DEUTSCHE
BUNDESBANK
EUROSYSTEM

Nutzung elektronischer Identifizierungsmittel (eIDs) im elektronischen Zahlungsverkehr und bei der Kontoeröffnung

herausgegeben vom Arbeitskreis eID

Zusammensetzung des Arbeitskreises eID

Vorsitz:
Dr. Heike Winter, Johannes Gerling, Karola Roth
Deutsche Bundesbank

Mitglieder:
Stephan Mietke
Bundesverband deutscher Banken e.V. (Bankenverband)

Martin Stein, Isabell Wingenbach
Deutscher Sparkassen- und Giroverband (DSGV)

Dr. Olaf Jacobsen
Bundesverband der Deutschen Volksbanken und Raiffeisenbanken e.V. (BVR)

Stephan Dumröse
Bundesverband der Zahlungs- und E-Geld-Institute (bvzi)

Regina Deisemann, Sabine Brüggemann
Verband Deutscher Treasurer e.V. (VDT)

Julian Grigo, Rebekka Weiß
Bitkom – Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V.

Sebastian Schulz
Bundesverband E-Commerce und Versandhandel Deutschland e.V. (bevh)

Gabriele Sieck, Dr. Mareike Lohmann, Agnes Speil
Gesamtverband der Deutschen Versicherungswirtschaft (GDV)

Ulrich Binnebößel
Handelsverband Deutschland (HDE)

Sachverständige staatlicher Stellen in beobachtender Funktion:
Barbara Buchalik, Dominic Steinrode, Julia Kowalski
Bundesministerium der Finanzen (BMF)

Andreas Polster
Bundesministerium des Inneren, für Bau und Heimat (BMI)

Stephan Kohzer, Rainer Schönen
Bundesamt für Sicherheit in der Informationstechnik (BSI)

Zeitweise einbezogen:
Dr. Stefan Afting, Marlene Letixerant
Bundesministerium für Wirtschaft und Energie (BMWi)

Dr. Stephanie Müller, Christian Kassman
Bundesbeauftragter für den Datenschutz und die Informationsfreiheit (BfDI)

Olaf Clemens
Bundesdruckerei

Inhaltsverzeichnis

Executive Summary

Die Digitalisierung des Wirtschaftslebens erfordert eine sichere elektronische Identifizierung und Authentifizierung von Geschäftspartnern. Wesentliche Voraussetzung ist die Etablierung geeigneter elektronischer Identifizierungsmittel (eIDs). Dies gilt umso mehr für das Angebot digitaler Zahlungs- und Finanzdienste, das besondere Anforderungen an die Sicherstellung der Identität von Neukunden und die Autorisierung von Transaktionen stellt.

Vor diesem Hintergrund hat sich der Arbeitskreis eID intensiv mit den Einsatzmöglichkeiten von eID-Lösungen im elektronischen Zahlungsverkehr und bei der Kontoeröffnung beschäftigt. Mit dem nun vorliegenden Bericht soll ein Beitrag zur Etablierung geeigneter eID-Lösungen im Zahlungsverkehr in Deutschland und Europa geleistet werden.

Der Bericht beschreibt zunächst die wesentlichen gesetzlichen Regelungen für den Einsatz von eIDs im Zahlungsverkehr in Deutschland. Hierzu zählen die Vorschriften des deutschen Geldwäschegesetzes (GwG), der Zweiten EU-Zahlungsdiensterichtlinie (PSD2)[1] und der eIDAS-Verordnung.[2]

Anschließend werden mögliche Anwendungsfälle für eID-Lösungen im Zahlungsverkehr aufgezeigt und dem aktuellen Ist-Zustand gegenübergestellt. Neben der Identitätsüberprüfung bei der Kontoeröffnung, dem Login in Online-Konten und der Absicherung von Transaktionen zählen hierzu auch Einsatzmöglichkeiten im Online-Handel und der Einsatz von eID-Lösungen als Basis für elektronische Signaturen.

Der darauffolgende Abschnitt gibt einen Überblick über die Funktionsprinzipien der im deutschen Markt befindlichen staatlichen und privaten eID-Lösungen, die für Einsatzwecke im Zahlungsverkehr als relevant angesehen wurden. Hierbei wird zwischen eID-Lösungen, die direkt auf die Online-Ausweisfunktion des Personalausweises (PA) aufsetzen, und weiteren relevanten privatwirtschaftlichen eID-Lösungen differenziert.

Daran anknüpfend geht der Bericht auf die Voraussetzungen für die erfolgreiche Etablierung von eID-Lösungen ein und identifiziert bestehende Hindernisse. Nach Ansicht des Arbeitskreises bringt die Online-Ausweisfunktion des PA gute Voraussetzungen mit, um die weitere Digitalisierung des Zahlungsverkehrs und der Kontoeröffnung zu unterstützen. Allerdings erfüllt sie gegenwärtig nicht alle Anforderungen des Marktes und findet in der Praxis bisher nur geringe Verwendung, sodass der Arbeitskreis die Berücksichtigung auch privater eID-Lösungen als notwendig erachtet.

Sowohl für die staatliche Online-Ausweisfunktion als auch für private eID-Lösungen bestehen derzeit jedoch noch entscheidende Hindernisse, die es für ihre breite und europaweite Akzeptanz im Bereich Zahlungsverkehr und Kontoeröffnung zu überwinden gilt. Vor diesem Hintergrund formuliert der Bericht acht Handlungsempfehlungen. Diese lauten:

- **Förderung der Marktdynamik im Bereich eID-Lösungen:**
  Angesichts der bisher geringen Verbreitung von eID-Lösungen in Deutschland sind sämtliche geeignete – öffentliche und privatwirtschaftliche – Ansätze zur vermehrten Nutzung von eIDs zu begrüßen und zu fördern.

- **Verbesserung der Voraussetzungen zur aktiven Nutzung der Online-Ausweisfunktion des PA:**
  Um die Relevanz der Online-Ausweisfunktion im

1 Richtlinie (EU) 2015/2366 des europäischen Parlaments und des Rates vom 25. November 2015 über Zahlungsdienste im Binnenmarkt, zur Änderung der Richtlinien 2002/65/EG, 2009/110/EG und 2013/36/EU und der Verordnung (EU) Nr. 1093/2010 sowie zur Aufhebung der Richtlinie 2007/64/EG

2 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

Alltag zu erhöhen, sollte die Reaktivierung von PAn mit deaktivierter Online-Ausweisfunktion vereinfacht und zeitnah mehr konkrete Anwendungsfälle in Verwaltungsverfahren ebenso wie – nach Möglichkeit – in privatwirtschaftlichen Anwendungen geschaffen werden.

- **Offene Systeme für die Nutzung von eIDs übers Smartphone:**
  Regulierungs- und Aufsichtsstellen sollten sich mit Nachdruck für die Etablierung offener Systeme und Schnittstellen für die Nutzung von eID-Lösungen übers Smartphone einsetzen und faire Wettbewerbsvoraussetzungen sicherstellen.

- **Erweiterung der Verfahren zur gesetzeskonformen elektronischen Identitätsfeststellung:**
  Um die Nutzung im Markt befindlicher Verfahren zur elektronischen Identitätsfeststellung zu ermöglichen, ohne die Integrität des Finanzsystems oder die innere Sicherheit zu gefährden, sollte der Diskurs zwischen der BaFin und den GwG-Verpflichteten hinsichtlich einer praktikablen Anwendung der regulatorischen Anforderungen des GwG fortgeführt werden.

- **Verstärkte Kooperation zwischen Wirtschaft und Staat bei der Identitätsfeststellung für private und staatliche Online-Dienste:**
  Um eine möglichst hohe Alltagsrelevanz von eID-Lösungen zu gewährleisten, sollte eine verstärkte Kooperation zwischen Wirtschaft und Staat bei der Identitätsfeststellung der Nutzerinnen und Nutzer von privaten und staatlichen Online-Diensten angestrebt werden. In diesem Zusammenhang sollte geprüft werden, ob aktuelle Freigabeverfahren für private eID-Anbieter gegenüber öffentlichen Verwaltungen vereinfacht werden könnten.

- **Überprüfung gesetzlicher Vorschriften auf alltagstaugliche Umsetzbarkeit in digitalen Prozessen:**
  Um die Vorteile des Einsatzes von eIDs voll auszuschöpfen, ist es von besonderer Bedeutung, dass neben der Identitätsüberprüfung auch alle weiteren relevanten Geschäftsprozesse digital abgebildet werden können. Zur Förderung des Einsatzes von eID-Lösungen sollten gesetzliche Anforderungen daher grundsätzlich daraufhin überprüft werden, ob und wie sie auch in digitalen Geschäftsbeziehungen sinnvoll und alltagstauglich umgesetzt werden könnten.

- **Einsatz für ein EU-weites Level-Playing-Field zur Nutzung von eID-Lösungen beim Kunden-Onboarding und der Erbringung von Vertrauensdiensten:**
  Die auf EU-Ebene angestoßenen Initiativen zur Vereinheitlichung der Rahmenbedingungen für die geldwäscherechtliche elektronische Identifizierung und Erbringung von Vertrauensdiensten sollten mit dem Ziel weiterverfolgt werden, EU-weit harmonisierte Standards herbeizuführen, die die sichere und nutzerfreundliche Verwendung von eIDs und Vertrauensdiensten im EU-weiten Finanzsektor ermöglichen und das innereuropäische Level-Playing-Field wahren.

- **Erleichterung der Notifizierung unter eIDAS für privatwirtschaftliche eID-Lösungen:**
  Der eIDAS- Interoperabilitätsrahmen ist ein wichtiges Element für die grenzüberschreitende Nutzung von eIDs in der EU. Die Hürden für die Notifizierung nach eIDAS werden von Teilen der Privatwirtschaft jedoch als sehr hoch angesehen, und zudem seien sie in Deutschland teils höher als in anderen Mitgliedstaaten. Um den ursprünglich auf Verwaltungsverfahren ausgerichteten eIDAS-Rahmen auch als wesentlichen Baustein für die Vertiefung des digitalen Binnenmarktes nutzbar zu machen, sollte geprüft werden, ob privatwirtschaftlichen Belangen stärker Rechnung getragen und die Notifizierung privater eID-Lösungen vereinfacht werden könnte.

Der Arbeitskreis eID wird die Entwicklungen im deutschen Markt für eID-Lösungen entlang der formulierten Handlungsempfehlungen weiter beobachten.

1 Einleitung

Die Digitalisierung des Wirtschaftslebens erfordert zunehmend eine sichere elektronische Identifizierung und Authentifizierung von Geschäftspartnern und die rechtssichere Abgabe von Willenserklärungen in elektronischer Form. Daher ist die Etablierung sicherer und zugleich nutzerfreundlicher elektronischer Identifizierungsmittel (eIDs)[1] elementare Voraussetzung für die weitere erfolgreiche Entwicklung der digitalen Wirtschaft. Dies gilt umso mehr für das Angebot digitaler Finanzdienste, das besondere Anforderungen an die Sicherstellung der Identität von Neukunden und die Autorisierung von Transaktionen stellt. Zur Stärkung des europäischen digitalen Binnenmarktes ist zudem auch die EU-weite Interoperabilität nationaler eID-Lösungen von besonderer Bedeutung.

Der deutsche Gesetzgeber hat den Bedarf sicherer eIDs frühzeitig erkannt und mit der Neufassung des Personalausweisgesetzes[2] (PAuswG) vom 18. Juni 2009 bereits vor rund zehn Jahren die Grundlage für eine staatliche eID-Lösung geschaffen. Seit 1. November 2010 bieten alle neu ausgegebenen Personalausweise grundsätzlich die Möglichkeit zur Verifizierung der eigenen Identität in elektronischen Transaktionen auf höchstem Sicherheitsniveau. Die Einführung des Personalausweises (PA) mit integrierter Online-Ausweisfunktion traf in der Öffentlichkeit auf große Zustimmung und war teils mit hohen Erwartungen verknüpft. Doch obwohl sich seit 2010 wirtschaftliche Transaktionen immer mehr ins Digitale verlagerten, hat sich die Nutzung der Online-Ausweisfunktion in der Breite bisher nicht durchgesetzt. Ebenso wenig haben sich im deutschen Markt bisher vergleichbare private eID-Lösungen etablieren können.

Durch das Inkrafttreten der eIDAS-Verordnung[3] am 1. Juli 2016 sowie die Novellierung des Geldwäschegesetzes[4] (GwG) im Juni 2017 und des PAuswG im Juli 2017 haben sich die Rahmenbedingungen für den Einsatz von eID-Lösungen im Online-Zahlungsverkehr und bei der Kontoeröffnung zuletzt verbessert. Als weitere Elemente kommen die Verpflichtung zur Gewährleistung des digitalen Zugangs zu allen relevanten öffentlichen Verwaltungsleistungen bis 2022 über das Onlinezugangsgesetz (OZG)[5], sowie die seit September 2019 geltenden Anforderungen der PSD2[6] an die starke Kundenauthentifizierung und die Autorisierung elektronischer Zahlvorgänge hinzu. So entsteht – nicht zuletzt auch durch neue privatwirtschaftliche Angebote von eID-Lösungen – aktuell eine neue Dynamik für die Etablierung von eID-Lösungen im Online-Zahlungsverkehr, die es zu nutzen und im Interesse der Allgemeinheit zu gestalten gilt.

---

1 Gemäß Artikel 3 der eIDAS-Verordnung beschreibt der Begriff „Elektronische Identifizierung" den Prozess der Verwendung von Personenidentifizierungsdaten in elektronischer Form, die eine natürliche oder juristische Person oder eine natürliche Person, die eine juristische Person vertritt, eindeutig repräsentieren. Ein „Elektronisches Identifizierungsmittel" wiederum ist eine materielle und/oder immaterielle Einheit, die Personenidentifizierungsdaten enthält und zur Authentifizierung bei Online-Diensten verwendet wird. Diese Definition wird für den Zweck dieses Berichts übernommen.
2 Gesetz über Personalausweise und den elektronischen Identitätsausweis (Personalausweisgesetz – PAuswG)
3 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
4 Gesetz über das Aufspüren von Gewinnen aus schweren Straftaten (Geldwäschegesetz - GwG)
5 Gesetz zur Verbesserung des Onlinezugangs zu Verwaltungsleistungen (Onlinezugangsgesetz – OZG)
6 Richtlinie (EU) 2015/2366 des Europäischen Parlaments und des Rates vom 25. November 2015 über Zahlungsdienste im Binnenmarkt, zur Änderung der Richtlinien 2002/65/EG, 2009/110/EG und 2013/36/EU und der Verordnung (EU) Nr. 1093/2010 sowie zur Aufhebung der Richtlinie 2007/64/EG

2 Zielsetzung des Arbeitskreises

Ziel des Arbeitskreises eID unter Vorsitz der Deutschen Bundesbank ist die Förderung der Verwendung sicherer, datenschutzgerechter, nutzerfreundlicher und interoperabler elektronischer Identifizierungs- und Authentifizierungsmittel im bargeldlosen Zahlungsverkehr und bei der Kontoeröffnung aus der Ferne. Konkret soll im vorliegenden Bericht erörtert werden, unter welchen Voraussetzungen vielfältig einsetzbare, also nicht auf den Zahlungsverkehr beschränkte, eID-Lösungen zur GwG-konformen Identitätsfeststellung genutzt werden sowie als Grundlage für Authentifizierungs- und Autorisierungsmittel im Onlinezahlungsverkehr dienen können.

Bei der *Identifizierung* geht es darum, die Identität des Zahlungsdienstnutzers bzw. der -nutzerin eindeutig festzustellen. Mit der *Authentifizierung* soll die Nutzeridentität oder die berechtigte Verwendung eines bestimmten Zahlungsinstruments, einschließlich der Verwendung der personalisierten Sicherheitsmerkmale des Nutzers oder der Nutzerin, überprüft werden (§ 1 Abs. 1 Nr. 23 ZAG). Bei der *Autorisierung* handelt es sich nach § 675j BGB um die Zustimmung (Einwilligung oder Genehmigung) des Zahlers bzw. der Zahlerin zum Zahlungsvorgang. Im elektronischen Zahlungsverkehr können diese drei Verfahren zeitlich und prozessual zusammenfallen.

Im Vordergrund der Betrachtungen des Arbeitskreises stehen Anwendungsfälle für natürliche Personen und technische Verfahren unter Rückgriff auf die Online-Ausweisfunktion des PA. Weitere, privatwirtschaftliche eID-Verfahren mit potenzieller Eignung für die oben genannten Anwendungsfälle werden ebenfalls berücksichtigt. Auch die Gewährleistung der EU-weiten Interoperabilität der betrachteten eID-Lösungen spielt in den Überlegungen des Arbeitskreises eine wesentliche Rolle. Das mittlerweile vielfach genutzte Videoidentifizierungsverfahren ist nicht Gegenstand der Betrachtungen des Arbeitskreises.

