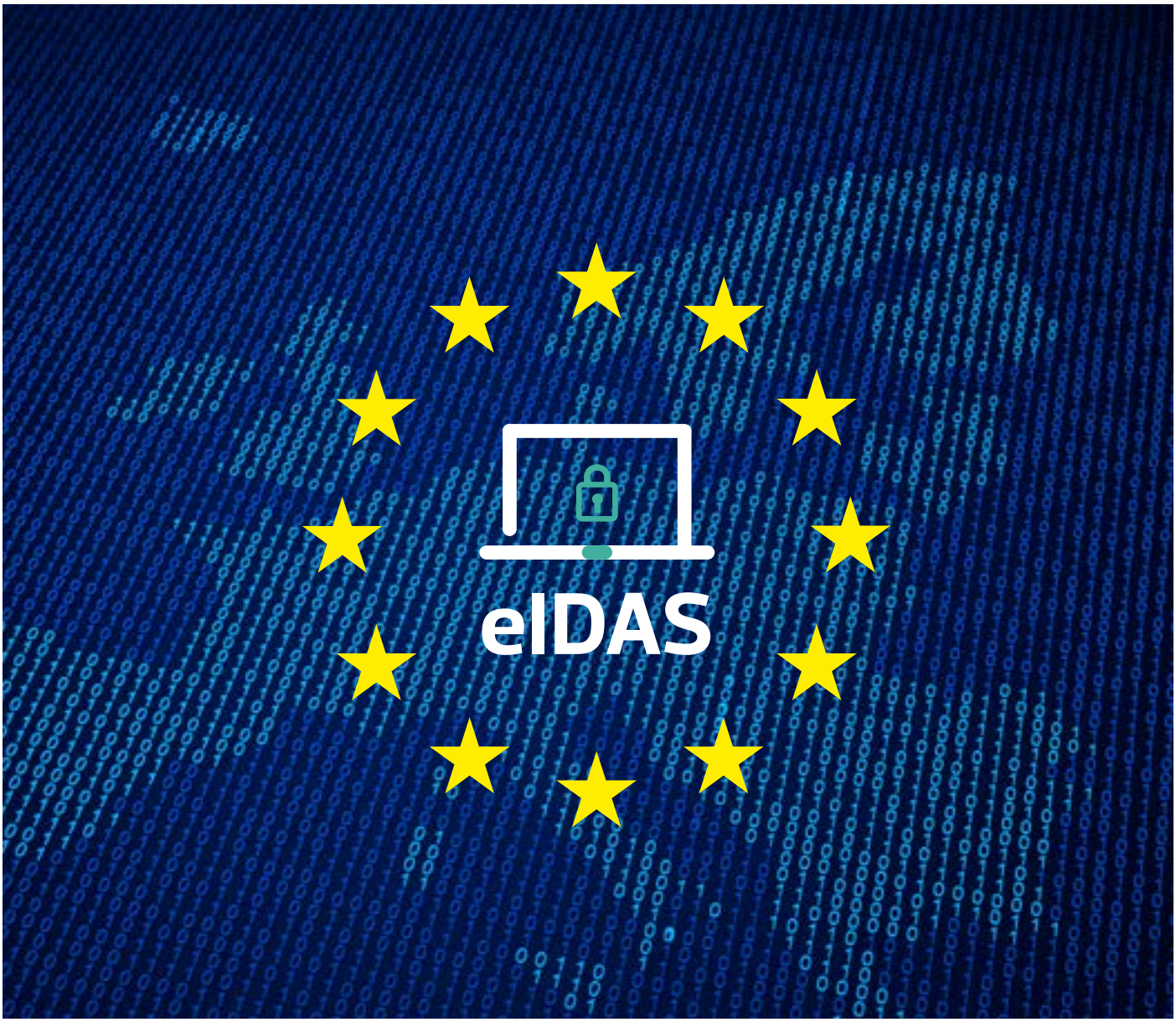
BUNDESDRUCKEREI

STUDIE

Vertrauensraum in der Digitalisierung.

