digitaler Identität basierenden – Authentifizierungstechnologien verwenden, senken ihre anfallenden Gesamtbetrugskosten auf die Hälfte des Branchendurchschnitts. Lösungen zur Bekämpfung und

---

32 https://www.forrester.com/report/the-state-of-retail-payments-in-2020/RES162235 (abgerufen am 14.11.2021); Graziani, The value of digital identity in payments (abrufbar unter: https://www.globalbankingandfinance.com/the-value-of-digital-identity-in-payments/; abgerufen am 14.11.2021).

33 Das „Consumer Sentinel Network“ ist ein von der amerikanischen „Federal Trade Commission“ (FTC) gesteuertes Tool, das die Beschwerden über Verbraucherbetrug und Identitätsdiebstahl verfolgt. Im Jahr 2020 gingen bei der FTC 4,8 Millionen Identitätsdiebstahl- und Betrugsmeldungen ein, 45 % mehr als im Jahr 2019 (3,3 Millionen Meldungen). Der Grund dafür ist hauptsächlich ein Anstieg von 113 % der Beschwerden über Identitätsdiebstahl. Im Jahr 2020 betrafen 1,4 Millionen Beschwerden Identitätsdiebstahl, gegenüber 651.000 im Jahr 2019. Beschwerden über Identitätsdiebstahl machten 29 % aller bei der FTC eingegangenen Beschwerden aus, gegenüber 20 % im Jahr 2019. Von allen Meldungen, die die FTC im Jahr 2020 erhielt, betrafen die meisten die Beschwerden über Identitätsdiebstahl. Vgl. dazu Birch, Digital Identity should be a big business for banks (abrufbar unter: https://www.forbes.com/sites/davidbirch/2021/09/16/digital-identity-should-be-a-big-business-for-banks/?sh=520368b57c3f; abgerufen am 14.11.2021).

34 Graziani, The value of digital identity in payments (abrufbar unter: https://www.globalbankingandfinance.com/the-value-of-digital-identity-in-payments/; abgerufen am 14.11.2021).

35 https://obamawhitehouse.archives.gov/blog/2011/04/15/president-obama-releases-national-strategy-trusted-identities-cyberspace (abgerufen am 14.11.2021).

36 https://foster.house.gov/sites/foster.house.gov/files/Digital%20Identity%20Act%20of%202020%20%28FOSTER_065_xml%29.pdf (abgerufen am 14.11.2021).

37 https://www.congress.gov/bill/116th-congress/house-bill/8215 (abgerufen am 14.11.2021).

38 https://foster.house.gov/media/in-the-news/us-congressmen-reintroduce-sweeping-digital-id-bill; https://www.congress.gov/bill/117th-congress/house-bill/4258?r=81&s=1 (abgerufen am 14.11.2021).

39 Eberwein/Martino, Digitale Identität für EU-Bürger, Öffentliche Sicherheit 9–10/21, S. 93 (94).

Prävention von Cyberkriminalität sind zunächst kostspielig, doch führen zu zukünftigen Einsparungen.[40] Das weitere Einsparungspotential findet sich in Hinblick auf die Zwei-Faktor-Identifizierung. Banken können nicht wie Privatkunden eine Flatrate kaufen, sondern müssen pro SMS durchschnittlich sechs Cent bezahlen. Große Banken haben für die Transaktionen ihrer Kunden einen hohen Kostenfaktor zu tragen, weshalb die Zukunft dieses Modells fraglich ist.[41]

Die Idee einer digitalen europäischen Identität wird vom „Bundesverband öffentlicher Banken Deutschlands" (VÖB) grundsätzlich begrüßt.[42] Ihrer Meinung nach muss die Wirkung des Gesetzesvorschlags eingehend geprüft werden. „Die EU-Kommission erwartet u. a., dass Banken die EUid für den Zugang zum Online-Banking implementieren und anbieten. Der erheblichen Investitionserfordernis der Banken steht eine nicht quantifizierbare Nutzung der EUid durch die Kunden gegenüber, da diese freiwillig ist. Die Bestimmungen der PSD2 [zweite Zahlungsdiensterichtlinie (EU) 2015/2366] nach unserer [VÖB] bisherigen Einschätzung nicht ausreichend berücksichtigt. Zudem ist die Frage ungeklärt, wer haftet z. B. wenn Zahlungen missbräuchlich mit Hilfe der EUid autorisiert werden. Zudem ist unklar, wie sich Banken in die Governance der EUid einbringen können."[43] Die Kritik des „Bundesverbands öffentlicher Banken Deutschlands" zeigt eine Reihe berechtigter Fragen auf. Diese stellen sich auch im Hinblick auf die Sicherheit der EUid bezüglich des Datenschutzes.[44] Denn nach der EU-Datenschutzgrundverordnung dürfen persönliche Daten nur für genau spezifizierte Zwecke im minimal nötigen Umfang erhoben und verarbeitet werden. Eine Sammlung und Speicherung umfassender Daten zu allgemeinen Verwaltungszwecken würde dieser Vorschrift widersprechen. Übrigens müssen die persönlichen Daten auch gelöscht werden, nachdem der spezifische Zweck ihrer Erhebung entfällt oder der Betroffene ihre Zustimmung zur Speicherung widerrufen hat.[45] Mit der Anwendung der Blockchain-Technologie treten andere Probleme auf: Alle Einträge bauen aufeinander auf, die einzelne Informationen können aber nicht gelöscht werden, weil ansonsten die Korrektheit der weiteren Informationen nicht mehr überprüft werden kann.