3 Gesetzliche Rahmenbedingungen

Bei der Erbringung digitaler Finanz- und Zahlungsdienste gilt es eine Vielzahl spezifischer Vorschriften zu beachten. Für die Zwecke des Arbeitskreises stehen konkret die Vorschriften des GwG und der Zweiten EU-Zahlungsdiensterichtlinie (PSD2) im Vordergrund. Das GwG regelt insbesondere die Anforderungen an die Identitätsfeststellung von Kundinnen und Kunden bei der Eröffnung eines Zahlungskontos in Deutschland. Mit der Umsetzung der PSD2 und ihrer begleitenden Durchführungsrechtsakte wurde ferner seit dem 14. September 2019 die starke Kundenauthentifizierung (SKA) grundsätzlich verpflichtend für Onlinekontozugriffe und die Auslösung elektronischer Zahlungsvorgänge.[7]

Der allgemeine Rahmen für den Einsatz elektronischer Identifizierungsmittel und elektronischer Vertrauensdienste in der EU wird durch die europäische eIDAS-Verordnung und die sie begleitenden Durchführungsrechtsakte geregelt. Diese schaffen einheitliche Rahmenbedingungen für die grenzüberschreitende Nutzung elektronischer Vertrauensdienste in Europa und einen Interoperabilitätsrahmen für die bei der EU-Kommission durch Mitgliedstaaten notifizierten

7 Die starke Kundenauthentifizierung gemäß PSD2 und begleitender Durchführungsrechtsakte schreibt die Authentifizierung mittels zweier unabhängiger Elemente der Kategorien „Besitz", „Wissen" und „Inhärenz" vor. Für elektronische Fernzahlungsvorgänge muss die SKA zudem eine dynamische Verknüpfung zu Zahlbetrag und Zahlungsempfänger umfassen.

Identifizierungssysteme[8] für die Verwaltung. Sie werden – ohne Rechtsbindung für den Privatsektor – auch oft allgemein als Referenzrahmen für eID-Lösungen herangezogen.

3.1 Vorschriften des Geldwäschegesetzes (GwG)

Das deutsche Geldwäschegesetz, welches in seiner aktuellen Fassung vom 23. Juni 2017 die vierte EU-Geldwäscherichtlinie[9] in deutsches Recht umsetzt, stellt an verpflichtete Institute als Teil der allgemeinen Sorgfaltspflichten strenge Anforderungen an die Identitätsüberprüfung von Vertragspartnern. Die Nutzung der Online-Ausweisfunktion des deutschen Personalausweises sowie weiterer nach eIDAS notifizierter elektronischer Identifizierungssysteme mit dem Vertrauensniveau „hoch" ist in der derzeitigen Fassung dabei ausdrücklich zulässig (vgl. hierzu die näheren Informationen in Abschnitt 4.1). Gleiches gilt für die Verwendung einer qualifizierten elektronischen Signatur (QES, ein Vertrauensdienst nach eIDAS-Verordnung, s. Abschnitt 3.3) zur Identitätsüberprüfung. Auf europäischer Ebene werden eIDs bzw. entsprechende Vertrauensdienste nach eIDAS mit Umsetzung der überarbeiteten vierten EU-Geldwäscherichtlinie[10] bis spätestens 10. Januar 2020 in allen Mitgliedstaaten der EU und des EWR ausdrücklich zulässig sein.[11] Die Anforderungen des GwG werden durch die aktuellen Auslegungs- und Anwendungshinweise (AuA) der Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) vom Dezember 2018 näher spezifiziert.[12]

3.2 Anforderungen der PSD2

Die PSD2 macht die starke Kundenauthentifizierung (SKA – vgl. Abschnitt 4.2) grundsätzlich verpflichtend beim Onlinezugriff aufs Zahlungskonto und für die Auslösung elektronischer Zahlvorgänge. Bei elektronischen Fernzahlungsvorgängen muss die SKA zudem dynamische Elemente umfassen, die die jeweilige Transaktion mit dem Betrag und dem Zahlungsempfänger verknüpfen.

Die Authentifizierung nach PSD2 soll sicherstellen, dass es sich bei dem Zahlungsdienstnutzer um den legitimen (authentischen) Nutzer handelt, der durch die Verwendung der personalisierten Sicherheitsmerkmale seine Zustimmung (Autorisierung) für den Transfer von Geldbeträgen und den Zugang zu Kontoinformationen erteilt. Eine (erneute) Identifizierung des bereits bei der Kontoeröffnung legitimierten Nutzers gegenüber dem Zahlungsdienstleister schreibt die PSD2 nicht vor.

---

8 Artikel 3 Nr. 4 der eIDAS-Verordnung definiert „Elektronisches Identifizierungssystem" als „ein System für die elektronische Identifizierung, in dessen Rahmen natürlichen oder juristischen Personen oder natürlichen Personen, die juristische Personen vertreten, elektronische Identifizierungsmittel ausgestellt werden".

9 Richtlinie (EU) 2015/849 des europäischen Parlaments und des Rates vom 20. Mai 2015 zur Verhinderung der Nutzung des Finanzsystems zum Zwecke der Geldwäsche und der Terrorismusfinanzierung, zur Änderung der Verordnung (EU) Nr. 648/2012 des Europäischen Parlaments und des Rates und zur Aufhebung der Richtlinie 2005/60/EG des Europäischen Parlaments und des Rates und der Richtlinie 2006/70/EG der Kommission

10 Richtlinie (EU) 2018/843 des europäischen Parlaments und des Rates vom 30. Mai 2018 zur Änderung der Richtlinie (EU) 2015/849 zur Verhinderung der Nutzung des Finanzsystems zum Zwecke der Geldwäsche und der Terrorismusfinanzierung und zur Änderung der Richtlinien 2009/138/EG und 2013/36/EU

11 Konkret wird Artikel 13 Absatz 1 a der 4. EU Geldwäscherichtlinie, der die Sorgfaltspflichten in Hinblick auf die Identitätsfeststellung des Kunden regelt, wie folgt angepasst: „Feststellung der Identität des Kunden und Überprüfung der Kundenidentität auf der Grundlage von Dokumenten, Daten oder Informationen, die von einer glaubwürdigen und unabhängigen Quelle stammen, einschließlich soweit verfügbar elektronischer Mittel für die Identitätsfeststellung, einschlägiger Vertrauensdienste gemäß der Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates [eIDAS Verordnung] oder mittels anderer von den zuständigen nationalen Behörden regulierter, anerkannter, gebilligter oder akzeptierter sicherer Verfahren zur Identifizierung aus der Ferne oder auf elektronischem Weg eingeholt wurden.

12 Die Auslegungs- und Anwendungshinweise der BaFin zum GwG gelten für alle Verpflichtete nach dem GwG, die unter Aufsicht der BaFin gemäß § 50 Nr. 1 GwG stehen. Sie sind abrufbar unter: https://www.bafin.de/SharedDocs/Downloads/DE/Auslegungsentscheidung/dl_ae_auas_gw_2018.html;jsessionid=EB368773 BF747DA36E14E1A3728E74E5.1_cid390?nn=9021442

Die Umsetzung der Anforderungen der PSD2 in Bezug auf die SKA in deutsches Recht erfolgt durch Artikel 55 Zahlungsdiensteaufsichtsgesetz (ZAG). Näheres zu Erfordernissen und Verfahren zur starken Kundenauthentifizierung, einschließlich etwaiger Ausnahmen von deren Anwendung sowie Anforderungen an Sicherheitsvorkehrungen für die Vertraulichkeit und die Integrität der personalisierten Sicherheitsmerkmale, werden gemäß § 55 Absatz 5 ZAG durch die unmittelbar geltenden Vorschriften der Delegierten Verordnung (EU) 2018/389 zur PSD2 („Regulatory Technical Standards for Strong Customer Authentication and Common and Secure Open Standards of Communication") geregelt.

3.3 eIDAS-Verordnung der Europäischen Union

Die eIDAS-Verordnung schafft einheitliche Rahmenbedingungen für die grenzüberschreitende Nutzung elektronischer Vertrauensdienste in der EU und im Europäischen Wirtschaftsraum (EWR).[13] Zugleich schafft sie einen technischen und regulatorischen Interoperabilitätsrahmen für die grenzüberschreitende Nutzung von bei der EU-Kommission notifizierten nationalen Identifizierungssystemen im Verwaltungsbereich. Sie löst damit die Signaturrichtlinie (Richtlinie 1999/93/EG) der EU ab und ersetzt gemeinsam mit dem deutschen Vertrauensdienstegesetz (VDG) als Durchführungsgesetz das deutsche Signaturgesetz.

Die eIDAS-Verordnung etabliert einheitliche Regelungen für die Vertrauensdienste: elektronische Signaturen, elektronische Siegel, elektronische Zeitstempel, elektronische Einschreiben und Webseiten-Zertifikate und bildet die rechtliche Grundlage für deren Gültigkeit und Anwendung in EU und EWR. Bei den Vertrauensdiensten wird zwischen allgemeinen und „qualifizierten" Vertrauensdiensten unterschieden[14], wobei qualifizierte Vertrauensdienste besonders strengen Anforderungen unterliegen. Diese Vertrauensdienste bilden eine wichtige Grundlage für sichere, rechtskräftige und effiziente Freigaben einer Vielzahl von elektronischen Transaktionen in EU und EWR. Elektronische Zahlungstransaktionen basieren allerdings überwiegend nicht auf den Vertrauensdiensten nach eIDAS, sondern auf individuell vereinbarten Mitteln zur Authentifizierung der Kundinnen und Kunden, die die Anforderungen der PSD 2 erfüllen müssen (vgl. Abschnitt 3.2). Der Vertrauensdienst der qualifizierten elektronischen Signatur (QES) ist eine Alternative unter mehreren für die GwG-konforme Identitätsüberprüfung (vgl. Abschnitte 3.1 und 4.1).

Für Vertrauensdienste nach eIDAS definiert die eIDAS-Verordnung Anforderungen an die Vertrauensdiensteanbieter[15], deren Aufsicht und an die Zusammenarbeit von Aufsichtsbehörden der Mitgliedstaaten. Vertrauensdiensteanbieter mit Sitz in der EU werden als „qualifiziert" betrachtet, wenn ihnen die Erfüllung der einschlägigen Anforderungen der eIDAS-Verordnung durch eine Konformitätsbewertungsstelle bestätigt und der Qualifikationsstatus durch die zuständige Aufsichtsbehörde verliehen wurde. Sie sind gesetzlich berechtigt, qualifizierte Vertrauensdienste in allen EU-Ländern anzubieten.[16] Als eine weitere wichtige Maßnahme für den nutzerfreundlichen Einsatz von Vertrauensdiensten im Alltag der Bürgerinnen und Bürger hat die eIDAS-Verordnung die Anforde-

---

13 Diese werden in Kapitel 3 der eIDAS-Verordnung spezifiziert.

14 Für elektronische Signaturen und elektronische Siegel wird zusätzlich näher zwischen „fortgeschritten" und „qualifiziert" differenziert, wobei „qualifiziert" dem höchsten Sicherheitsniveau entspricht.

15 Die eIDAS-Verordnung unterscheidet zwischen Vertrauensdiensteanbietern allgemein und „qualifizierten" Vertrauensdiensteanbietern. Letztere unterliegen besonderes strengen Anforderungen und einer verschärften Aufsicht. Auf diese Weise soll ein hohes Level an Vertrauen der Nutzerinnen und Nutzer in alle von qualifizierten Vertrauensdiensteanbietern erbrachten Vertrauensdienste gewährleistet werden. Sie sind gesetzlich berechtigt, qualifizierte Vertrauensdienste (z. B. qualifizierte elektronische Signaturen, Siegel oder Zertifikate) in allen EU-Ländern anzubieten.

16 Vertrauensdienste, die von Vertrauensdiensteanbietern aus einem Drittland bereitgestellt werden, werden als rechtlich gleichwertig mit den qualifizierten Vertrauensdiensten anerkannt, sofern sie im Rahmen einer geschlossenen Vereinbarung zwischen der Union und dem betreffenden Drittland oder einer internationalen Organisation anerkannt sind.

rungen an QES erheblich vereinfacht. War zu ihrer Erstellung zuvor der Einsatz von Signaturkarten und der dafür notwendigen Lesegeräte durch Endnutzer nötig, können diese nun beispielsweise auch als sogenannte Fernsignaturen von einem qualifizierten Vertrauensdiensteanbieter im Auftrag der unterzeichnenden Person erstellt werden. Dies vereinfacht die Erstellung von QES für Nutzerinnen und Nutzer erheblich und ermöglicht beispielsweise auch „cloud-basierte" Fernsignaturen vom Mobiltelefon aus. Voraussetzung für die Erstellung von QES in Form einer Fernsignatur ist die sichere Identifizierung der unterzeichnenden Person gegenüber dem Fernsignaturdienstleister.

Die eIDAS-Verordnung regelt darüber hinaus die grenzüberschreitende Nutzung von Identifizierungssystemen für öffentliche Verwaltungsdienste in der EU und im EWR. Dies tut sie durch die Schaffung eines technischen und rechtlichen Interoperabilitätsrahmens für die gemeinsame Nutzung nationaler, bei der EU-Kommission notifizierter Identifizierungssysteme im europäischen eIDAS-Netzwerk.[17] Zugleich verpflichtet sie öffentliche Stellen zur Anerkennung notifizierter Identifizierungssysteme anderer Mitgliedstaaten.[18]

Für den Privatsektor besteht keine Pflicht zur Anerkennung notifizierter Identifizierungssysteme, aber die Möglichkeit, sich an das eIDAS-Netzwerk anzubinden[19] und sich die europaweite Interoperabilität zunutze zu machen sowie ggf. auch nationale Lösungen nach Prüfung der Bundesregierung über den nationalen Single Point of Contact (in Deutschland: Bundesministerium des Innern, für Bau und Heimat, BMI) zur eIDAS-Notifizierung als Identifizierungssystem bei der EU-Kommission vorzuschlagen.[20]

Bei der Notifizierung von nationalen Identifizierungssystemen unterscheidet die eIDAS-Verordnung die Vertrauensniveaus „niedrig", „substanziell" und „hoch" und legt entsprechende Anforderungen fest.[21] Die genauen Anforderungen zur Erreichung der verschiedenen Vertrauensniveaus werden in der die eIDAS-Verordnung begleitenden Durchführungsverordnung (EU) 2015/1502[22] näher spezifiziert. Die

---

17 Jenseits der Spezifizierung technischer Mindestanforderungen und Verfahrensregeln als Grundlage für die technische Interoperabilität nationaler eID-Verfahren wird der Interoperabilitätsrahmen des eIDAS-Netzwerks durch zusätzliche Angebote der Connecting Europe Facility zur Unterstützung der Mitgliedstaaten bei der Implementierung des eIDAS Netzwerks ergänzt.

18 Mitgliedstaaten können ihre elektronischen Identifizierungsmittel bei der EU-Kommission notifizieren. Die Notifizierung erfolgt auf freiwilliger Basis, der notifizierende Mitgliedsstaat übernimmt jedoch Haftung für etwaige Schäden, die natürlichen oder juristischen Personen vorsätzlich oder fahrlässig zugefügt werden und die auf eine Verletzung der festgelegten Pflichten bei einer grenzüberschreitenden Transaktion zurückzuführen sind. Seit 29. September 2018 sind alle Mitgliedstaaten verpflichtet ihre eigenen Verwaltungsverfahren für notifizierte elektronische Identifizierungsmittel anderer Mitgliedstaaten zu öffnen, wenn die betreffenden Verwaltungsverfahren eine elektronische Identifizierung auf „substanziellem" oder „hohem" Vertrauensniveau vorsehen.

19 Das Personalausweisportal des BMI (https://www.personalausweisportal.de/DE/Wirtschaft/wirtschaft_node.html) bietet einen guten Einblick, wie die eID-Funktion des Personalausweises im Geschäftsverkehr eingebunden werden kann. Die wichtigsten Umsetzungsschritte finden sich unter: https://www.personalausweisportal.de/DE/Wirtschaft/Diensteanbieter-werden/diensteanbieter_node.html. Ein detaillierter Leitfaden für die Anbindung an das eIDAS-Netzwerk ist zudem unter https://www.personalausweisportal.de/DE/Verwaltung/eIDAS_Verordnung_EU/eID_handlungs-und_umsetzungsbedarf/eID_handlungs_und_umsetzungsbedarf_node.html verfügbar. Dieser richtet sich zwar an öffentliche Behörden, viele der enthaltenen Informationen sind aber auch für die Anbindung privatwirtschaftlicher Diensteanbieter relevant.