Herausforderungen bei der Umsetzung der eIDAS-Verordnung in Deutschland



IMPRESSUM

Vertrauensraum in der Digitalisierung
Herausforderungen bei der Umsetzung der eIDAS-Verordnung in Deutschland

Herausgeber (V. i. S. d. P.)/Verleger
(zugleich Inhaber ausschließlicher Nutzungsrechte)
Bundesdruckerei GmbH
Antonia Maas
Kommandantenstraße 18
10969 Berlin
Tel.: +49 (0)30 2598-0
E-Mail: info@bdr.de
www.bundesdruckerei.de
AG Berlin-Charlottenburg HRB 80443
USt.-Id.-Nr.: DE813210005

Ort und Jahr der Veröffentlichung
Berlin, Juni 2019

Autor
Rechtsanwalt Cornelius G. Kopke

Fachexperten
Enrico Entschew und Christian Seegebarth, Bundesdruckerei GmbH

Projektleitung und Ansprechpartner
Patrick von Braunmühl und Jonas Kotzott, Bundesdruckerei GmbH

Lektorat
Ursula Birkel, Bundesdruckerei GmbH

Layout
Theodora Miehlke, Bundesdruckerei GmbH

Bundesdruckerei–Studie Vertrauensraum in der Digitalisierung

INHALT

EXECUTIVE SUMMARY

Die Europäische Union hat mit der eIDAS-Verordnung einen einheitlichen gesetzlichen Rahmen geschaffen, um digitale Geschäfts- und Verwaltungsprozesse sicher und einfach abwickeln zu können. Die Verordnung enthält die standardisierten Vertrauensdienste des europäischen digitalen Binnenmarkts, zu denen die qualifizierte elektronische Signatur (QES), das qualifizierte elektronische Siegel (QSiegel) oder qualifizierte Website-Zertifikate (QWACs) gehören. Mithilfe dieser Werkzeuge kann eine elektronische Kommunikation abgesichert werden. Sie ermöglichen einen sogenannten Vertrauensraum in der Digitalisierung, in dem eine sichere Interaktion zwischen Menschen, Software und Maschinen stattfinden kann.

QES
Die individuelle digitale Unterschrift

Einschreib- und Zustelldienst
Die sichere digitale Nachricht wie bei der Post oder dem Gerichtsvollzieher

QSiegel
Der verlässliche digitale Stempel für Behörden und Unternehmen

Zeitstempel
Die digitale Stoppuhr wie ein elektronischer Fotobeweis

QWAC
Die sichere Identifizierung eines Website-Betreibers

Bewahrungsdienste
Das digitale ewige Archiv

Validierungsdienst
Der automatische unabhängige Prüfer

Die Werkzeuge des digitalen Vertrauensraums

In Deutschland sind diese Werkzeuge noch weitestgehend unbekannt und was noch schwerer wiegt: Sie wurden noch nicht sinnvoll in das deutsche Recht integriert. Folglich werden sie hierzulande kaum angewendet. Dabei haben sie enormes Potenzial. So wie der Euro europäisches Zahlungsmittel ist, könnten die eIDAS-Vertrauensdienste EU-weit für alle rechtlichen Verwaltungs- und Geschäftsprozesse genutzt werden – und somit die gleiche digitale Sprache sprechen.