Es ist unklar, ob die Banken verpflichtet sein werden, den Kunden die Benutzung der EUid anzubieten – insbesondere deswegen, weil die EUid den Bürgern freiwillig zur Verfügung gestellt wird. Die Banken müssen ebenfalls mit großen Kosten für die Schaffung technischer Rahmenbedingungen (für die Verwendung von EUid) rechnen und ebenso Kosten für die Instandhaltung der technischen Systeme berücksichtigen. Ob der Staat oder die Banken die Kosten dafür tragen ist ebenfalls unklar. Unserer Meinung nach sollte der Staat die Anschaffungskosten übernehmen, weil bei Überwälzung der Kosten auf die Banken die Gefahr besteht, dass die Banken dieselben Kosten weiter auf die Kunden überwälzen. Außerdem liegt es im staatlichen Interesse, die Hoheit über die Identität ihrer Bürger zu haben.

Die digitale Identität könne künftig als Menschenrecht gesehen werden. Auch könnte das Reisen ohne schriftliche Dokumente möglich sein. Die digitale Identität ist nicht für Banking, sondern auch in anderen Bereichen wie Gesundheit, Verwaltung und e-commerce relevant. Die Kritik wird im Hinblick auf die globale Überwachung der Bürger und die Cybersicherheit geübt, weil niemand die Hacker-Techniken der Zukunft kennt. Um das Vertrauen der Bevölkerung in EUid zu steigern, könnte in der digitalen Brieftasche die Option entwickelt

40 Mühl, Bank 4.0, S. 82.

41 Mühl, Bank 4.0, S. 193.

42 Bundesverband Öffentlicher Banken Deutschlands (Hrsg.), Kreditwirtschaftlich wichtige Vorgaben der EU, Oktober 2021, S. 236f (abrufbar unter: https://kredwi.voeb.de/2/; abgerufen am 6.11.2021).

43 Bundesverband Öffentlicher Banken Deutschlands (Hrsg.), Kreditwirtschaftlich wichtige Vorgaben der EU, Oktober 2021, S. 236f (abrufbar unter: https://kredwi.voeb.de/2/; abgerufen am 6.11.2021).

44 Aus technischer Sicht spielt das API-Banking (Application Programming Interface Banking; Deutsch: Programmierschnittstelle-Banking) eine Rolle. Es ist bisher unklar, wie die Banken auf die Daten von Kunden, die in der digitalen Brieftasche gespeichert sind, zugreifen werden. Über APIs wird die einfache und schnelle Integration von Daten oder Banking-Funktionen in die Applikationen und Services von Drittanbietern ermöglicht. Vlg. dazu Bramberger, Open Banking: Neupositionierung europäischer Finanzinstitute, S. 17.

45 Art 5 Abs 1 lit e DSGVO; Vgl. Jahnel, Kommentar zur Datenschutz-Grundverordnung Art. 5 DSGVO Rz 46–50.

werden, dass die Bürger selber entscheiden, ob sie die Brieftasche in nur begrenztem Umfang „freischalten“. Die Bürger könnten z. B. die digitale Brieftasche nur für die Behördenwege „freischalten“, aber für den Zahlungsverkehr „sperren“.

## 8. Literatur

Andrae, Silvio, Digitale Kompetenzen im Corporate Banking, Carl Hanser Verlag, München 2021.

Birch, David G.W., Digital Identity should be a big business for banks (abrufbar unter: https://www.forbes. com/sites/davidbirch/2021/09/16/digital-identity-should-be-a-big-business-for-banks/?sh=520368b57c3f; abgerufen am 14.11.2021).

Bramberger, Markus, Open Banking: Neupositionierung europäischer Finanzinstitute, Springer Gabler, Wiesbaden 2019.

Bundesverband Öffentlicher Banken Deutschlands (Hrsg.), Kreditwirtschaftlich wichtige Vorgaben der EU, Berlin Oktober, 2021(abrufbar unter: https://kredwi.voeb.de/2/; abgerufen am 6.11.2021).

Eberwein, Helgo/Martino, Antonio M., Digitale Identität für EU-Bürger, Öffentliche Sicherheit 9–10/21, S. 93.

Eberwein, Helgo, Digitalisierung vorantreiben, Öffentliche Sicherheit 5–6/21, S. 83.

Graziani, Vince, The value of digital identity in payments (abrufbar unter: https://www.globalbankingandfinan ce.com/the-value-of-digital-identity-in-payments/; abgerufen am 14.11.2021).

Hafen, Thomas, Die prekäre Zukunft der digitalen Identität (abrufbar unter: https://computerwelt.at/news/die-prekaere-zukunft-der-digitalen-identitaet; abgerufen am 14.11.2021).

IT Finanzmagazin (2018H): Nect startet Selfie-Ident für Banken & Versicherer: Identitätsfeststellung in 2 Minuten – per KI-Analyse! In: IT Finanzmagazin (16.11.2018), https://www.it-finanzmagazin.de/nect-selfie-ident-2-minuten-ki-80951/ (abgerufen am 13.11.2021).

Jahnel, Dietmar, Kommentar zur Datenschutz-Grundverordnung, Jan Sramek Verlag, Wien 2021.

Mühl, Kim Y., Bank 4.0, BoD, Hamburg 2020.

Gorzala, Jeannette, Online-Identifikation von Bankkunden, ÖBA 2019, S. 120.

Koch, Bernhard in Zankl, Wolfgang, Rechtshandbuch der Digitalisierung, Manz Verlag, Wien 2021.

Steinschaden, Jakob, Wie Europas Fintechs digitale Identität in den Mainstream bringen (abrufbar unter: https://www.trendingtopics.eu/wie-europas-fintechs-digitale-identitaet-in-den-mainstream-bringen/; abgerufen am 10.12.2021).

* Die Darstellung gibt die wissenschaftliche Meinung der Autoren wieder und ist weder als Äußerung im Rahmen der Dienstpflicht noch als Rechtsauffassung der Behörde zu verstehen.