20 Grundsätzlich steht es allen Anbietern privater Identifizierungssysteme frei, ihre Lösungen für eine eIDAS-Notifizierung bei der EU Kommission über das BMI vorzuschlagen. Hierfür wäre analog zum Zulassungsverfahren für private Anbieter von Identifizierungs- und Authentisierungslösungen für den Zugang zu den interoperablen Nutzerkonten des Portalverbundes von Bund und Ländern (vgl.: https://www.personalausweisportal.de/DE/Wirtschaft/Zulassungsverfahren/zulassungsverfahren_node.html) eine vorgeschaltete Konformitätsüberprüfung durch das Bundesamt für Sicherheit in der Informationstechnik (BSI) hilfreich. Weitergehende Informationen zur eIDAS-Notifizierung und zum maßgeblichen Regelwerk finden sich unter: https://www.bsi.bund.de/DE/Themen/DigitaleGesellschaft/eIDAS/Elektronische_Identifizierung/eIDAS-Notifizierung./eIDAS-Notifikation_node.html

21 Die Anforderungen beziehen sich unter anderem auf die Ausgabe und Sicherheit von Identifizierungsmitteln.

22 Durchführungsverordnung (EU) 2015/1502 der Kommission vom 8. September 2015 zur Festlegung von Mindestanforderungen an technische Spezifikationen und Verfahren für Sicherheitsniveaus elektronischer Identifizierungsmittel gemäß Artikel 8 Absatz 3 der Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt

Vertrauensniveaus binden eID-Lösungen, die außerhalb des eIDAS-Interoperabilitätsrahmens zum Einsatz kommen, nicht.[23] Dennoch werden sie häufig als Referenzrahmen auch für den privatwirtschaftlichen Einsatz von eID-Lösungen herangezogen.

Zusammengenommen schafft die eIDAS-Verordnung die Grundlage für die sichere, nutzerfreundliche und rechtsverbindliche grenzüberschreitende elektronische Kommunikation in EU-weiten digitalen Geschäftsbeziehungen.

Für den Arbeitskreis eID wesentliche Elemente der eIDAS Verordnung Abbildung 1

Wesentliche Elemente der eIDAS Verordnung

Grenzüberschreitende Nutzung von eIDs in der öffentlichen Verwaltung

- eIDAS setzt nicht auf die Schaffung einer gemeinsamen EU-weiten eID-Lösung, sondern die **Interoperabilität nationaler eID-Lösungen.**
- Zu diesem Zweck: **Etablierung eines regulatorischen und technischen Interoperabilitätsramens** für nationale eID-Lösungen.
- **Notifizierung nationaler eID-Systeme** bei der EU-Kommission ermöglicht deren technische Anbindung an das eIDAS-Netzwerk und bildet die Grundlage für deren Anerkennung in Verwaltungsverfahren in anderen Mitgliedstaaten.
- **Für den Privatsektor** besteht keine Pflicht zur Anerkennung notifizierter eID-Systeme, aber die **Möglichkeit, sich auf freiwilliger Basis an das eIDAS-Netzwerk anzubinden,** um sich die europaweite Interoperabilität zunutze zu machen.
- Die für den eIDAS Interoperabilitätsrahmen entwickelten **eIDAS Vertrauensniveaus „niedrig", „substanziell" und „hoch"** binden eID-Lösungen, die außerhalb des eIDAS Interoperabilitätsrahmen zum Einsatz kommen, nicht, werden jedoch auch dort häufig als Referenzrahmen herangezogen.

Einheitlicher Regulierungsrahmen für Vertrauensdienste in EU und EWR

- eIDAS schafft **einheitliche Rahmenbedingungen** für die grenzüberschreitende **Nutzung von Vertrauensdiensten** in EU und EWR und bildet die Grundlage für deren rechtssichere Anwendung.
- Zudem: **Definition regulatorischer Anforderungen an Vertrauensdienstanbieter,** deren Aufsicht und an die Zusammenarbeit von nationalen Aufsichtsbehörden.
- **„Passporting":** in einem Mitgliedsstaat zugelassene qualifizierte Vertrauensdiensteanbieter sind berechtigt, qualifizierte Vertrauensdienste in allen Mitgliedstaaten von EU und EWR anzubieten.
- Für den Arbeitskreis ist insbesondere der **Vertrauensdienst der qualifizierten elektronischen Signatur (QES)** relevant, da dieser gemeinsam mit einer Referenzüberweisung zur GwG-konformen Identitätsüberprüfung verwendet werden kann. (vgl. Abschnitt 4.1).

23 Auch das für den Zweck dieses Berichts besonders relevante GwG stützt sich nicht auf diese Klassifizierungen.

4 Einsatzmöglichkeiten von eID-Lösungen im elektronischen Zahlungsverkehr und bei der Kontoeröffnung

eID-Lösungen können im elektronischen Zahlungsverkehr und bei der Kontoeröffnung insbesondere für Identifizierungs-, Authentifizierungs- und Autorisierungsverfahren genutzt werden. Darüber hinaus könnten eID-Lösungen, die um weitere persönliche Informationen angereichert sind, auch dazu genutzt werden, um in einem Nutzerprofil hinterlegte Zahlungs- und Rechnungsinformationen auf komfortable Weise an Geschäftspartner zu übermitteln – z.B. beim Bezahlvorgang in Onlinehandel.

4.1 Mögliche Anwendungsfälle bei der Identitätsfeststellung

Für die Identitätsfeststellung ist der wichtigste mögliche Anwendungsfall die gemäß §10 Abs. 1 Nr. 1 GwG als Teil der allgemeinen Sorgfaltspflichten von geldwäscherechtlich Verpflichteten geforderte Identifizierung des Vertragspartners. §12 Absatz 1 Nr. 2 GwG erlaubt für die Identitätsfeststellung bei natürlichen Personen ausdrücklich die Verwendung eines elektronischen Identitätsnachweises nach §18 PAuswG oder nach §78 Absatz 5 des Aufenthaltsgesetzes – also der staatlichen eID-Lösung (vgl. Abschnitt 5.1). Nach §12 Absatz 1 Satz 1 Nr. 3 und 4 GwG ist ferner auch der Identitätsnachweis mittels eines eIDAS notifizierten Identifizierungssystems des Vertrauensniveaus „hoch" oder mittels einer qualifizierten elektronischen Signatur nach Artikel 3 Nummer 12 der eIDAS-Verordnung und zusätzlicher Referenzüberweisung zulässig.[24]

Neben diesen explizit genannten Formen der elektronischen Identifizierung ist nach §13 Absatz 1 Nummer 2 GwG auch die Anwendung sonstiger, durch das Bundesministerium der Finanzen gebilligter Verfahren, die ein Sicherheitsniveau aufweisen, das der angemessenen Prüfung eines vor Ort vorgelegten Dokuments gleichwertig ist, zur Identitätsfeststellung möglich.[25]

Neben der Identifizierung durch Zahlungsdienstleister spielen eID-Lösungen auch im nicht durch das GwG regulierten Onlinehandel eine wichtige Rolle. So ist der Identitätsmissbrauch für Onlinehändler ein äußerst wichtiges Thema. Insbesondere für die Zahlartensteuerung und die Entscheidung, ob Kaufinteressierten ein Zahlungsmittel mit kreditorischem Risiko angeboten werden kann, ist die verlässliche elektronische Identifizierung sehr relevant.

Ist-Zustand

Ungeachtet der beschriebenen Zulässigkeit elektronischer Identifizierungsmittel erfolgt die Identitätsfeststellung natürlicher Personen auch bei digital angebahnten Geschäftsbeziehungen bisher oftmals nach wie vor durch persönliches Erscheinen in der Filiale, per PostIdent-Verfahren oder per Videoidentifizierung.

Möglichkeiten des Einsatzes von eID-Lösungen

eID-Lösungen könnten eine sichere und nutzerfreundliche Alternative zu den bisher zur Verfügung stehenden Methoden der GwG-konformen Identitätsüberprüfung darstellen. Die digitale Anbahnung von Geschäftsprozessen, insbesondere die Kontoeröffnung,

24 Im Fall der Identitätsüberprüfung anhand einer qualifizierten elektronischen Signatur hat der Verpflichtete eine Validierung der qualifizierten elektronischen Signatur nach Artikel 32 Absatz 1 der eIDAS Verordnung vorzunehmen. Zudem ist zum Zwecke der zusätzlichen Verifizierung die Transaktion von einem geeigneten Zahlungskonto notwendig (vgl. hierzu § 12 Absatz 1, Satz 2 ff. GwG).
25 Absatz 2, Nummer 2 des § 13 GwG besagt ferner, dass das Bundesministerium der Finanzen im Einvernehmen mit dem Bundesministerium des Innern durch Rechtsverordnung, die nicht der Zustimmung des Bundesrates bedarf, Verfahren bestimmen kann, die zur geldwäscherechtlichen Identifizierung nach Absatz 1 Nummer 2 geeignet sind.

könnte deutlich vereinfacht und der unfreiwillige Rückgriff auf papierhafte und analoge Prozesse weiter reduziert werden. Denn sowohl im B2C- als auch im B2B-Kontext (z.B. Händler-Onboarding im Acquiring, Identitätsüberprüfung von Bevollmächtigten eines Unternehmens) bestehe nach Ansicht der Mitglieder des Arbeitskreis gegenwärtig noch erhebliches Verbesserungspotenzial durch Beseitigung heutiger Medienbrüche.

eID-Lösungen, die Angaben zur Person auf Wunsch um zusätzliche Informationen wie beispielsweise Zahlungsdaten oder Rechnungs- bzw. Lieferadresse erweitern, könnten zudem im Online-Handel eine wichtige Rolle spielen. So könnten bei nutzerseitiger Zustimmung beispielsweise Zahlungsinformation sowie Rechnungs- und Lieferadresse an den Online-Händler übertragen und gleichzeitig die Käuferidentität verifiziert werden. Auf diese Weise könnte Betrug vorgebeugt und zugleich Nutzerinnen und Nutzern eine sichere und bequeme Möglichkeit der Übertragung von Zahlungs- und Rechnungsinformationen geboten werden.

4.2 Starke Kundenauthentifizierung (SKA) beim Zugriff aufs Zahlungskonto oder andere Online-Nutzerkonten

Ein weiterer möglicher Anwendungsfall für eID-Lösungen kann der Zugriff aufs Zahlungskonto sein. Seit dem 14. September 2019 ist hierfür die starke Kundenauthentifizierung (SKA) gemäß § 55 Abs. 1 Nr. 1 ZAG verpflichtender Standard. Dies bedeutet, dass die Authentifizierung des Kunden in der Regel durch zwei unabhängige Elemente der Kategorien

– Wissen (etwas, das nur der Nutzer weiß)

– Besitz (etwas, das nur der Nutzer besitzt) oder

– Inhärenz (etwas, das der Nutzer ist)

erfolgen muss.

Ist-Zustand
Bislang greifen kontoführende Institute in der Regel auf proprietäre oder sektorspezifische Authentifizierungsverfahren zurück, die sie ihren Kundinnen und Kunden selbst zur Verfügung stellen. Neben PIN oder Passwort wird der vorgeschriebene zweite Faktor in der Regel durch die Bereitstellung beispielsweise von TAN-Generatoren, photo- oder SMS-TAN-Verfahren oder die Verknüpfung eines mobilen Endgerätes mit einem Zahlungskonto ermöglicht. Die bankeigenen Verfahren für den Login ins Konto können üblicherweise auch zur Transaktionsabsicherung (vgl. Abschnitt 4.3) verwendet werden.

Möglichkeiten des Einsatzes von eID-Lösungen
Die Online-Ausweisfunktion und weitere im Markt befindliche eID-Lösungen (vgl. Kapitel 5) bieten die Möglichkeit einer PSD2-konformen SKA und kämen somit als institutsübergreifendes Authentifizierungsmittel für den Login ins Online-Banking in Frage. Nutzerinnen und Nutzer könnten hiervon profitieren, indem sie sich nicht wie bisher mit bankindividuellen Authentifizierungsmitteln vertraut machen und ggf. die jeweils notwendige Hardware mit sich führen müssten, sondern auf ein universelles Verfahren zurückgreifen könnten, das sie prinzipiell auch außerhalb des Zahlungsverkehrs zur sicheren Authentifizierung verwenden könnten.

Ob eID-Lösungen für den regelmäßigen Login ins Online-Banking tatsächlich einen Mehrwert bieten können, hängt neben der offenkundig notwendigen hohen Sicherheit und Nutzerfreundlichkeit der Lösungen auch davon ab, ob die Verfahren neben dem Login ins Zahlungskonto auch zur Absicherung von Transaktionen genutzt werden könnten und wie sich eine Abkehr von eigenen Verfahren auf die Flexibilität der kontoführenden Institute, beispielsweise im Falle der Sperrung von Authentifizierungsmitteln auswirken, würde.

Weitere Anwendungsfälle für sichere eID-Lösungen im Online-Banking könnten im Nachweis der Kunden-

identität bei der Beantragung eines Online-Banking-Zugangs (bei bereits bestehender Geschäftsbeziehung) oder beim Wechsel des Kunden auf ein anderes vom kontoführenden Institut angebotenes Sicherungsverfahren bzw. bei der Änderung wichtiger Kundendaten etwa nach Umzug bestehen. Auch bei der Mitteilung einer Kontoänderung an eine Versicherung, z.B. über deren Online-Kundenportal, könnten eID-Lösungen zum Einsatz kommen. Denn insbesondere für die Auszahlung im Schadens-/Leistungsfall muss die richtige Identität des Kontoinhabers gerichtsfest festgestellt und geprüft sein, um eine – vielleicht sogar mit krimineller Absicht veranlasste – Überweisung auf ein falsches Konto zu verhindern.

Über die Anwendungsfälle im Zahlungsverkehr hinaus besteht für eID-Lösungen grundsätzlich eine Vielzahl weiterer Einsatzmöglichkeiten für die Authentifizierung, z.B. zum elektronischen Abruf sensibler Daten, fürs Login in Online-Nutzerkonten – etwa bei der öffentlichen Verwaltung oder einer Versicherung – oder aber als Ausweichauthentifizierungslösung bei Verlust des Passworts oder Änderung der Nutzer- und/oder Zugangsdaten eines bestehenden Nutzerkontos.

4.3 Starke Kundenauthentifizierung (SKA) bei Einleitung elektronischer Zahlungsvorgänge

Seit dem 14. September 2019 ist gemäß § 55 Abs. 1 Nr. 2 ZAG auch zur Auslösung von durch den Zahler initiierten elektronischen Zahlvorgängen eine SKA erforderlich. Bei elektronischen Fernzahlungsvorgängen ist zudem zusätzlich eine „dynamische Verknüpfung" der SKA an den spezifischen Zahlbetrag und Zahlungsempfänger notwendig (§55 Abs. 2 ZAG).[26]

Ist-Zustand

Wie in Abschnitt 4.2. geschildert greifen die kontoführenden Institute bislang in der Regel auf die Verwendung eigener Lösungen unter Rückgriff beispielsweise auf TAN-Generatoren, photo- oder SMS-TAN-Verfahren oder die Verknüpfung eines mobilen Endgerätes mit einem Zahlungskonto zurück, die sowohl für den Login ins Konto als auch zur Transaktionsabsicherung verwendet werden.

Möglichkeiten des Einsatzes von eID-Lösungen

Auch zur Transaktionsabsicherung könnten grundsätzlich institutsübergreifende eID-Lösungen zum Einsatz kommen. Diese könnten perspektivisch auch als standardisierte und wettbewerbsneutrale Verfahren zur Authentifizierung von Zahlungen in verschiedensten Zahlsituation dienen (z.B. zur Authentifizierung von Instant Payment Zahlungen an der Ladenkasse). Die Online-Ausweisfunktion beispielsweise bietet technisch die Möglichkeit der Transaktionsabsicherung.[27] Die PSD2-Konformität dieser Funktion ist durch die BaFin bisher jedoch noch nicht geprüft worden.

Durch den institutsübergreifenden Einsatz von eID-Lösungen zur Transaktionsabsicherung wären Nutzerinnen und Nutzer in ihrem Alltag vermutlich auf weniger Verfahren zur Authentifizierung angewiesen.

Für kontoführende Institute würde die Attraktivität des Einsatzes externer Verfahren ähnlich wie bei der Nutzung für den Login ins Online-Banking (vgl. Abschnitt 4.2) letztlich u.a. davon abhängen, wie viel Flexibilität der Rückgriff auf Lösungen Dritter den kontoführenden Instituten bei der technischen und organisatorischen Gestaltung der Authentifizierungsverfahren und des Risikomanagements ließe.

---

26 Ausnahmen von der Verpflichtung zur SKA regeln die Artikel 10-20 der Delegierten Verordnung (EU) 2018/389 („RTS zu SCA und CSC") zur PSD2.

27 Die Online-Ausweisfunktion sieht eine sog. „TransactionInfo" ausdrücklich vor (vgl. BSI-TR-03112, Part 7, 3.6.3, TransactionInfo: „This element MAY contain transaction-related information, which MUST be displayed in the eID-PIN dialogue before the PACE-protocol is performed."). Es ist also möglich, eine Transaktion bspw. an die Anzeige eines Betrages oder Zahlungsempfängers zu binden, diese Elemente werden dann auch in das Transportprotokoll mit aufgenommen.

4.4 Anwendung zur Mandatserteilung für den Lastschrifteinzug

eID-Lösungen könnten auch eine Rolle in der rechtssicheren Authentifizierung von übers Internet erteilten SEPA-Lastschriftmandaten spielen.