Um dieses Ziel zu erreichen, müssen einige gesetzliche Lücken geschlossen werden. Bestehende Gesetze müssen dort erweitert werden, wo bestimmte eIDAS-Werkzeuge noch nicht implementiert wurden. Dies gilt etwa für die E-Government-Gesetze des Bundes und der Länder, für die Verwaltungsgerichtsordnung, die Zivilprozessordnung oder das Sozialgesetzbuch. Hier müssen die eIDAS-Werkzeuge in die Gesetzestexte integriert werden, um digitale und standardisierte Kommunikationsprozesse zu ermöglichen. Gänzlich neue gesetzliche Lösungen müssen dort geschaffen werden, wo digitale Prozesse noch nicht mitgedacht wurden. Notwendig sind z. B. neue Regelungen für den elektronischen Rechtsverkehr. Dies gilt etwa für das Bürgerliche Gesetzbuch, wo eine neue Regelung zu digitalen Kommunikationsbeziehungen aufgenommen werden muss, oder für die Berufsordnungen für Rechtsanwälte und Steuerberater. Nicht zuletzt braucht es ein neues Verständnis für Formerfordernisse. Dafür ist eine Vertrauensfunktion als neues Element im deutschen Recht zu etablieren.

Für die Politik ergeben sich konkrete Handlungsempfehlungen: Die Bundesregierung sollte die Defizite bei der Umsetzung der eIDAS-Verordnung schnellstmöglich aufarbeiten. Insbesondere in Bezug auf das QSiegel und QWACs sind neue gesetzliche Regelungen erforderlich, wie sie beispielsweise bereits in der Payment Services Directive 2 (PSD2) vorhanden sind. Dabei sollte die Bundesregierung die Umsetzung der eIDAS-Verordnung als wichtigen Beitrag für mehr Daten- und Verbraucherschutz in Deutschland verstehen. Im Rahmen der „digitalen Gesetzgebung" sollte zudem eine Orientierung an der „Better Regulation Toolbox #23" der Europäischen Kommission erfolgen. Dazu gibt es bereits das Projekt „Bessere Rechtsetzung" des Bundesministeriums des Innern, für Bau und Heimat. Dieses Projekt sollte um eine Folgenabschätzung von Gesetzen für die digitale Transformation ergänzt werden, welche die Werkzeuge der eIDAS-Verordnung explizit berücksichtigt. Für das Jahr 2020 ergibt sich im Rahmen der deutschen EU-Ratspräsidentschaft die Gelegenheit, die Weiterentwicklung der eIDAS-Verordnung als Priorität zu behandeln. So kann die Bundesregierung die Verhandlungsführung bei der Überarbeitung der eIDAS-Verordnung übernehmen, um neue Werkzeuge einzuführen (z. B. eine eID-Funktion für Unternehmen) sowie eine stärkere Verbindlichkeit bei der Nutzung und Anerkennung der Vertrauensdienste zu erwirken. Gleichzeitig kann auch eine weitere Harmonisierung der Voraussetzungen für die Zertifizierung und Zulassung von Vertrauensdiensten in die Wege geleitet werden.

1 EINLEITUNG

Die digitale Transformation schreitet unaufhörlich voran und hat nahezu alle Bereiche des privaten und öffentlichen Lebens erreicht. Gleichwohl steht Deutschland erst am Anfang von tiefgreifenden Umwälzungen, die Wirtschaft, Staat und Gesellschaft nachhaltig verändern werden. Die damit verbundenen Potenziale sind enorm und doch werden sie hierzulande nur bedingt ausgeschöpft.

Mit dem inzwischen außer Kraft getretenen Signaturgesetz (SigG) war Deutschland in den 1990er-Jahren Vorreiter bei der sicheren elektronischen Kommunikation. Doch im Zuge der voranschreitenden Digitalisierung haben sich die Voraussetzungen verändert. Heute werden die gesetzlichen Rahmenbedingungen für digitale Kommunikationsprozesse vor allem auf europäischer Ebene geschaffen. Nationale Sonderwege scheinen nicht mehr zielführend zu sein und so gilt das Motto: Wer Digitalisierung voranbringen möchte, muss europäisch denken.

Elektronische Rechtsgeschäfte brauchen Vertrauen und Sicherheit

Das Rennen um die besten digitalen Standorte hat in Europa längst begonnen. Deutschland droht im europäischen Wettbewerb den Anschluss zu verlieren, wenn es nicht gelingt, digitale Geschäftsmodelle zuverlässig, rechtssicher und vor allem standardisiert abzuwickeln.[1] Die dafür nötigen Werkzeuge existieren bereits: Die europäische eIDAS-Verordnung[2] enthält die Vertrauensdienste des europäischen digitalen Binnenmarkts. Sie sind der Schlüssel für vertrauensvolle und sichere elektronische Rechtsgeschäfte in ganz Europa und können Deutschland fit für die digitale Zukunft machen. Bislang werden sie jedoch nur unzureichend angewendet.

Die vorliegende Studie zeigt Herausforderungen bei der Umsetzung der eIDAS-Verordnung in Deutschland auf und beschreibt, welche rechtlichen Änderungen notwendig sind, um die Vertrauensdienste der eIDAS-Verordnung in das deutsche Recht zu integrieren.[3] Dafür werden zunächst die aktuellen gesetzlichen Rahmenbedingungen in Deutschland skizziert. Wir identifizieren Regelungslücken und Handlungsbedarf. So lässt sich erkennen, welche Gesetze wie geändert werden müssen. Eine der Erkenntnisse: Eine konsequente Umsetzung und Implementierung der eIDAS-Werkzeuge ins deutsche Recht kann einen enormen Beitrag zur Digitalisierung der Verwaltung leisten. Davon profitieren am Ende Bürger, Unternehmen und nicht zuletzt die Verwaltung selbst.

Verschenktes Potenzial

Analoge Postkarten, Briefe und Verträge gehören schon bald der Vergangenheit an. Die Kommunikation in Verwaltungen und Unternehmen und mit Bürgern* wird in den kommenden fünf bis zehn Jahren beinahe vollständig digitalisiert. Hierfür müssen sich alle Beteiligten neu aufstellen.

Aktuell liegt Deutschland bei der Digitalisierung öffentlicher Dienste mit Platz 21 von 28 Ländern auf einem hinteren Platz.[4] Die deutsche Wirtschaft nutzt ihre digitalen Möglichkeiten bislang nur zu zehn Prozent. So verschenkt Deutschland 500 Milliarden Euro Potenzial.[5]

1 Deutschland liegt beim Digital Economy and Society Index (DESI) der Europäischen Kommission regelmäßig auf den hinteren Plätzen, insbesondere bei der Digitalisierung der Verwaltung und des Gesundheitswesens. Vgl.: Europäische Kommission: DESI 2018, Länderprofil Deutschland, aufgerufen am 01.05.2019 unter https://ec.europa.eu/digital-single-market/en/scoreboard/germany.

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, aufgerufen am 01.05.2019 unter *https://bit.ly/2WfoPy9*.

3 In der Studie wird Kapitel II der eIDAS-Verordnung nicht weiter betrachtet. Zudem werden keine vollständigen Gesetzesformulierungen vorgenommen.

* Die männliche Schreibweise wird ausschließlich aus Gründen der Leserfreundlichkeit verwendet. Wir weisen an dieser Stelle ausdrücklich darauf hin, dass wir hiermit immer alle Geschlechter meinen.

4 Europäische Kommission: Digital Economy and Society Index (DESI) 2018, Länderprofil Deutschland, aufgerufen am 01.05.2019 unter https://ec.europa.eu/digital-single-market/en/scoreboard/germany.

5 McKinsey Global Institute, Digital Europe: Pushing the frontier, capturing the benefits, Juni 2016, aufgerufen am 01.05.2019 unter https://mck.co/2w8FuUv.

Die nächste Herausforderung: Die digitale Transformation schreitet mit enormer Geschwindigkeit voran. Das trifft vor allem die sehr mechanisch und organisatorisch geprägte deutsche Wirtschaft mit ihrem Hang zu Hierarchien und Perfektion in der klassischen Produktion. Dies wiederum führt zu enormem Handlungsdruck für die Politik. Sie muss sich der verändernden Bedingungen annehmen und sie gestalten. Schließlich können sich die deutschen Unternehmen nur dann anpassen, wenn der entsprechende Rechtsrahmen vorhanden ist. Gleiches gilt für die Verwaltung: Eine digitale Verwaltung kann es nur dann geben, wenn die Nutzung digitaler Technologien rechtlich abgesichert wird.