Ist-Zustand

Gemäß Verständigung des SEPA-Rates und einer gemeinsamen Erklärung des Bundesministeriums der Finanzen und der Deutschen Bundesbank aus dem Jahr 2013 ist die einfache Erteilung von Lastschriftmandaten über das Internet zwar möglich,[28] der Zahlungsempfänger trägt jedoch die Darlegungs- und Beweislast eines vom Zahler erteilten Mandats. Seit 2015 sehen die Rulebooks für das SEPA-Lastschriftverfahren vor, dass neben einem schriftlichen Mandat elektronische Dokumente zulässig sind, die mittels einer „rechtlich bindenden Zeichnungsmethode" gezeichnet sind. Für die Akzeptanz der in diesem Zusammenhang denkbaren Zeichnungsmethoden maßgebend ist die Frage, ob die Übereinstimmung der Identität von Mandatserteiler und Zahler durch die Bank des Zahlers hinreichend sichergestellt werden kann.

Möglichkeiten des Einsatzes von eID-Lösungen

Der freiwillige Einsatz einer rechtssicheren und nutzerfreundlichen eID-Lösung bei der Erteilung eines elektronischen Lastschriftmandates könnte eine Möglichkeit darstellen, eine nutzerfreundliche europaweite Lösung zur beweissicheren elektronischen Erteilung von Lastschriftmandaten im Internet zu schaffen und so bestehende Rechtsunsicherheit bei Zahlungsempfängern zu reduzieren. Insbesondere bei der Erteilung von Mandaten zum wiederholten bzw. regelmäßigen Lastschrifteinzug könnten eID-Lösungen herangezogen werden. Für die Online-Ausweisfunktion gibt es beispielsweise bereits mehrere praktisch erprobte Lösungen für die Kundenauthentifizierung bei der Erteilung von SEPA-Lastschriftmandaten.

4.5 eID-Lösungen als Grundlage für elektronische Signaturen

Neben den oben aufgeführten möglichen Anwendungsfällen können eID-Lösungen allgemein als Grundlage zur Erstellung elektronischer Signaturen für vielfältige Einsatzzwecke dienen. Denn Voraussetzung für eine elektronische Signatur ist stets die zuvorige sichere Identifizierung der unterzeichnenden Person gegenüber dem Signaturdienstleister. Die potenziellen Einsatzmöglichkeiten von elektronischen Signaturen im Finanzsektor sind grundsätzlich sehr vielfältig, sollen in diesem Bericht jedoch nicht näher erörtert werden.

---

28 Die Bank des Lastschrifteinreichers entscheidet, ob sie im Internet erteilte Mandate akzeptiert. Ausschlaggebend sind die vertraglichen Vereinbarungen zwischen dem Zahlungsempfänger und seinem Zahlungsdienstleiter.

Mögliche Anwendungsfälle von eID-Lösungen im Online-Zahlungsverkehr Abbildung 2

Identitätsfeststellung	Authentifi beim L ins Kund	Authentifizierung bei der Einleitung elektronischer Zahlungsvorgänge	Mandatserteilung für den Lastschrifteinzug	eIDs als Grundlage für elektronische Signaturen
Einsatz z.B. – gemäß Anforderungen des GwG bei Kontoeröffnung – beim Check-Out im Online-Handel (auf Kundenwunsch ggf. inkl. Übertragung von Zahlungsinformationen und Rechnungs- und Lieferadresse)	**Einsatz z.B.** – zur Starken Kundenauthentifizierung (SKA) gemäß PSD2 beim Login ins Online-Banking – bei Änderung sensibler Kundendaten	**Einsatz z.B.** – zur SKA gemäß PSD2 bei der Einleitung von Fernzahlungsvorgängen – potenziell auch zur Initiierung von Instant Payment Zahlungen an der Ladenkasse	**Einsatz z.B.** – auf freiwilliger Basis zur Authentifizierung elektronischer Lastschriftmandate zur Stärkung der Rechtssicherheit bei Zahlungsempfängern	**Einsatz z.B.** – eID-Lösungen können als Grundlage zur Erstellung elektronischer Signaturen mit vielfältigen Einsatzmöglichkeiten dienen

Vielfältige Einsatzmöglichkeiten für eID-Lösungen im Online-Zahlungsverkehr und angrenzenden Diensten steigern die Relevanz von eID-Lösungen im Alltag der Bürgerinnen und Bürger und unterstützen ihre erfolgreiche Etablierung auch über den Online-Zahlungsverkehr hinaus.

5 Relevante eID-Lösungen auf dem deutschen Markt

Ein umfassendes Verständnis der im Markt befindlichen eID-Lösungen und ihrer grundsätzlichen Funktionsprinzipien ist eine wichtige Voraussetzung dafür, die Etablierung geeigneter Verfahren zu fördern und bestehende Herausforderungen für ihre Verwendung identifizieren und adäquat adressieren zu können. Aus diesem Grund gibt der folgende Abschnitt eine Übersicht über für die Zwecke des Arbeitskreises relevante eID-Lösungen im deutschen Markt.

eIDs können sehr verschieden ausgestaltet sein und mitunter sehr unterschiedliche Sicherheits- und Vertrauensniveaus aufweisen. Angesichts der spezifischen technischen Sicherheitsanforderungen im Zahlungsverkehr und der oben beschriebenen einschlägigen Vorschriften des GwG erscheinen für die vom Arbeitskreis identifizierten Einsatzzwecke insbesondere solche eID-Lösungen als relevant, die

– (potentiell)[29] eine GwG-konforme Identifizierung zulassen[30] und
– zur starken Kundenauthentifizierung eingesetzt werden könnten

Bei der Betrachtung der im Markt existierenden eID-Lösungen wird folgende Untergliederung vorgenommen: (1) eID-Lösungen, die direkt auf die Online-Ausweisfunktion des Personalausweises zurückgreifen (2) weitere relevante eID-Lösungen.

5.1 eID-Lösungen unter Rückgriff auf die Online-Ausweisfunktion des Personalausweises (PA)

Seit 1. November 2010 wird der deutsche Personalausweis mit Chip ausgegeben, der die Nutzung der Online-Ausweisfunktion erlaubt. Auch seit 2011 ausgegebene elektronische Aufenthaltstitel (eAT) enthalten die Online-Ausweisfunktion.[31] Bis Ende Oktober 2020 wird der vollständige Austausch alter Personalausweise durch neue mit Online-Ausweisfunktion erreicht.

Mit dem Gesetz zur Förderung des elektronischen Identitätsnachweises traten zum 15. Juli 2017 eine Reihe von Vereinfachungen in Kraft mit dem Ziel die Nutzerfreundlichkeit und Akzeptanz der Online-Ausweisfunktion bei Diensteanbietern, wie beispielsweise Online-Händlern oder Kreditinstituten, und Personalausweisinhaberinnen und -inhabern zu stärken. Hierzu zählen u.a. die Ausgabe jedes neuen Ausweises mit eingeschalteter Online-Ausweisfunktion[32], die vereinfachte Erteilung von Berechtigungen für Diensteanbieter zur Nutzung der Online-Ausweisfunktion, die Etablierung der neuen Funktion des „Vor-Ort-Auslesens" der Ausweisdaten[33] und die Zulassung von Identifizierungsdienstleistern, die auf Grundlage der Online-Ausweisfunktion elektronische Identifizierungsdienste für Dritte anbieten. So haben Diensteanbieter mittlerweile auch die Möglichkeit über sogenannte Identifizierungsdiensteanbieter[34] Identifizierungsdienste auf Basis der Online-Ausweisfunktion zu beziehen (eID-as-a-Service) und in das eigene Online-Angebot einzubinden. Eine Reihe von Anbietern ist bereits in diesem neuen Markt aktiv.[35]

---

29 Nach §13 Absatz 1 Nummer 2 GwG ist die Anwendung sonstiger, durch das Bundesministerium der Finanzen gebilligter Verfahren, die ein Sicherheitsniveau aufweisen, das der angemessenen Prüfung eines vor Ort vorgelegten Dokuments gleichwertig ist, zur Identitätsfeststellung möglich. Nach Auffassung der BaFin können weitere solcher sonstiger geeigneter Verfahren ausschließlich durch Rechtsverordnung gemäß § 13 Abs. 2 Nr. 2 GwG zugelassen werden (d.h. durch Rechtsverordnung des BMF in Einvernehmen mit dem BMI; vgl. hierzu Abschnitt 5.1.3.2. der Auslegungs- und Anwendungshinweise zum Geldwäschegesetz der BaFin aus dem Dezember 2018). Elektronische Identifizierungsmittel, für die eine derartige zukünftige Zulassung möglich erscheint, sollen ebenfalls Gegenstand der weiteren Betrachtungen sein.

30 Ob sich einzelne der als „weitere relevante eID-Lösungen" kategorisierten Lösungen tatsächlich zur GwG-konformen Identitätsfeststellung und weitere Anwendungen im Onlinezahlungsverkehr eignen würden, bedürfte einer eingehenden Prüfung der einzelnen Lösungen in Abhängigkeit des spezifischen Einsatzzwecks. Eine solche Prüfung – aller in Frage kommenden eID-Lösungen für alle in Frage kommenden Anwendungsfälle – ist jedoch ausdrücklich nicht Ziel dieses Berichts.

31 Die im Folgenden für die Online-Ausweisfunktion des PA getroffenen Aussagen gelten daher analog auch für die Online-Ausweisfunktion des elektronischen Aufenthaltstitels.

32 Zuvor war die Online-Ausweisfunktion des Ausweises bei Ausgabe standardmäßig deaktiviert und Bürgerinnen und Bürger mussten der Aktivierung explizit zustimmen. Mittlerweile ist ein Deaktivieren nicht mehr vorgesehen.

33 Das „Vor-Ort-Auslesen" ermöglicht bei physischer Anwesenheit des Ausweisinhabers und Identitätsprüfung gegen den Ausweis bei Einverständnis das Auslesen von in dem Chip gespeicherten personenbezogenen Daten ohne PIN-Eingabe und weiteres Zutun des Inhabers. Auf diese Weise wird die Erfassung persönlicher Daten beschleunigt und die Fehlerquellen einer manuellen Übertragung der Daten vermieden. Behörden und Unternehmen, die diese Funktion anbieten wollen, benötigen dazu eine staatliche Berechtigung (Schlüssel-Zertifikat) für das Vor-Ort-Auslesen und ein entsprechendes Lesegerät nebst Software.

34 § 2 Absatz 3a PAuswG definiert „Identifizierungsdiensteanbieter" als „Diensteanbieter, deren Dienst darin besteht, für einen Dritten eine einzelfallbezogene Identifizierungsleistung mittels des elektronischen Identitätsnachweises nach § 18 [PAuswG] zu erbringen".

35 Eine Übersicht über derzeitig im Markt befindliche Identifizierungslösungen auf Grundlage der Online-Ausweisfunktion findet sich unter: https://www.personalausweisportal.de/DE/Wirtschaft/Anwendungsbeispiele/Identifizierungsloesungen/identifizierungsloesungen_node.html

Während ein Teil der angebotenen Identifizierungsdienste direkt in das Online-Angebot integriert wird, dem gegenüber die Identifizierung stattfinden soll, werden bei anderen Lösungen die Kundinnen und Kunden zur Identitätsfeststellung zur Webseite des eID-Lösungsanbieters weiter- und anschließend wieder zum betreffenden Online-Angebot zurückgeleitet.

Diensteanbieter, die auf die Online-Ausweisfunktion zurückgreifen wollen, benötigen keine eigene oder gehostete eID-Server-Infrastruktur. Die vom Bundesamt für Sicherheit in der Informationstechnik (BSI) zertifizierten und von der Vergabestelle für Berichtigungszertifikate zugelassen Identifizierungsdiensteanbieter[36] ermöglichen eine einfache und sichere elektronische Identitätsfeststellung mit der Online-Ausweisfunktion auf dem eIDAS Vertrauensniveau „hoch" und erfüllen gleichzeitig die Anforderungen des GwG.

Voraussetzung für die Anwendung der Online-Ausweisfunktion ist, dass auf dem Personalausweis diese Funktion eingeschaltet ist. Für seit Juli 2017 ausgegebene Ausweise ist das regelmäßig der Fall. Ausweisinhaberinnen und -inhaber benötigen darüber hinaus neben ihrer PIN eine eID-Client-Software (integriert in die Anwendung oder als zusätzliche App) auf dem Smartphone, Tablet, PC/ Mac oder am Terminal. Während zum Auslesen der im Chip gespeicherten Daten bis vor ein paar Jahren darüber hinaus noch ein dediziertes Lesegerät notwendig war, können die Daten mittlerweile auch über die NFC-Funktionalität eines geeigneten Smartphones bzw. Tablets ausgelesen werden. Seit Ende September dieses Jahres ist dies auch für Apple Smartphones ab dem iPhone 7 möglich.

Die Online-Ausweisfunktion gewährleistet eine starke Kundenauthentifizierung durch Rückgriff auf die beiden Faktoren Wissen (PIN-Abfrage) und Besitz (Ausweisbesitz, kryptographisch nachgewiesen durch Chipauthentisierung) sowie die Ende-zu-Ende Verschlüsselung der Daten vom Client bis zum Server (Chip- und Terminalauthentisierung). Durch die starke Identifizierung auf hohem Vertrauensniveau ist sie das technisch sicherste Mittel für die Erstellung einer QES in Form einer eIDAS-Fernsignatur[37], sodass Identifizierungsdiensteanbieter, die zugleich qualifizierter Vertrauensdiensteanbieter sind oder mit einem solchen zusammenarbeiten, auch QES auf Basis der Online-Ausweisfunktion anbieten können. Mindestens ein Anbieter im Markt bietet zudem nach eigenen Angaben Lösungen für den PSD2-konformen Onlinezugriff aufs Zahlungskonto und die Transaktionsfreigabe an.

Durch Notifizierung bei der EU-Kommission besteht seit 29. September 2018 eine Anerkennungspflicht der Online-Ausweisfunktion durch EU Mitgliedstaaten in elektronischen Verwaltungsdiensten, wenn diese eine elektronische Identifizierung auf „substanziellem" oder „hohem" Vertrauensniveau voraussetzen.

Zur Sicherstellung der Vollausstattung der Wohnbevölkerung und Beschäftigten in Deutschland (ausgenommen nicht-EU Ausländer ohne eAT, Langzeittouristen und andere Visumsinhaber) mit einem sicheren elektronischen Identifizierungsmittel sieht ein aktueller Gesetzentwurf die Einführung der „eID-Karte" ab 1.11.2020 vor, einer Chipkarte für EU Bürgerinnen und Bürger mit der Online-Ausweisfunktion aber ohne Sichtausweisfunktion und ohne biometrische Daten.

Die Online-Ausweisfunktion des Personalausweises stellt als staatliche und wettbewerbsneutrale eID-Lösung ein wichtiges Element für die sichere digitale Identifizierung in Deutschland dar.

---

36 Die Voraussetzungen, um als Identifizierungsdiensteanbieter im Sinne des § 2 Absatz 3a PAuswG Identifizierungsleistungen auf Grundlage der Online-Ausweisfunktion des PA für Dritte erbringen zu können, werden durch § 21b PAuswG bestimmt.
37 Dazu ist der Erwerb eines entsprechenden Signatur-Zertifikats nötig. Derzeit gibt es jedoch erst einen Anbieter in Deutschland, der die notwendigen Zertifikate und den Fernsignaturdienst für die Online-Ausweisfunktion anbietet.

In Ergänzung zur Online-Ausweisfunktion unterstützt die Bundesregierung mit dem Förderprojekt „OPTIMOS 2.0" (s. Kasten) die Entwicklung einer sicheren Mobile-eID auf substantiellem Vertrauensniveau. Mit dem neuen Identifizierungsmittel wird ein gleichermaßen nutzerfreundlicher wie ausreichend sicherer Einsatz in Alltagsanwendungen in Wirtschaft und Verwaltung angestrebt.

Projekt OPTIMOS 2.0

OPTIMOS 2.0[38] soll ein offenes, praxistaugliches Ökosystem sicherer Identitäten für mobile Dienste definieren und dessen Nutzen anhand von sicheren, skalierbaren eID-Anwendungen in den Marktsektoren eID, eGovernment, Internet of Things und Mobilität exemplarisch demonstrieren.

Verbraucher nehmen heute über ihr Smartphone zahlreiche Dienste in Anspruch, die ein hohes Sicherheitsniveau voraussetzen: Sie entriegeln etwa die Türen von Carsharing-Fahrzeugen, eröffnen Bankkonten oder melden ihre neue Adresse an die Stadtverwaltung. Dazu legen sie meist direkt beim Anbieter des Dienstes eine Identität (eID) an, die dann über ein vertrauenswürdiges – meist langwieriges – Verfahren verifiziert werden muss. Hier fehlen bislang digitale Technologien mit einem ausreichend hohen Schutzniveau, die das ad hoc vom Smartphone unterstützen. Neben Login/Registrierung bei Dienstanbietern kann die sichere eID auch vor Ort mit Nahfeldkommunikationstechnologie (NFC) eingesetzt werden. Dazu hält der Nutzer das Mobilgerät nah an einen anderen Gegenstand mit NFC-Chip, etwa den Türgriff eines Hotelzimmers. Das macht die Nutzung der eID sehr einfach.