Realität: Hürden bei der Digitalisierung

Digitalisierungsprojekte scheitern in Deutschland immer wieder an fehlenden gesetzlichen Voraussetzungen. Ein Beispiel aus der Praxis: Beim Amtsgericht Olpe begann im Jahr 2005 ein Pilotprojekt zur elektronischen Verfahrensführung.[6] Scheidungsverfahren sollten beschleunigt, effizienter und bürgerfreundlicher gestaltet werden. Es scheiterte daran, dass die Mittel der elektronischen Signatur nicht ausreichten. So akzeptierten die Scheidungsämter die von den Richtern mit einer qualifizierten elektronischen Signatur (QES) unterschriebenen Scheidungsurteile mangels sicherer Herkunftsnachweise nicht.[7] Ihnen reichte Name und Dienstbezeichnung des Richters für den Nachweis einer Erlassbehörde nicht aus. Die Folge: Die Urteile wurden ausgedruckt, ausgefertigt und per Post verschickt.

In diesem Praxisbeispiel wird deutlich, dass die QES nicht ausreicht, um rechtssicher nachzuweisen, dass eine konkrete Behörde ein Dokument ausgestellt hat. Mit der QES wird juristisch nur unterstellt, dass das Dokument von der signierenden natürlichen Person stammt. Die Frage, ob diese Person immer noch Richter ist, an ein anderes Gericht versetzt wurde oder derzeit in Elternzeit ist, wird durch eine QES nicht rechtssicher beantwortet.

Die Lösung: das qualifizierte elektronische Siegel (QSiegel) der eIDAS-Verordnung.[8]

Die eIDAS-Verordnung verfügt über die Lösung des Problems: das QSiegel. Es müsste lediglich ergänzend auf dem Dokument angebracht werden, um Herkunft und persönliche Unterschrift von Urteilen elektronisch sicher zu belegen. Hierfür fehlt allerdings bislang die Rechtsgrundlage in den Prozess- und Verfahrensordnungen. **Ob das QSiegel aber in Deutschland eingeführt wird und bei welchen Prozessen es zulässig ist, entscheidet allein der deutsche Gesetzgeber.**

Der Vertrauensraum in der Digitalisierung

Die deutsche Gesetzgebung ist also gefordert. Nur eine rechtssichere Verständigung zwischen Menschen, Software und Maschinen ist eine verlässliche Verständigung. Dazu können die Vertrauensdienste der eIDAS-Verordnung einen wertvollen Beitrag leisten. Wenn sie effektiv eingesetzt werden, entsteht ein Vertrauensraum, in dem eine vertrauensvolle Interaktion zwischen allen Beteiligten ermöglicht wird und durch den das Digitalisierungspotenzial in Verwaltungs- und Geschäftsprozessen ausgeschöpft werden kann.

6 Justiz NRW: Elektronisches Scheidungsverfahren. Elektronischer Datenaustausch bei dem Amtsgericht Olpe, aufgerufen am 01.05.2019 unter *https://bit.ly/2XbGtPI*.

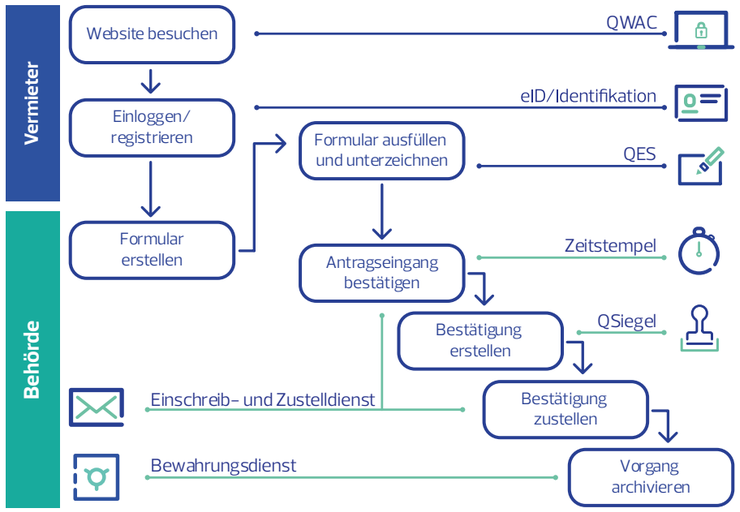
7 Seiffge, Jennifer/Henke, Eva-Maria: Zeitersparnis, Entbürokratisierung, Optimierung. e-Justice Ausgabe 01/2017. S. 13, aufgerufen am 01.05.2019 unter *https://bit.ly/2WsZvno*.

8 Vgl.: Hölters, Jennifer/Henke, Eva-Maria: Verwendungsmöglichkeiten und Nutzen des qualifizierten elektronischen Siegels. In: Internet-Zeitschrift für Rechtsinformatik und Informationsrecht. JurPC Web-Dok. 44/2017, Abs. 1–36, aufgerufen am 01.05.2019 unter *https://bit.ly/2YSZ8jp*.

9 Siehe für das Land Berlin: Berliner Morgenpost: Berliner Verwaltung soll besser werden: Umsetzung dauert. 07.03.2018, aufgerufen am 01.05.2019 unter *https://bit.ly/2HXT3LP*.

10 Die Abkürzung QWAC ergibt sich aus dem englischen Begriff „qualified website authentication certificate". Eine genaue Definition folgt auf S. 12.

Auch hierfür ein Beispiel: Wer seinen Wohnort ummelden will, muss mit einem hohen Aufwand und nicht selten mit wochenlangen Wartezeiten für einen Termin bei der zuständigen Behörde rechnen.[9] Viel einfacher wäre eine digitale Ummeldung. Damit das online funktioniert, muss der Bürger sicher identifiziert werden. Dafür eignet sich die Online-Ausweisfunktion des elektronischen Personalausweises. Die Sicherheit der jeweiligen Website wird durch qualifizierte Website-Zertifikate (QWACs)[10] nachgewiesen. Meldebescheinigung und Erklärung des Vermieters werden mit einer QES und einem QSiegel versehen. Der gesamte Prozess und die Dokumente erhalten qualifizierte elektronische Zeitstempel und QSiegel, damit der Vorgang auf lange Zeit nachvollziehbar und unverändert gespeichert und archiviert werden kann. Durch dieses Vorgehen ist die gesamte Kommunikation im Meldeprozess abgesichert. Zusätzlich werden die örtlichen Ämter von Routineaufgaben befreit. Wenn der Bürger zeitgleich mit der Meldebescheinigung auch einen kurzfristigen Termin im Amt erhält, kann die neue Adresse schnell im Personalausweis nachgetragen werden.



Der digitale Vertrauensraum am Beispiel der Ummeldung einer Wohnung

eIDAS-Vertrauensdienste können für viele Fälle genutzt werden: bei der Ausstellung von Führungszeugnissen, Arbeitsbescheinigungen oder Fortbildungsnachweisen, der Zustellung von Wahlunterlagen, der Ummeldung von Fahrzeugen oder bei Bescheiden oder Verwarnungen im Straßenverkehr. All diese Kommunikations- und Serviceprozesse brauchen Werkzeuge, damit sie in der digitalen Welt sicher und vertrauenswürdig gestaltet werden können. Die eIDAS-Verordnung schafft mit ihren Vertrauensdiensten die Voraussetzung dafür. Sie ermöglicht einen Vertrauensraum, in dem komplett digitalisierte behördliche oder unternehmerische Workflows möglich sind, weil alle dahinter stehenden Dienste und Produkte zertifiziert sind und ein kontrolliert hohes Niveau sichergestellt wird. Zudem ergibt sich so ein einheitlicher Umgang mit juristischen Fragen, etwa zur Haftung. Solche Vertrauensräume sind eine notwendige Bedingung, um die deutsche Verwaltung erfolgreich digitalisieren zu können.