Im Projekt OPTIMOS 2.0 wird ein offenes Ökosystem etabliert, das die Technologien für sichere eID-Dienste bereitstellt. Mithilfe dieser Technologien werden eID-Dienstanbieter in die Lage versetzt, mobile eID-Services mit dem Schutzniveau „substanziell" und „hoch" nach der EU-Verordnung über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen (eIDAS) anzubieten. Das im Projekt entwickelte Ökosystem soll auf dem Schutzniveau „substantiell" bei der EU notifiziert und dadurch in ganz Europa anwendbar gemacht werden.

Anbieter von mobilen Services können von dem offenen Ökosystem profitieren, wenn sie neben der eID weitere sensible Daten auf dem Smartphone ablegen wollen: Fluggesellschaften beispielsweise die Bordkarte, Verkehrsbetriebe eine persönliche Jahreskarte oder Car-Sharing-Unternehmen und Hotels den digitalen Autoschlüssel resp. Zimmerschlüssel. Diese anwendungsspezifischen Daten auf dem Smartphone der Kunden sicher abzulegen, ist bislang für jeden Service-Anbieter eine komplexe Herausforderung. Denn unterschiedliche Handy-Arten und Mobilfunkanbieter sorgen für große Heterogenität bei der Hardware. Das Förderprojekt OPTIMOS 2.0 soll eine Plattform schaffen, die den Service Providern den aufwändigen Teil abnimmt und gleichzeitig eine hohe hardwaregestützte Sicherheit ermöglicht.

OPTIMOS 2.0 ist ein Forschungsprojekt, das vom Bundesministerium für Wirtschaft und Energie im Rahmen der Smart Service Welt II gefördert wird. Das Bundesministerium des Innern, für Bau und Heimat und das Bundesamt für Sicherheit in der Informationstechnik sind in das Projekt eng eingebunden.

38 Weitergehende Informationen zum Projekt OPTIMOS 2.0 finden sich unter: https://www.digitale-technologien.de/DT/Redaktion/DE/Standardartikel/SmartServiceWeltProjekte/Wohnen_Leben/SSWII_Projekt_OPTIMOS_20.html

5.2 Weitere relevante Lösungen

In jüngster Zeit werden verstärkt auch eID-Lösungen am deutschen Markt angeboten, die nicht zwingend auf die Online-Ausweisfunktion aufsetzen. Während sich diese eID-Lösungen bezogen auf Einsatzzwecke sowie Sicherheits- bzw. Vertrauensniveau untereinander teils erheblich unterscheiden, streben einige Anbieter Einsatzgebiete mit besonderen Anforderungen an die technische und organisatorische Sicherheit an. Einzelne dieser eID-Lösungen werden bereits für die primäre GwG-konforme Identitätsfeststellung und weitere der in Kapitel 4 aufgeführten Anwendungsfälle im Onlinezahlungsverkehr eingesetzt.

Die relevanten Lösungen funktionieren in der Regel gewissermaßen als „eID-Plattformen" bzw. als „eID-Vermittler", d.h., sie erheben Identitätsdaten[39] und geben diese – unter Einverständnis der Inhaberinnen und Inhaber – an Dritte weiter[40] bzw. vermitteln die Weitergabe ohne selbst in den Besitz der Daten zu kommen. Die hier betrachteten eID-Lösungen nutzen eigene – von der Online-Ausweisfunktion oder anderen notifizierten Identifizierungssystemen unabhängige – IT-Infrastrukturen.[41] Da nicht bei jeder Identifizierung auf die Online-Ausweisfunktion zurückgegriffen wird, verwenden sie andere Authentifizierungsmittel als die der Online-Ausweisfunktion und können somit beispielsweise auch auf biometrische Merkmale zurückgreifen.[42] Dies kann die Nutzerfreundlichkeit und Alltagstauglichkeit dieser Lösungen erhöhen, jedoch auch mit verringerter technischer Sicherheit der Verfahren einhergehen. Insofern erreichen diese Lösungen ohne Rückgriff auf eine Hardware-Komponente wie den Chip des PA nicht das eIDAS-Vertrauensniveau „hoch".[43]

Unerlässliche Voraussetzung für die sinnvolle Nutzung dieser eID-Lösungen für die allermeisten der vom Arbeitskreis identifizierten Anwendungsfälle ist – neben der adäquaten technischen und organisatorischen Sicherheit[44] der genutzten Prozesse – insbesondere die sichere und verlässliche initiale Identifizierung der Nutzerinnen und Nutzer durch die Lösungsanbieter („Enrolment Prozess"). Von besonderer Relevanz für den Arbeitskreis sind hierbei GwG-konforme Verfahren zur initialen Identifizierung.

---

39 Bei einzelnen der Lösungen im Markt besteht neben der GwG-konformen Erhebung von Identität auch die Möglichkeit beim Dienst ein „einfaches" eID-Nutzerprofil zu erstellen, für das keine Erhebung der Identität des Nutzers in Konformität mit dem GwG notwendig ist. Im Vordergrund der Betrachtung stehen hier jedoch die GwG-konform erhobenen Nutzerprofile.

40 Auf welche Weise die „Weitergabe der Identität" an Dritte erfolgt, variiert zwischen den verschiedenen eID-Lösungen und mitunter auch bei ein und derselben Lösung von Anwendungsfall zu Anwendungsfall. In einigen Fällen speichern die eID-Plattformen selbst die Identifizierungsdatensätze, in anderen Fällen greifen sie lediglich auf bei anderen Instituten gespeicherte Datensätze zurück.

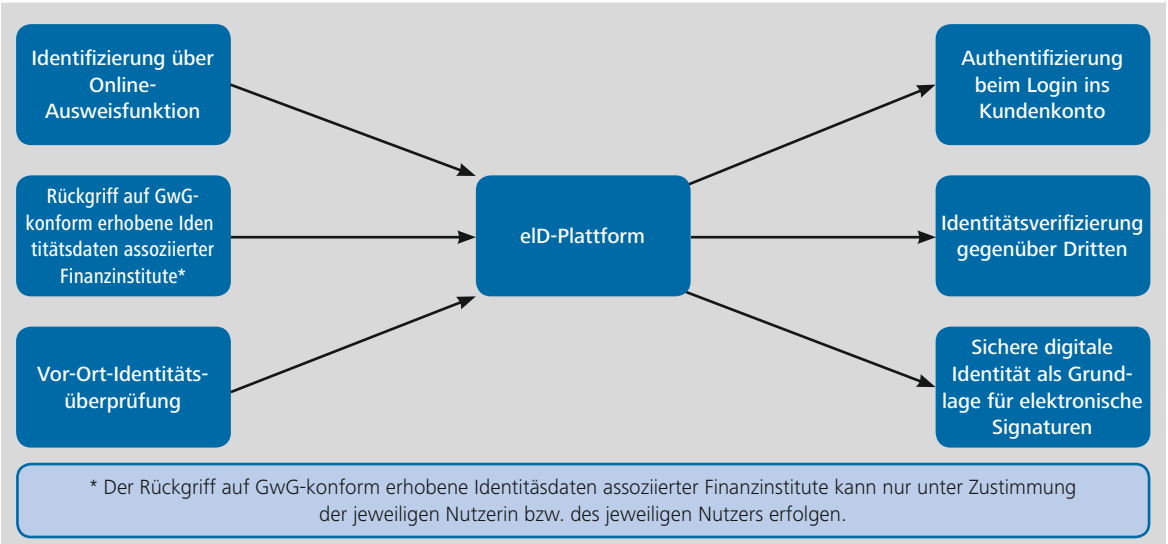
41 Die zugrundeliegende technische Infrastruktur kann prinzipiell sehr vielseitig sein und neben traditionellen Technologien, prinzipiell auch auf geeignete innovative Technologien zurückgreifen.

42 Bei der Verwendung biometrischer Authentifizierungsmittel ist besonders auf Datenschutzkonformität zu achten. Denn biometrische Daten gehören nach Art. 9 DSGVO zu den besonderen Kategorien personenbezogener Daten, deren Verarbeitung nur unter besonderen Voraussetzungen zulässig ist.

43 Um das Vertrauensniveau „substantiell" zu erreichen, sind die sichere primäre Identifizierung bei der Ausgabe und zusätzliche Sicherheitsanforderungen an die alleinige Verfügungsgewalt des Inhabers oder der Inhaberin des Identifizierungsmittels unerlässliche Voraussetzungen.

44 Die Bewertung, welches Niveau technischer und organisatorischer Sicherheit der Prozesse angemessen wäre, hängt vom spezifischen Anwendungsfall bzw. Einsatzzweck ab und soll hier nicht näher erörtert werden.

Schematische Übersicht über das Funktionsprinzip von „eID-Plattformen“ Abbildung 3



Hier besteht im Markt eine Vielzahl verschiedener Verfahren (z.B. Identitätsfeststellung vor Ort, Videoidentifizierungsverfahren, Übernahme bzw. Übergabe GwG-konform erhobener Identitäten von bzw. an kooperierende Unternehmen oder durch Nutzung der Online-Ausweisfunktion). Viele Anbieter bieten ihren Kundinnen und Kunden zudem mehrere Verfahren zur initialen Identitätsfeststellung zur Auswahl an.

Die auf diese Weise geschaffenen eIDs sind prinzipiell für viele verschiedene Anwendungsfälle einsetzbar und können in der Regel mittels geeigneter Schnittstellen in die Onlineangebote von Diensteanbietern wie z.B. Online-Händlern integriert werden. In Abhängigkeit vom Einsatzzweck und der Sensibilität der übertragenen Daten bietet mitunter derselbe Lösungsanbieter unterschiedliche Authentifizierungsmittel (einfache Authentifizierung mit Nutzername und Passwort vs. 2-Faktor-Authentifizierung). Darüber hinaus bieten viele der Lösungsanbieter Zusatzdienste wie etwa die Erstellung einer QES oder die gezielte Bestätigung einzelner personenbezogener Daten z.B. zur Altersverifizierung an.

Da es sich bei verschiedenen eID-Lösungen um technisch unabhängige Systeme handelt, ist die Interoperabilität zwischen verschiedenen Lösungen nicht ohne weiteres gegeben. Bisher ist keine dieser privatwirtschaftlichen Lösungen durch die Bundesregierung bei der Europäischen Kommission als Identifizierungssystem notifiziert worden. Die Notifizierung wäre Voraussetzung für den Rückgriff auf den Interoperabilitätsrahmen des eIDAS-Netzwerks.

6 Voraussetzungen für die erfolgreiche Etablierung von eID-Lösungen, bestehende Herausforderungen und mögliche Fehlentwicklungen

6.1 Voraussetzungen für die erfolgreiche Etablierung von eID-Lösungen

Für den Einsatz von eID-Lösungen in den in Kapitel 4 beschriebenen Anwendungsfällen wäre die Erfüllung der unmittelbaren technischen Anforderungen und gesetzlichen und aufsichtlichen Vorschriften[45] sowie für den jeweiligen Anwendungsfall und die Sensibilität der verarbeiteten Daten angemessene Sicherheitsstandards natürlich unerlässliche Voraussetzung.

Um das Potenzial von eID-Lösungen für den Online-Zahlungsverkehr und den zunehmend digitalen Alltag der Bürgerinnen und Bürger voll ausschöpfen zu können, ist es jedoch elementar, dass sich eID-Lösungen entwickeln, die nicht auf spezifische Anwendungsfälle beschränkt sind, sondern den Bürgerinnen und Bürgern die Möglichkeit bieten, sich mit einer einzigen – oder nur wenigen – von ihnen favorisierten eID-Lösungen gegenüber einer Vielzahl von Diensteanbietern identifizieren und/oder authentifizieren zu können – ohne ständige Neuregistrierung. Aus diesem Grund gilt es für die erfolgreiche Etablierung von eID-Lösungen in der Breite neben den unmittelbaren Anforderungen einzelner Anwendungsfälle auch eine Reihe allgemeiner Marktdynamiken und Nutzeranforderungen zu beachten:

Zweiseitiger Markt: Die Einbindung spezifischer eID-Lösungen hängt bei den Online-Diensteanbietern davon ab, ob das Verfahren den Kunden in ausreichender Breite zur Verfügung steht. Umgekehrt besteht aber auf Kundenseite nur dann ein Anreiz sich für eine solche Lösung registrieren zu lassen, wenn es auch genügend Einsatzmöglichkeiten gibt („Henne-Ei-Problematik").

Diese gegenseitige Bedingtheit für den Erfolg bestimmter Dienste ist das wesentliche Kennzeichen zweiseitiger Märkte, wie sie auch im Zahlungsverkehr generell zu finden sind. Die anfängliche Etablierung neuer eID-Lösungen kann daher für die Lösungsanbieter mit erheblichen Anstrengungen verbunden sein, um beide Marktseiten für die Nutzung der angebotenen Lösung zu gewinnen. Bei Verfahren, die auf bekannte und bereits weit verbreitete Elemente aufsetzen, wie etwa die Online-Ausweisfunktion[46] oder Lösungen, die bestehende Authentifizierungsmittel des Online-Bankings nutzen, stellt sich dieses Problem jedoch nur in abgeschwächter Form.

Für die erfolgreiche Etablierung von eID-Lösungen auf dem deutschen Markt wird es darauf ankommen, die bestehende „Henne-Ei-Problematik" durch klare Bekenntnisse zum Einsatz von eID-Lösungen und die rasche Implementierung auf Seiten der Diensteanbieter in Privatwirtschaft und öffentlichem Sektor zu überwinden.

Nutzerfreundlichkeit: Von entscheidender Bedeutung für die Etablierung von eID-Lösungen ist deren Nutzerfreundlichkeit. Grundsätzlich erwarten beide Marktseiten eine möglichst einfache Verwendbarkeit, was in manchen Fällen mit den Sicherheitsanforderungen

---

45 Einschließlich und insbesondere derer zum Datenschutz, für die nationale Sicherheit und zur Gewährleistung der Integrität des Finanzsystems.

46 Bei der Online-Ausweisfunktion des PA besteht die Besonderheit, dass zwar die große Mehrheit der Bevölkerung über einen PA verfügt, der für die Online-Ausweisfunktion geeignet ist, diese bei vielen PAs, die bis 2017 ausgegeben wurden, derzeit jedoch noch ausgeschaltet ist (vgl. hierzu Abschnitt 8.1).

an die Verfahren kollidieren kann. Um die erfolgreiche Verbreitung von eID-Lösungen nicht durch mangelnde Nutzerfreundlichkeit zu untergraben, sollten die Anforderungen an die Authentifizierung durch Nutzerinnen und Nutzer und die spezifischen Sicherheitserfordernisse der genutzten Dienste in einem ausgewogenen Verhältnis zueinander stehen. Für die Anbieterseite gilt es daher im Einzelfall – und im Rahmen der gesetzlichen und aufsichtlichen Vorschriften – zu entscheiden, wie sie in diesem häufig vorliegenden Zielkonflikt für den jeweiligen Anwendungszweck geeignete eID-Lösungen finden. Genauso gilt es auch für Nutzerinnen und Nutzer für sie geeignete Lösungen zu finden, die in ihrem Alltag gut zu verwenden sind und zugleich den eigenen Ansprüchen insb. an Datensicherheit und Datenschutz genügen. eID-Lösungen, die je nach Anwendungsfall und Risikogehalt unterschiedliche Ausprägungen des Verhältnisses von Nutzerfreundlichkeit und Sicherheit zulassen, könnten sich aus Nutzersicht als vorteilhaft erweisen. Auch die Etablierung sicherer Smartphone-basierter eID-Lösungen wie beispielsweise im Projekt OPTIMOS 2.0 angestrebt (vgl. Kasten oben) könnte die Nutzerfreundlichkeit von eID-Lösungen spürbar erhöhen.

Alltagsrelevanz durch vielfältige Einsetzbarkeit: Insbesondere für eID-Lösungen, die für die Authentifizierung der Nutzerinnen und Nutzer auf den Faktor „Wissen" (z.B. PIN-Abfrage) zurückgreifen, ist auch eine gewisse Regelmäßigkeit in der Nutzung besonders wichtig, da andernfalls die Wahrscheinlichkeit hoch ist, dass Nutzerinnen und Nutzer die zur Authentifizierung notwendigen Informationen vergessen oder verlegen und ihre eID (vorerst) nicht mehr einsetzen können. Betroffene eID-Lösungen könnten somit schnell ihre Alltagsrelevanz verlieren.
Die Voraussetzungen für die erfolgreiche Etablierung von eID-Lösungen scheinen daher insbesondere dann günstig zu sein, wenn diese von Nutzerinnen und Nutzern möglichst vielfältig und regelmäßig eingesetzt werden können.[47] Diese Einschätzung deckt sich mit den Ergebnissen einer aktuellen Umfrage im Rahmen des eGovernment Monitor 2018, wonach sich die Bürgerinnen und Bürger eID-Lösungen wünschen, die sie für private und behördliche Zwecke gleichermaßen einsetzen können, sowie mit den Erfahrungen aus Ländern, in denen sich eID-Lösungen erfolgreich etablieren konnten (z.B. gemeinsame Identitätslösungen für den privaten und öffentlichen Sektor in Skandinavien). Der verstärkte Einsatz von eID-Lösungen in öffentlichen Verwaltungsverfahren könnte daher als wichtiger Katalysator auch für die privatwirtschaftliche Nutzung von eIDs fungieren (vgl. Kasten).

Im Finanzsektor bestehen in vielen Fällen aufgrund der besonderen Sensibilität der Dienste sowie gesetzlicher Vorschriften strenge Anforderungen an die eindeutige Identifizierung und Authentifizierung von Kundinnen und Kunden (vgl. Kapitel 4). Die elektronische GwG-konforme Identifizierung ist hier ein zentrales Element. Die Notwendigkeit eine solche durchzuführen, ergibt sich im Laufe einer traditionellen Geschäftsbeziehung zwischen Kunden und Finanzinstitut derzeit jedoch nicht regelmäßig, was die erfolgreiche Etablierung von eID-Lösungen zu diesem Zwecke bisher deutlich erschwert. Wünschenswert wäre es, einen effektiven Prozess zu gestalten, in dem die Legitimierung digital und nicht über ein zeitintensives papierhaftes Verfahren durchgeführt wird. Bei einem solchen entfiele auch die beleghafte Weitergabe von Ausweiskopien, was aus Datenschutzgründen zu begrüßen wäre.

Mit der zunehmenden Digitalisierung der Geschäftsbeziehungen, der stetig wachsenden Bedeutung von Vergleichsportalen – auch für Finanzdienstleistungen –

47 In diesem Zusammenhang besonders geeignet erscheint aus Sicht der Handelsvertreter auch die Nutzung von eID-Lösungen im B2C-Geschäft. Einkäufe im stationären Geschäft durch den Self-Checkout über eine APP oder online im Webshop könnten mittels eID-Autorisierung eine Alltagsrelevanz entwickeln, wenn einfache, nutzerfreundliche Prozesse entwickelt werden.

und einem sich allgemein stark wandelnden Verbraucherverhalten werden viele Geschäftsbeziehungen im Finanzmarkt jedoch kurzlebiger bzw. finden parallel zueinander statt, da Verbraucherinnen und Verbraucher kontextspezifisch mit einer Vielzahl von Finanzinstituten Geschäftsbeziehungen unterhalten. Dies dürfte den Bedarf an GwG-konformen Fernidentifizierungen und universell einsetzbaren Instrumenten zur Kundenauthentifizierung perspektivisch deutlich steigern. Auch die verstärkte Nutzung von eID-Lösungen, um den Aktualisierungspflichten des GwG[48] nachzukommen, könnte zu einer erhöhten Einsatzhäufigkeit GwG-konformer Fernidentifizierungsmittel beitragen.

Dennoch stellt sich für eID-Lösungen, die ein vergleichsweise hohes Vertrauensniveau gewährleisten, nach wie vor die Herausforderung eine ausreichende Frequenz an Interaktionen zu erreichen, um im Alltag präsent zu bleiben.

Viele Bürgerinnen und Bürger loggen sich mehrmals täglich in Onlinenutzerkonten (z.B. Emailkonto, Social Media Account, Onlinehandel) ein. Für viele Produkte ist die eindeutige Identifizierung und sichere Authentifizierung der Nutzerinnen und Nutzer jedoch nicht so entscheidend, so dass hier vielfach proprietäre Zugangsdaten unter Rückgriff auf Nutzername und Passwort vergeben werden, die bei Verlust sofort ersetzbar sind. Dies mag aus Sicht der Anbieter zwar ein gangbarer Weg sein, hat allerdings nutzerseitig den Nachteil, dass die private Passwortverwaltung im Laufe der Zeit immer umfangreicher und schlechter handhabbar wird – mitunter auch auf Kosten der Sicherheit. Daher könnte hier für die Anbieter von Services ohne besonderes Sicherheitsniveau ebenfalls ein Einsatzfeld für universelle eID-Lösungen als Ersatz von „Single-Sign-On-Diensten" entstehen, da diese so die zunehmende Abneigung ihrer Kunden überwinden könnten, sich weitere Login-Daten zu beschaffen und zu verwahren.

Mögliche Zusatzdienste für den Zahlungsverkehr
Für die erfolgreiche Etablierung von eID-Lösungen im Zahlungsverkehr könnte es außerdem vorteilhaft sein, wenn eID-Lösungen geeignete auf den Zahlungsverkehr zugeschnittene Zusatzdienste anbieten. Elemente wie die auf Nutzerwunsch erfolgende automatisierte Übermittlung der nötigen Informationen zu Zahlungsdaten sowie Rechnungs- und Lieferadresse im Rahmen der Verifizierung der Käuferidentität beim Checkout im Onlinehandel oder die direkte Übernahme der IBAN bei der freiwilligen Authentifizierung von übers Internet erteilten SEPA-Lastschriftmandaten könnten hier entscheidende Faktoren sein. Die Möglichkeit in Kombination mit der eID-Lösung (qualifizierte) elektronische Signaturen erstellen zu können, könnte die Relevanz von eID-Lösungen für einige der in Kapitel 4 skizzierten potenziellen Einsatzgebiete zusätzlich steigern.

48 § 10 Abs. 1 Nr. 5 GwG schreibt u.a. vor, dass die zur Identitätsüberprüfung herangezogenen Dokumente, Daten oder Informationen unter Berücksichtigung des jeweiligen Risikos im angemessenen zeitlichen Abstand aktualisiert werden. Vgl. hierzu Abschnitt 5.5.2 der BaFin AuA aus dem Dezember 2018.

eID-Lösungen in der öffentlichen Verwaltung als möglicher Katalysator für die breitere Nutzung

Mit zunehmender Digitalisierung steigt der Druck auf die öffentlichen Verwaltungen, elektronische Verwaltungsdienste anzubieten, die Identifizierung und Authentifizierung sowie an manchen Stellen die Abgabe rechtsverbindlicher Willenserklärungen in elektronischer Form erlauben. Zudem schreibt das Onlinezugangsgesetz bis 2022 für Bund, Länder und Kommunen vor, die Möglichkeit zur onlinebasierten flächendeckenden Nutzung von Verwaltungsdiensten vorzuhalten und die Verwaltungsportale des Bundes und der Länder zu einem Portalverbund zu verknüpfen.

Hinzu kommt die Verpflichtung für alle EU-Mitgliedstaaten aus der eIDAS-Verordnung seit 29. September 2018 ihre eigenen Verwaltungsverfahren für notifizierte eIDs anderer Mitgliedstaaten zu öffnen, wenn die eigenen Verwaltungsverfahren eine elektronische Identifizierung auf „substanziellem" oder „hohem" Vertrauensniveau voraussetzen.

Vor diesem Hintergrund arbeiten Bund, Länder und Kommunen verstärkt daran, das Online-Angebot der öffentlichen Verwaltung zu erweitern. Auch dafür wurden die Voraussetzungen für die Anwendung der Online-Ausweisfunktion des PA deutlich vereinfacht (vgl. Abschnitt 5.1). Darüber hinaus befinden sich Bürger- und Unternehmenskonten in der Entwicklung, die nach primärer Identifizierung den Zugang zu Verwaltungsdiensten auf allen drei Vertrauensniveaus (hoch, substanziell, niedrig) erlauben.

Die verstärkte Verwendung von eIDs in elektronischen Verwaltungsverfahren könnte die Relevanz von eIDs im Alltag der Bürgerinnen und Bürger erhöhen und so eine Katalysatorfunktion für den breiteren Einsatz von eID-Lösungen auch in der Privatwirtschaft entfalten. Es wäre daher zu prüfen, ob die neu eingerichteten Bürger- und Unternehmenskonten in Zukunft auch für den Zugang zu assoziierten nichtstaatlichen Angeboten nutzbar gemacht und ob im Gegenzug mit Identifizierungsmitteln privatwirtschaftlicher Kundenkonten ebenso bestimmte Verwaltungsdienste genutzt werden könnten.

6.2 Hindernisse für die breite und durchgängige Verwendung der Online-Ausweisfunktion

Die bisher mangelnde Anwendung der Online-Ausweisfunktion ist unter anderem darauf zurückzuführen, dass diese derzeit bei nur rund 42 % der PA-Inhaberinnern und -Inhaber eingeschaltet ist. Es ist jedoch davon auszugehen, dass sich dieser Anteil durch die seit Juli 2017 standardmäßig erfolgende Einschaltung der Funktion bei Ausgabe des PA bis Ende 2020 auf rund 60% erhöhen wird. Damit wären dann eine beachtliche Zahl von rund 36 Mio. PAs mit eingeschalteter Online-Ausweisfunktion im Umlauf, bei rund 25 Mio PAs ohne eingeschaltete Online-Ausweisfunktion. Der turnusmäßige Austausch aller mit ausgeschalteter Online-Ausweisfunktion bis Juli 2017 ausgegebenen PAs durch PAs mit angeschalteter Online-Ausweisfunktion bis Mitte 2027 sollte jedoch nicht untätig abgewartet werden, wenn man die Verwendung des PA in digitalen Transaktionen zeitnah fördern möchte. Vielmehr sollte es darum gehen, Bürgerinnen und Bürger zu motivieren, ihre vormals nicht aktivierte Online-Ausweisfunktion wieder einschalten zu lassen. Nur so könnte zeitnah eine flächendeckende Ausstattung mit der Online-Ausweisfunktion des PA ermöglicht werden.

Die Aktivierung ausgeschalteter Online-Ausweisfunktionen gestaltet sich derzeit jedoch als verhältnismäßig aufwendig und ist für Ausweisinhaberinnen und -inhaber gebührenpflichtig,[49] sodass ohne unterstützende Maßnahmen Wiederaktivierungen in signifikantem Umfang nicht zu erwarten sind.

Darüber hinaus sind den Bürgerinnen und Bürgern die bereits verfügbaren Möglichkeiten und Angebote zur Nutzung der Online-Ausweisfunktion teilweise noch unbekannt. Der Erstkontakt der Bürgerinnen und Bürger mit ihrem Ausweis findet typischerweise in den Bürgerämtern statt und hat für die Aufklärung über die Einsatzmöglichkeiten der Online-Ausweisfunktion eine besondere Bedeutung.

Auch die zunächst notwendige und von vielen als sehr umständlich wahrgenommene Verwendung eines dedizierten Lesegeräts zum Auslesen der Daten aus dem PA hat die Etablierung der Online-Ausweisfunktion des PA sicherlich behindert. Die seit einigen Jahren bestehende Möglichkeit auch NFC-fähige Smartphones zum Auslesen der Daten aus dem Chip des PA zu verwenden (vgl. Abschnitt 5.1) stellt daher einen äußerst wichtigen Schritt zu mehr Nutzerfreundlichkeit dar. War die Nutzung der Online-Ausweisfunktion über iPhones bisher nicht möglich, dürfte die Ende September dieses Jahres erfolgte Öffnung der NFC-Schnittstelle des iPhones[50] den Einsatz der Online-Ausweisfunktion auch für diese Nutzergruppe spürbar erleichtern.

Doch auch bei Nutzung der Online-Ausweisfunktion übers Smartphone wird die Relevanz des PA für viele potenzielle Anwendungsfälle dadurch eingeschränkt, dass für das Einlesen der Daten aus dem Chip des PA die gleichzeitige Handhabung des PA und des Smartphones (Positionierung des PA-Chips an der NFC-Schnittstelle des Smartphones) sowie der Aufruf der eID-Anwendung am Smartphonebildschirm bzw. der AusweisApp notwendig ist.

Auch wenn diese relativ umständliche Handhabung unter Rückgriff auf eine zusätzliche Hardware-Komponente (Chip im PA) der technischen Sicherheit der Lösung dient, so mindert sie doch die Attraktivität des PA für eine Vielzahl alltäglicher Anwendungen, für die schon ein etwas geringeres Sicherheitsniveau unter Rückgriff auf einfachere Verfahren ausreichend wäre. Hier könnten eID-Lösungen, die – ggf. auf Kosten verringerter technischer Sicherheit – nicht auf eine zusätzliche Hardware-Komponente zurückgreifen, sondern bei denen die nötigen Daten beispielsweise direkt in sicherer Umgebung auf dem Smartphone hinterlegt sind, durch einfachere und schnellere Nutzbarkeit im Vorteil sein.

Aus diesem Grund besteht auch für den Personalausweis das Ziel die Chipkryptografie vom Ausweischip in ein Sicherheitselement auf dem Smartphone (eSIM, eIUCC) zu übertragen, so dass dieses selbstständig als eID-Client eingesetzt oder sogar als NFC-Token am Terminal eingesetzt werden kann.

Jenseits dieser technischen Weiterentwicklungen des PA stellt die Schaffung weiterer konkreter Anwendungsmöglichkeiten für die Online-Ausweisfunktion in der öffentlichen Verwaltung sowie durch Diensteanbieter in der Privatwirtschaft einen wichtigen Erfolgsfaktor für die breite Verwendung der Online-Ausweisfunktion in vielfältigen Alltagsanwendungen dar.

---

48 Die Wiedereinschaltung der Online-Ausweisfunktion kann nur über spezielle Hardware beim Bürgeramt erfolgen und ist für Bürgerinnen und Bürger mit Kosten in Höhe von 6,- € verbunden. Zwar sind Kosten in vergleichbarer Höhe auch in anderen ähnlich gelagerten Kontexten üblich, doch können sie für Bürgerinnen und Bürger ein zusätzliches Hindernis darstellen, die Wiedereinschaltung ihrer Online-Ausweisfunktion vorzunehmen.

49 Vgl.: https://www.personalausweisportal.de/SharedDocs/Kurzmeldungen/DE/2019/Online_Ausweisen_bald_mit_IPhone.html

6.3 Hindernisse für die Nutzung von eID-Lösungen, die nicht auf die Online-Ausweisfunktion aufsetzen

Die gesetzlichen und aufsichtlichen Vorschriften für die allermeisten der in Kapitel 4 beschriebenen Anwendungsfälle lassen privatwirtschaftlichen Akteuren ein relativ hohes Maß an Entscheidungsspielraum in Bezug darauf, welche spezifischen technischen Lösungen sie verwenden möchten. Damit ermöglichen sie prinzipiell auch den Einsatz vielfältiger eID-Lösungen. Ausnahme ist die GwG-konforme Identifizierung (vgl. Abschnitt 4.1).

Das Erbringen GwG-konformer Identifizierungen ist für eID-Lösungsanbieter, die nicht auf die Online-Ausweisfunktion zurückgreifen und auch keine der weiteren im GwG explizit aufgeführten Verfahren nutzen, nicht ohne weiteres möglich. Derzeit ergeben sich für diese im Prinzip nur zwei Möglichkeiten. So erlaubt das GwG zum einen gemäß § 17 grundsätzlich die Ausführung der Sorgfaltspflichten auch durch „Dritte" (gemäß § 17 Abs. 1 Nr. 1-3 GwG) und andere geeignete Personen und Unternehmen, worauf eID-Lösungsanbieter ggf. zurückgreifen könnten. Die Ausführung der Sorgfaltspflichten durch Dritte ist jedoch an strenge Auflagen geknüpft.[51]

Zum anderen erlaubt das GwG auch die Weitergabe eines zu einem früheren Zeitpunkt erhobenen Identifizierungsdatensatzes. Dies gilt jedoch nur für die Weitergabe zwischen zwei GwG-Verpflichteten.[52] Die Möglichkeit der GwG-konformen Weitergabe von Identifizierungsdaten an GwG-Verpflichtete bleibt damit de facto eID-Lösungsanbietern vorbehalten, die selbst GwG-Verpflichtete sind.

Abschnitt 8.4 der BaFin AuA zum GwG stellt weiterhin klar, dass eine solche Weitergabe von Identifizierungsdatensätzen an eine Reihe von zusätzlichen Voraussetzungen geknüpft ist. So darf beispielsweise ein solcher Rückgriff auf zu einem früheren Zeitpunkt erhobene Identifizierungsdatensätze etwa nur bei dem Dritten[53] erfolgen, der die Erstidentifizierung vorgenommen hat, die Erhebung der Daten darf nicht länger als 24 Monate zurückliegen und ihre Herkunft muss dokumentiert werden. Eine Reihe weiterer Voraussetzungen wird durch Abschnitt 8.4. der BaFin AuA zum GwG klargestellt.[54]

Auch der mögliche Rückgriff auf die durchs GwG explizit zugelassene Identifizierung mit Hilfe einer QES (zusammen mit einer Referenzüberweisung) wird in der Praxis dadurch erschwert, dass in diesem Fall zum Zwecke der zusätzlichen Verifizierung der Identität die Transaktion von einem geeigneten Zahlungskonto notwendig ist (vgl. hierzu § 12 Absatz 1, Satz 2 ff. GwG).[55]

---

50 Die Auflagen zur Auslagerung geldwäscherechtlicher Sorgfaltspflichten, einschließlich der Identitätsüberprüfung des Kunden, werden im § 17 GwG geregelt und in Abschnitt 8 der BaFin AuA spezifiziert. Als „Dritte" zählen nur die in §17 Abs. 1 Nr. 1-3 GwG abschließend aufgezählten geeigneten selbst geldwäscherechtlich Verpflichteten. Während für GwG-Verpflichtete der Rückgriff auf „Dritte" ohne gesonderte vertragliche Basis möglich ist, bedarf die Auslagerung an andere geeignete Personen und Unternehmen einer Auslagerungsvereinbarung und ist nur unter den Voraussetzungen des § 17 Abs. 5-9 GwG möglich.