2 DIE AKTUELLEN RECHTLICHEN RAHMENBEDINGUNGEN VON VERTRAUENSDIENSTEN

11 Europäische Kommission: Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen. Eine Digitale Agenda für Europa. 19.05.2010. S. 8, aufgerufen am 01.02.2019 unter *https://www.kowi.de/Portaldata/2/Resources/fp/2010-com-digital-agenda-de.pdf*.

12 Vgl.: Hölters, Jennifer/Henke, Eva Maria: Verwendungsmöglichkeiten und Nutzen des qualifizierten elektronischen Siegels. In: Internet-Zeitschrift für Rechtsinformatik und Informationsrecht. JurPC Web-Dok. 44/2017. Abs. 4f, aufgerufen am 01.02.2019 unter *https://bit.ly/2YSZ8jp*.

Die digitale Agenda 2010 der EU-Kommission kam zu dem Schluss, dass die heterogenen Regelungen bei der elektronischen Signatur in den einzelnen Ländern für den Aufbau eines digitalen Binnenmarkts hinderlich waren.[11] Obwohl die Gleichstellung der QES mit der händischen Unterschrift unter anderem in der EU-Signaturrichtlinie rechtlich festgeschrieben worden war, war eine entsprechende Kommunikation unter den Mitgliedstaaten nur in Ausnahmefällen möglich. Es gab schlicht keine einheitlichen rechtlichen und technischen Lösungen, die miteinander kompatibel waren und gegenseitig anerkannt wurden.

Diese Probleme wurden mit der eIDAS-Verordnung gelöst. Als europäische Verordnung gilt sie unmittelbar in allen Mitgliedstaaten der Europäischen Union und hat Vorrang vor nationalem Recht. Das bis dato in Deutschland geltende SigG wurde am 29. Juli 2017 durch die eIDAS-Verordnung abgelöst. Sie lässt im Gegensatz zum SigG zu, dass QSiegel in den Mitgliedstaaten eingeführt werden können. Ermöglicht wird dies in Art. 37 Abs. 1 (Elektronische Siegel in öffentlichen Diensten).[12] Zusätzlich wurde in Deutschland das Vertrauensdienstegesetz (VDG)[13] geschaffen, das die Verordnung seit 29. Juli 2017 ergänzt und auch bislang offen gelassene Bereiche im deutschen Recht regeln soll. Damit verbunden ist im Februar 2019 zudem die Vertrauensdiensteverordnung (VDV)[14] in Kraft getreten.

2.1 Die eIDAS-Verordnung

13 Vertrauensdienstegesetz (VDG). 18.07.2017, aufgerufen am 01.05.2019 unter *http://www.gesetze-im-internet.de/vdg/index.html*.

14 Verordnung zu Vertrauensdiensten (Vertrauensdiensteverordnung – VDV). 15.02.2019, aufgerufen am 01.05.2019 unter *https://bit.ly/2HXAZI3*.

15 Bundesdruckerei-Whitepaper: Die eIDAS-Verordnung – Die Basis für ein starkes digitales Europa. S. 6, aufgerufen am 01.05.2019 unter *https://www.bundesdruckerei.de/de/whitepaper-eIDAS*.

Die eIDAS-Verordnung der Europäischen Union ist seit dem 17. September 2014 geltendes Recht in allen 28 Mitgliedstaaten und im Europäischen Wirtschaftsraum. Sie ist von Island, Liechtenstein und Norwegen adaptiert worden. Durch die Verordnung wird die EU-Signaturrichtlinie (1999/93/EG) aufgehoben.[15] Die eIDAS-Verordnung bildet somit das regulatorische Dach, um sichere und vertrauenswürdige elektronische Geschäftsprozesse in Europa umsetzen zu können. Nationale Regelungen werden zwar nicht außer Kraft gesetzt, sie dürfen aber der eIDAS-Verordnung nicht widersprechen oder müssen sich auf spezifische nationale Anwendungen beschränken (Anwendungshoheit). Das deutsche SigG wurde daher aufgehoben, um Rechtssicherheit zu schaffen. Eine Evaluation der Verordnung durch die Europäische Kommission ist für das Jahr 2020 vorgesehen.