51 Vgl. hierzu Abschnitt 8.4. der BaFin AuA zum GwG.

52 „Dritter" gemäß § 17 Abs. 1, 2 und 4 mit Ausnahme von Mitgliedsorganisationen oder Verbänden (§ 17 Abs. 1 Nr. 3 erste Alternative GwG). Vgl. hierzu Abschnitt 8.4 der BaFin AuA zum GwG.

53 Nach Abschnitt 8.4. der BaFin AuA zum GwG muss u.a. der Dritte (i.S.v. § 17 Abs. 1 Nr. 1-3 GwG) die Daten des Vertragspartners zur Begründung der eigenen Geschäftsbeziehung im Sinne von. § 1 Abs. 4 GwG entsprechend geldwäscherechtlichen Vorgaben erhoben haben. Die Weitergabe von auf der Grundlage vereinfachter Sorgfaltspflichten erhobener Daten ist nicht zulässig. Ferner darf das Gültigkeitsdatum des Identifikationsdokuments zum Zeitpunkt der Nutzung der Identifizierungsdaten noch nicht abgelaufen sein, außerdem muss dem Verpflichteten jeweils das Datum der „Erstidentifizierung" mitgeteilt werden.

54 Das BSI weist in diesem Zusammenhang darauf hin, dass die Nutzung einer QES zur Identifizierung technisch nicht von der Nutzung einer QES für die Abgabe einer Willenserklärung unterschieden werden kann. Bei der Verwendung der QES zu Identifizierungszwecken sollte nach Ansicht des BSI daher besondere Sorgfalt darauf verwendet werden, unerwünschte Nebeneffekte wie die Auslösung einer nicht intendierten Rechtsfolge zu vermeiden. Vgl. hierzu etwa TR-03107-1 „Elektronische Identitäten und Vertrauensdienste im E-Government" Abschnitt 2.2, S. 11

Wie in Abschnitt 6.1 erörtert ist es für die erfolgreiche Etablierung von eID-Lösungen wichtig, dass diese für möglichst viele verschiedene Anwendungszwecke eingesetzt werden können. Die fehlende oder nur eingeschränkte Einsetzbarkeit einzelner eID-Lösungen für die GwG-konforme Identifizierung könnte daher ein wesentliches Hindernis für deren erfolgreiche Verbreitung auch für Anwendungsfälle außerhalb des Geltungsbereichs des GwG darstellen.

Wesentliche Eigenschaften der Online-Ausweisfunktion und anderer relevanter eID-Lösungen im Vergleich Abbildung 4

eID-Lösung	Nutzbarkeit für GwG-konforme Identitätsfeststellung	EU-weite Nutzbarkeit	Abdeckung vielfältiger Anwendungsfälle	Wesentliche Hindernisse zur erfolgreichen Etablierung
Online-Ausweisfunktion des PA	Nutzung im GwG explizit vorgesehen. Uneingeschränkt nutzbar.	Durch Notifizierung bei der EU Kommission und die Anbindung an den eIDAS-Interoperabilitätsrahmen ist die Grundlage für die EU-weite Nutzbarkeit in öffentlichen Verwaltungsverfahren gelegt. Der eIDAS-Interoperabilitätsrahmen kann prinzipiell auch für privatwirtschaftliche Zwecke genutzt werden.	Prinzipiell kann ein breites Spektrum an verschiedenen Einsatzzwecken abgedeckt werden. Nutzung als Grundlage für QES und zur Initiierung von Zahlungsvorgängen technisch möglich. Mit der Online-Ausweisfunktion auf dem Personalausweis, eAT und der eID-Karte für EU-Bürger sowie dem eIDAS-eID-Framework ist auf Endnutzerseite prinzipiell eine sehr hohe Kundenabdeckung in DE und EU gegeben. Vor allem für Anwendungsfälle mit relativ geringen Sicherheitsanforderungen spielt die Online-Ausweisfunktion in der Praxis bisher jedoch keine Rolle. Die Übertragung zusätzlicher Daten wie beispielsweise von Zahlungsinformationen oder einer Lieferadresse ist derzeit nicht möglich.	Bisher verhältnismäßig geringe Nutzung („Henne-Ei-Problem"). Verstärkte Schaffung konkreter Anwendungsfälle daher wichtige Erfolgsvoraussetzung. Bei vielen Bürgerinnen und Bürgern ist die Online-Ausweisfunktion derzeit nicht aktiviert. Eine Reaktivierung oder erstmalige Aktivierung ist mit relativ hohem Aufwand für Bürgerinnen und Bürger verbunden (nur in den Einwohnermeldeämtern möglich und gebührenpflichtig). Die Identifizierung/Authentifizierung auf dem höchsten Sicherheitsniveau erfordert zusätzliche Hard- und/oder Software. Dies kann für Alltagsanwendungen mit relativ geringen Sicherheitsanforderungen die Attraktivität der Lösung einschränken. Geringere Flexibilität bei der Anpassung auf Markterfordernisse kann die Attraktivität der Lösung für manche privatwirtschaftliche Anwendungen verringern.

eID-Lösung	Nutzbarkeit für GwG-konforme Identitätsfeststellung	EU-weite Nutzbarkeit	Abdeckung vielfältiger Anwendungsfälle	Wesentliche Hindernisse zur erfolgreichen Etablierung
Weitere relevante eID-Lösungen	Weitergabe erhobener Identitäten zur GwG-konformen Identitätsfeststellung bei Dritten nur unter den in Abschnitt 6.3 aufgeführten Voraussetzungen möglich. Zuverlässige und GwG-konforme initiale Identitätsfeststellung („Enrolment", vgl. Abschnitt 5.2) dabei von besonderer Bedeutung.	Bisher ist keine der im Markt befindlichen privatwirtschaftlichen Lösungen eIDAS-notifiziert. Die EU-weite Nutzbarkeit könnte sich daher perspektivisch als Herausforderung darstellen. Für Lösungen, die als „eID-Broker" auf die von kontoführenden Instituten erhobenen Identitätsdaten zurückgreifen, könnten sich jenseits des eIDAS-Interoperabilitätsrahmens Chancen für die EU-weite Interoperabilität aus einem SEPA API Access Scheme ergeben (vgl. Kasten „Grenzüberschreitende Nutzung von eID-Lösungen").	Grundsätzlich werden vielfältige Einsatzzwecke abgedeckt. Nutzung als Grundlage für QES und zur Initiierung von Zahlungsvorgängen grundsätzlich möglich. Einzelne Lösungen bieten auf den Einsatzzweck angepasste Anforderungen an die Sicherheit der Authentifizierung. Zusätzliche Daten können auf Kundenwunsch prinzipiell verhältnismäßig einfach ergänzt werden. Dies steigert Nutzerfreundlichkeit und Alltagsrelevanz. GwG-konforme Identifizierung nur unter Auflagen möglich (vgl. Abschnitt 6.3).	Bisher verhältnismäßig geringe Nutzung ("Henne-Ei-Problem"). Problematik für Lösungen, die auf Zugangsdaten des Online-Bankings zurückgreifen, jedoch verringert. Verstärkte Schaffung vielfältiger Anwendungsfälle wichtige Erfolgsvoraussetzung. Ggf. fehlende Einsetzbarkeit für GwG-konforme Identifizierung schränkt Einsatzspektrum und damit Einsatz als „universelle eID-Lösung" ein.

6.4 Weitere Herausforderungen und mögliche Fehlentwicklungen

Einzelne Mitglieder des Arbeitskreises wiesen darauf hin, dass eine zu geringe Innovationsgeschwindigkeit staatlicher Verfahren eine weitere wesentliche Herausforderung für die erfolgreiche Etablierung geeigneter eID-Verfahren in Deutschland darstellen könnte und plädierten dafür, sich nicht allein auf staatliche Verfahren zu konzentrieren. Vielmehr sollte auch die Etablierung geeigneter privater eID-Lösungen unterstützt werden, um sich deren Innovationskraft für den deutschen Markt zunutze zu machen und somit potenziell ein breiteres Spektrum an möglichen Einsatzzwecken abdecken zu können.

Zudem wurde darauf verwiesen, dass es zur erfolgreichen Digitalisierung von Geschäftsbeziehungen essentiell sei, dass alle relevanten Geschäftsprozesse digital abgebildet werden können. So sollten gesetzliche Anforderungen grundsätzlich daraufhin überprüft werden, ob und wie sie auch in digitalen Transaktionen sinnvoll und alltagstauglich umgesetzt werden könnten.

Ein großes Problem sahen viele der privatwirtschaftlichen Vertreter im Arbeitskreis außerdem in zwischen einzelnen EU-Mitgliedstaaten divergierenden Anforderungen an die technische und organisatorische Sicherheit der zugrundeliegenden Prozesse für Vertrauensdienste, insbesondere in Bezug auf die für den Arbeitskreis relevante QES. Verwiesen wurde hierbei vor allem auf eine von der Bundesnetzagentur im Juni 2018 erlassene Verfügung[56], die die Zulassung des Videoidentifizierungsverfahrens auf die

55 Vgl.: Amtsblatt der Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen, Mitteilung Nr. 208/2018, S. 931, abrufbar unter: https://www.bundesnetzagentur.de/SharedDocs/Downloads/DE/Sachgebiete/QES/Verf%C3%BCgungIdentmethoden/Erstverfuegung2018.pdf?__blob=publicationFile&v=4

Erstellung von sogenannten Einmalzertifikaten beschränkt. Während in verschiedenen anderen EU Mitgliedstaaten per Videoidentifizierungsverfahren erhobene Identitäten mehrfach zur Erstellung einer QES herangezogen werden könnten, sei dies in Deutschland auf die Ausgabe von sogenannten Ad-Hoc-Zertifikaten, also auf die einmalige Verwendung, beschränkt. Dies störe das Level-Playing-Field zwischen qualifizierten Vertrauensdiensteanbietern innerhalb der EU.[57] So sei festzustellen, dass (qualifizierte) Vertrauensdiensteanbieter ins Ausland abwandern bzw. sich deutsche Unternehmen Vertrauensdienste lieber von einem ausländischen Anbieter ausstellen lassen, um diese dann in Deutschland, u.a. zur Identifizierung nach § 12 Abs. 1 Nr. 3 GwG zu verwenden. Dies sei für die Entwicklung der gerade erst entstehenden Branche deutscher und europäischer Identitätsdienstleister nicht wünschenswert.

Unterschiede zwischen einzelnen Mitgliedstaaten bei den geldwäscherechtlichen Anforderungen an eIDs könnten die EU-weite Nutzbarkeit zusätzlich herausfordern. Denn vor dem Hintergrund mangelnder Standardisierung und länderindividueller Anforderungen und Auslegungen von eID- und Geldwäschevorschriften seien EU-weit einsetzbare eID-Lösungen derzeit kaum realisierbar. Eine Expertengruppe der EU-Kommission befasst sich aktuell mit dieser Problematik und hat zum Ziel, die grenzüberschreitende elektronische Identifizierung innerhalb der EU zu vereinfachen[58] (vgl. Kasten „Grenzüberschreitende Nutzung von eID-Lösungen").

Ferner wird die technische Interoperabilität nationaler eID-Lösungen zwar durch den eIDAS-Interoperabilitätsrahmen unterstützt, dieser gilt jedoch nur für bei der EU-Kommission notifizierte Identitätssysteme, sodass privatwirtschaftliche eID-Lösungen in Deutschland bisher noch nicht von ihm profitieren. Die Notifizierung privatwirtschaftlicher Identitätssysteme ist zwar grundsätzlich möglich, jedoch an eine Reihe von Anforderungen geknüpft.[59] Diese könnten für privatwirtschaftliche eID-Lösungsanbieter in der Praxis als entscheidende Hindernisse für die Notifizierung der eigenen Systeme angesehen werden. Nach Ansicht einzelner Mitglieder des Arbeitskreises bestehe daher die Gefahr, dass Markterfordernisse der Wirtschaft für grenzüberschreitende Identifizierungen nicht ausreichend berücksichtigt würden.

Da zugleich davon auszugehen ist, dass der Bedarf an alltagstauglichen eID-Lösungen auch grenzüberschreitend weiter steigen wird, könnte dies die Marktposition internationaler Technologieunternehmen wie Facebook, Google oder Amazon stärken. Diese bieten ihren Kundinnen und Kunden bereits niedrigschwellige eID-Lösungen an, die sich nicht auf nationale Märkte begrenzen. Bisher sind die angebotenen Lösungen meist auf Einsatzzwecke mit relativ niedrigen Sicherheitsanforderungen beschränkt, eine Ausweitung des Angebots ist jedoch nicht unwahrscheinlich. Eine marktbeherrschende Stellung außereuropäischer Konzerne in dem wichtigen Bereich der eID-Lösungen könnte nicht nur die „digitale Souveränität" Deutschlands und der EU in Frage stellen, sondern angesichts der datenbasierten Geschäftsmodelle dieser Konzerne auch aus Datenschutzsicht bedenklich sein.

Eine weitere mögliche Fehlentwicklung könnte in der bis dato auch auf nationaler Ebene nicht absehbaren Interoperabilität der verschiedenen privatwirtschaftlichen eID-Lösungen liegen. Diese könnte in der Zukunft zu einer Fragmentierung des deutschen

56 Vgl. beispielsweise eine diesbezügliche Stellungnahme des Bitkom aus dem Mai 2018. Diese bezieht sich noch auf den Entwurf der Verfügung der Bundesnetzagentur: https://www.bitkom.org/sites/default/files/file/import/20180712-Bitkom-Position-zum-Videoident-verfahren-als-national-anerkannte-Identifikationsmethode.pdf

57 Nähere Informationen zur Commission Expert Group zu "Electronic Identification and remote Know-Your-Customer processes" finden sich unter: https://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetail&groupID=3571&NewSearch=1&NewSear ch=1

58 Die relativ strengen Anforderungen ergeben sich unter anderem vor dem Hintergrund der verpflichtenden Anerkennung notifizierter Identitätssysteme durch öffentliche Stellen anderer Mitgliedstaaten und der Übernahme von (Mit-)Haftung für notifizierte Systeme durch den notifizierenden Mitgliedsstaat.

Marktes für eID-Lösungen führen. Auch wenn sie bisher nicht konkret absehbar ist, sollte eine Situation, in der Bürgerinnen und Bürger in ihrem Alltag auf eine Vielzahl verschiedener eID-Lösungen auf substanziellem oder hohem Vertrauensniveau angewiesen sind, im Sinne der Nutzerfreundlichkeit perspektivisch vermieden werden.

Auf der anderen Seite könnte mangelnde Interoperabilität von eID-Lösungen aber auch dazu führen, dass sich eine einzige privatwirtschaftliche Lösung durchsetzt und es angesichts starker Netzwerkeffekte im Markt zu einer Verdrängung anderer Lösungsanbieter und somit zu einer privaten Monopolbildung des Marktes kommt. Eine große Abhängigkeit des deutschen Marktes von einem einzigen privaten eID-Lösungsanbieter sollte im gesellschaftlichen und volkswirtschaftlichen Interesse vermieden werden. Unter den Mitgliedern des Arbeitskreises überwog jedoch die Einschätzung, dass derartige Fehlentwicklungen zum gegenwärtigen Zeitpunkt nicht absehbar wären und es zunächst darum gehen müsse, überhaupt geeignete eID-Lösungen im deutschen Markt zu etablieren. Dessen ungeachtet sollte die Frage der Interoperabilität von eID-Lösungen jedoch im Blick behalten werden – innerhalb Deutschlands wie auch in der EU.

Staatliche Initiativen wie die Weiterentwicklung der Online-Ausweisfunktion und insbesondere die Entwicklung eines offenen Mobile-eID Ökosystems (vgl. Projekt „OPTIMOS 2", Innovationswettbewerb Schaufenster Sichere Digitale Identitäten[60]) sowie Überlegungen, öffentliche Bürger- und Unternehmenskonten auch für privatwirtschaftliche Anwendungen nutzbar zu machen, stellen daher sehr begrüßenswerte Maßnahmen dar. Denn sie könnten für Bürgerinnen und Bürger auch für privatwirtschaftliche Anwendungsfälle als Alternative zu privaten eID-Lösungen dienen und so ein Gegengewicht bilden, falls sich unerwünschte Marktentwicklungen ergeben. Darüber hinaus scheinen sie derzeit auch besser in der Lage EU-weite Interoperabilität zu gewährleisten.

59 https://www.digitale-technologien.de/DT/Navigation/DE/Foerderaufrufe/Sichere_Digitale_Identitaeten/sichere_digitale_identitaeten.html

Grenzüberschreitende Nutzung von eID-Lösungen

Die grenzüberschreitende Nutzbarkeit von eID-Lösungen ist wichtige Voraussetzung für die effiziente und komfortable Abwicklung digitaler Verwaltungsverfahren und Geschäftsprozesse in der EU.

Der eIDAS-Interoperabilitätsrahmen schreibt für öffentliche Stellen in allen Mitgliedstaaten die Anerkennung der bei der EU-Kommission notifizierten nationalen eID-Systeme vor und bietet die für deren Interoperabilität nötige technische Infrastruktur (vgl. Abschnitt 3.3). Ungeachtet des Schwerpunkts auf Verwaltungsverfahren steht das eIDAS-Netzwerk auch der privatwirtschaftlichen Nutzung offen. So können sich zum einen private Online-Diensteanbieter anbinden, um auch Kundinnen und Kunden aus dem EU-Ausland die einfache digitale Identifizierung zu ermöglichen. Zum anderen können private eID-Lösungsanbieter ihre eID-Systeme zur Notifizierung vorschlagen, um so die Anerkennung der eigenen eID-Lösung innerhalb der Verwaltung in den EU-Staaten verbindlich zu machen und potenziell auch darüber hinaus zu befördern. Der eIDAS-Interoperabilitätsrahmen ist damit wichtiger Baustein für die grenzüberschreitende Nutzung von eID-Lösungen in der EU.

Eine weitere Chance zur Schaffung einer standardisierten und europaweit einsetzbaren eID-Lösung könnte in den aktuellen Arbeiten der Euro Retail Payments Board[61] Arbeitsgruppe zur Entwicklung eines „SEPA API Access Scheme" liegen. Ein solches API Scheme würde für teilnehmende Zahlungsdienstleister gemeinsame Regeln und technische Standards für die Nutzung von Kundendaten über APIs festlegen. Neben der Abwicklung von Zahlungen könnte es auch zur Bestätigung der Kundenidentität gegenüber Dritten durch das kontoführende Institut dienen. Grundlage wäre, dass der Kunde die Verifizierung gegenüber Dritten wünscht und sich über seine aus dem Online-Banking bekannten Zugangsmittel authentifiziert.

Für den grenzüberschreitenden Einsatz von eID-Lösungen im europäischen Finanzsektor bestehen neben der technischen Interoperabilität jedoch weitere wesentliche Hürden in divergierenden geldwäscherechtlichen Anforderungen. So können eID-Verfahren, die in einem Mitgliedstaat zulässig sind, u.U. in einem anderen Mitgliedstaat nicht angewendet werden, da sie etwa die dortigen gesetzlichen Anforderungen an die Identitätsüberprüfung nicht erfüllen. Die weitere Harmonisierung der geldwäscherechtlichen Anforderungen in der EU ist daher eine essentielle Voraussetzung für die grenzüberschreitende Nutzung von eIDs im europäischen Finanzsektor und die erfolgreiche weitere Integration des digitalen Binnenmarktes für Finanzdienstleistungen.

Die von der EU-Kommission ins Leben gerufene Expert Group on „Electronic Identification and Remote Know-Your-Customer Processes"[62] soll bis Ende 2019 u.a. Vorschläge für einen zukünftigen europäischen Rahmen zur Erfüllung von geldwäscherechtlichen Sorgfaltspflichten erarbeiten. Der zielgerichteten Umsetzung dieser Empfehlungen wird voraussichtlich eine große Bedeutung zukommen.

Das Thema eID beschäftigt auch die Financial Action Task Force (FATF), die die internationalen Standards zur Bekämpfung von Geldwäsche und Terrorismusfinanzierung setzt. Diese erarbeitet derzeit internationale Richtlinien für den Einsatz von eIDs im Finanzsektor.

---

60 Das Euro Retail Payments Board (ERPB) unter Leitung der EZB hat zur Aufgabe die Entwicklung eines integrierten, innovativen und wettbewerbsfähigen Marktes für Massenzahlungen in Euro in der Europäischen Union voranzutreiben. Der ERPB löste im Jahr 2014 den SEPA-Council ab und ist aus jeweils sieben Verbänden der Nachfrageseite und der Angebotsseite des europäischen Massenzahlungsverkehrs zusammengesetzt. Hinzu kommen fünf Vertreterinnen und Vertreter der nationalen Zentralbanken des Euro-Währungsgebiets und ein Vertreter bzw. eine Vertreterin der nationalen Zentralbanken der nicht dem Eurogebiet angehörenden EU-Mitgliedstaaten. Nähere Infor-mationen (in englischer Sprache) finden sich unter: https://www.ecb.europa.eu/paym/retpaym/euro/html/index.en.html

61 Für weitergehende Informationen (in englischer Sprache):
https://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetail&groupID=3571&NewSearch=1&NewSear ch=1

7 Handlungsempfehlungen

Marktdynamik fördern: Grundsätzliche Offenheit für eID-Lösungen

Dem Arbeitskreis eID geht es darum, die Digitalisierung im bargeldlosen Zahlungsverkehr voranzubringen und online-basierte Zahlungsdienste medienbruchfrei zu ermöglichen. Dazu sollte neben einer nutzerfreundlichen sicheren Authentifizierung und Autorisierung von Zahlungen auch die erstmalige gesetzeskonforme Identitätsfeststellung bei Aufnahme der Geschäftsbeziehung mit einem Zahlungsdiensteanbieter online durchführbar sein. Hierzu bedarf es der Weiterentwicklung und Etablierung von eID-Lösungen, die marktgängig sind und eine hohe Kundenakzeptanz genießen, etwa durch Abdeckung eines breiten Anwendungsspektrums. Die Online-Ausweisfunktion des Personalausweises bringt gute Voraussetzungen mit, da ihr als staatliche Lösung eine Sonderrolle zukommt und andere eID-Lösungen auf sie aufsetzen können. Allerdings erfüllt sie gegenwärtig nicht alle Anforderungen des Marktes für die aufgezeigten unterschiedlichen Einsatzzwecke und findet in der Praxis bisher nur geringe Verwendung.

Angesichts der noch geringen Akzeptanz von staatlichen wie privaten eID-Lösungen in Deutschland begrüßt der Arbeitskreis eID ausdrücklich, neben der Online-Ausweisfunktion auch geeignete privatwirtschaftliche Ansätze zur Nutzung von eIDs. Dazu sollten die gesetzlichen Rahmenbedingungen neuen Technologien gegenüber offen sein. Auch auf europäischer Ebene sollte die Verfügbarkeit von interoperablen eID-Lösungen in allen Mitgliedstaaten sowie deren grenzüberschreitende Nutzbarkeit und Interoperabilität gefördert werden. Nur so kann auf diesem Gebiet der einheitliche Binnenmarkt entstehen.

Voraussetzungen zur aktiven Nutzung der Online-Ausweisfunktion des Personalausweises

Seit 2010 wird der Personalausweis mit Online-Ausweisfunktion ausgegeben. Eine Vollausstattung der Bevölkerung mit Personalausweisen mit aktivierter Online-Ausweisfunktion ist jedoch erst ab 2027 gewährleistet, denn bei einem Großteil der bis Juli 2017 ausgegebenen Personalausweise ist die Online-Ausweisfunktion noch nicht eingeschaltet.

Darüber hinaus bestehen für die Online-Ausweisfunktion bisher nur verhältnismäßig wenige konkrete Anwendungsfälle, was ihre Relevanz im Alltag der Bürgerinnen und Bürgern erheblich schmälert.

Um die Nutzung der Online-Ausweisfunktion zu fördern und bereits vor 2027 für eine flächendeckende Verfügbarkeit in der Bevölkerung zu sorgen, müsste die nachträgliche Einschaltung der Online-Ausweisfunktion des Personalausweises vereinfacht werden. Hierzu wäre zu prüfen, wie Anlässe für eine nachträgliche Einschaltung bei Bürgerinnen und Bürgern geschaffen werden können und ob ggfs. zusätzliche Stellen mit der Wiedereinschaltung betraut werden könnten. Zudem könnte die mit der Wiedereinschaltung einhergehende Gebührenpflicht aufgegeben werden. Eine solche Reaktivierung der Online-Ausweisfunktion sollte von einer breitangelegten öffentlich finanzierten Informationskampagne entlang der Online- und Vor-Ort-Anwendungen des Personalausweises flankiert werden. Ferner gilt es konkrete Anwendungsfälle für die Online-Ausweisfunktion in Verwaltungsverfahren ebenso wie nach Möglichkeit in privatwirtschaftlichen Anwendungen zeitnah zu erweitern, um die Relevanz der Online-Ausweisfunktion im Alltag zu erhöhen.

Offene Systeme für die Nutzung von eID-Lösungen übers Smartphone

Smartphones spielen eine herausgehobene Rolle für die einfache und nutzerfreundliche Verwendung von eID-Lösungen im Alltag. ***Regulierungs- und Aufsichtsstellen sollten sich daher mit Nachdruck für die Etablierung offener Systeme und Schnittstellen für die Nutzung von sicheren und nutzerfreundlichen eID-Lösungen übers Smartphone einsetzen und faire Wettbewerbsvoraussetzungen gewährleisten.***

Erweiterung der Verfahren zur gesetzeskonformen elektronischen Identitätsfeststellung

Das Geldwäschegesetz regelt die für geldwäscherechtlich verpflichtete Institute zulässigen analogen und elektronischen Verfahren zur Identitätsfeststellung von Kundinnen und Kunden. Der bestehende Diskurs zwischen BaFin und den Verpflichteten hinsichtlich einer praktikablen Anwendung der regulatorischen Anforderungen – unter Berücksichtigung der im Dezember 2018 niedergelegten Konkretisierungen in den Abschnitt 8.4. der BaFin AuA zum GwG – sollte fortgeführt werden, ***um die Nutzung im Markt befindlicher Verfahren zur elektronischen Identitätsfeststellung zu ermöglichen, ohne die Integrität des Finanzsystems und die innere Sicherheit zu gefährden.***

Verstärkte Kooperation zwischen Wirtschaft und Staat bei der Identitätsfeststellung für privatwirtschaftliche und staatliche Online-Dienste

Um die Sicherheit von Online-Anwendungen im Alltag zu steigern und eine möglichst hohe Alltagsrelevanz von eID-Lösungen zu gewährleisten, sollte eine verstärkte Kooperation zwischen Wirtschaft und Staat bei der Identitätsfeststellung der Nutzerinnen und Nutzer von privatwirtschaftlichen und staatlichen Online-Diensten angestrebt werden.

Insbesondere sollten Privatwirtschaft und staatliche Stellen gemeinsam prüfen, ob und unter welchen insbesondere sicherheitstechnischen und datenschutzrechtlichen Voraussetzungen privatwirtschaftliche eID-Lösungen auch für den Zugang zu behördlichen Online-Diensten genutzt und im Gegenzug öffentliche Nutzerkonten des Portalverbunds von Bund, Ländern und Kommunen („Bürger- und Unternehmenskonten“) für den Zugang zu privatwirtschaftlichen Online-Diensten eingesetzt werden könnten. ***In diesem Zusammenhang sollte geprüft werden, ob aktuelle Freigabeverfahren für private eID-Anbieter gegenüber öffentlichen Verwaltungen vereinfacht werden könnten.***

Der größte Hebel im öffentlichen Sektor ist die Digitalisierung von Unternehmensanfragen, da diese im Vergleich zu Bürgeranfragen häufiger vorkommen. Einheitliche Vorschriften oder Standards, wie man eine digitale Unternehmens-Identität online erzeugen und berechtigte Personen festlegen kann, existieren jedoch noch nicht – hier wären Vorgaben zur Standardisierung auf Basis der ersten Erfahrungen von Marktteilnehmern sinnvoll, um bundesländerübergreifende Lösungen generieren und die Umsetzung beschleunigen zu können.

Überprüfung gesetzlicher Vorschriften auf alltagstaugliche Umsetzbarkeit in digitalen Prozessen

Um die Mehrwerte des Einsatzes von eID-Lösungen in digitalen Geschäftsbeziehungen in vollem Umfang auszuschöpfen, ist es von besonderer Bedeutung, dass neben dem Zahlungsverkehr und der Identitätsüberprüfung auch alle weiteren relevanten Geschäftsprozesse digital abgebildet werden können. ***Zur Förderung des Einsatzes von eID-Lösungen und der weiteren erfolgreichen Digitalisierung von Geschäftsbeziehungen sollten gesetzliche Anforderungen daher grundsätzlich daraufhin überprüft werden, ob und wie sie auch in digitalen Transaktionen sinnvoll und alltagstauglich umgesetzt werden könnten.***

EU-weites Level-Playing-Field zur Nutzung von eID-Lösungen beim Kunden-Onboarding und der Erbringung von Vertrauensdiensten

Der eIDAS-Verordnung entsprechend können qualifizierte Vertrauensdiensteanbieter aus dem EU-Ausland ihre eIDAS-konformen Vertrauensdienste in Deutschland anbieten, wie umgekehrt deutsche Anbieter auch im EU-Ausland aktiv werden dürfen. Damit sollten prinzipiell für alle Vertrauensdiensteanbieter in der EU auch die gleichen Anforderungen gelten.[63] Dennoch scheint das eigentlich angestrebte innereuropäische Level-Playing-Field in der Praxis nicht immer gewährleistet. So berichten Marktteilnehmer von wesentlich strengeren deutschen Anforderungen bei der Erbringung von Vertrauensdiensten, insbesondere bei der auch für die hier aufgezeigten Anwendungsfälle relevanten QES (vgl. Abschnitt 6.4). So sei festzustellen, dass Vertrauensdiensteanbieter ins Ausland abwandern bzw. sich deutsche Unternehmen Vertrauensdienste lieber von einem ausländischen Anbieter erbringen lassen, um diese dann in Deutschland, u.a. zur GwG-konformen Identifizierung zu verwenden.

Darüber hinaus seien auch Unterschiede zwischen einzelnen Mitgliedstaaten bei den geldwäscherechtlichen Anforderungen an eIDs zu beobachten. Dies sei nicht nur aus Wettbewerbssicht bedenklich, sondern stelle auch eine Herausforderung für die EU-weite Nutzbarkeit elektronischer Identifizierungsmittel dar. Diesen Einschätzungen aus der Privatwirtschaft sollte auf nationaler und europäischer Ebene nachgegangen und nach geeigneten Lösungsansätzen gesucht werden. ***Die auf EU-Ebene angestoßenen Initiativen zur Vereinheitlichung der Rahmenbedingungen für die geldwäscherechtliche elektronische Identifizierung und Erbringung von Vertrauensdiensten sollten mit dem Zielbild verfolgt werden, EU-weit harmonisierte Standards herbeizuführen, die die sichere und nutzerfreundliche Verwendung von eIDs und Vertrauensdiensten im EU-weiten Finanzsektor ermöglichen und das innereuropäische Level-Playing-Field wahren.***

Erleichterung der Notifizierung unter eIDAS für privatwirtschaftliche e-ID-Lösungen

Neben den oben geschilderten zwischen EU-Mitgliedstaaten divergierenden Anforderungen an die geldwäscherechtliche Identifizierung stellt auch die oftmals mangelnde technische Interoperabilität eine Herausforderung für die grenzüberschreitende Nutzung von eID-Lösungen dar. Der Ansatz, über eIDAS einen Interoperabilitätsrahmen für bei der EU-Kommission notifizierte nationale eID-Lösungen zu etablieren, ist diesbezüglich ein wichtiger Schritt. Die Hürden für die Notifizierung nach eIDAS werden von Teilen der Privatwirtschaft jedoch als sehr hoch angesehen und seien in Deutschland zudem teilweise höher als in anderen EU Mitgliedstaaten. ***Um den ursprünglich auf öffentliche Verwaltungsverfahren ausgerichteten eIDAS-Interoperabilitätsrahmen auch als wesentlichen Baustein für die Vertiefung des digitalen Binnenmarktes nutzbar zu machen, sollte geprüft werden, ob privatwirtschaftlichen Belangen stärker Rechnung getragen und die Voraussetzungen für die Notifizierung privater eID-Lösungen im Einklang mit den EU-weiten Vorgaben vereinfacht werden könnten.***

62 Die Anforderungen der eIDAS-Verordnung in Bezug auf Vertrauensdienste müssen - anders als die unmittelbar geltenden Vorschriften für die grenzüberschreitende Nutzung von Identifizierungssystemen im Verwaltungsbereich - durch nationale Gesetzgebung in nationales Recht umgesetzt werden. In Deutschland geschieht dies durch das Vertrauensdienstegesetz (VDG).