2.1.1 Die Werkzeuge des elektronischen Rechtsverkehrs

Vertrauensdienste für den elektronischen Rechtsverkehr gibt es schon länger. Allerdings wurden sie bislang von Endanwendern eher selten genutzt. Das lag wohl vor allem an der komplexen Ausgestaltung der technischen Werkzeuge auf Basis der früher geltenden rechtlichen Grundlagen (EU-Signaturrichtlinie [1999] und SigG [1997]). Denn der Einsatz von Signaturen, die auf Zertifikaten akkreditierter Anbieter von Hochsicherheitsmodulen mit abgesicherten Anwendungskomponenten beruhen, ist ein ebenso weites wie komplexes Feld.

Prinzipiell wird zwischen Vertrauensdiensten und qualifizierten Vertrauensdiensten unterschieden. Qualifizierte Vertrauensdienste sind in allen Mitgliedstaaten gleichwertig anzuerkennen und können somit standardisiert in der Europäischen Union angewandt werden.

Alle qualifizierten Vertrauensdienste der eIDAS-Verordnung zeichnen sich durch zwei Eigenschaften aus:

1. Qualifizierte Vertrauensdienste sind mit einem EU-Vertrauenssiegel gekennzeichnet. Dadurch sollen Verbraucher die Qualität der Produkte, ähnlich wie beim EU-Biosiegel, auf den ersten Blick erkennen und einschätzen können. Das EU-Vertrauenssiegel wurde mit der ersten Durchführungsverordnung Nr. 2015/806 der eIDAS-Verordnung eingeführt.

Das EU-Vertrauenssiegel

2. Qualifizierte Vertrauensdienste werden in eine nationale Vertrauensliste aufgenommen, die die qualifizierten Vertrauensdiensteanbieter eines Landes enthält. Dafür sind die nationalen Aufsichtsbehörden zuständig. In Deutschland sind dies die Bundesnetzagentur oder das Bundesamt für Sicherheit in der Informationstechnik. Sie stellen die nationale Liste in Form einer TLS (strukturiert nach ETSI Technical Specification ETSI TS 119 612) maschinenlesbar zur Verfügung und ermöglichen so eine automatische Prüfung. Die EU-Kommission stellt alle nationalen Vertrauenslisten zentral in einer „List of Trusted Lists" bereit. Somit können Anbieter von technischen Komponenten die Liste von einer zentralen und vertrauenswürdigen Stelle beziehen und die Vertrauenswürdigkeit von Zertifikaten prüfen.

Europäische Standardisierung

Um technische Normen und Standards zu erarbeiten, gibt es in der Europäischen Union zwei Standardisierungsorganisationen:

- **ETSI** (European Telecommunications Standards Institute) und
- **CEN** (Comité Européen de Normalisation).

Beide Organisationen wurden beauftragt, die bestehenden Interoperabilitätsnormen grundsätzlich neu zu strukturieren und umfassend zu überarbeiten. So wird sichergestellt, dass in Europa eingesetzte eIDAS-Vertrauensdienste interoperabel und grenzüberschreitend verwendet werden können.

Die eIDAS-Verordnung sieht verschiedene qualifizierte Vertrauensdienste vor, die wir im Folgenden erläutern und die alle auf einem elektronischen Zertifikat basieren.[16]

16 Alle eIDAS-Werkzeuge basieren auf etablierten und erprobten Public-Key-Infrastruktur-Verfahren.

Das elektronische Zertifikat

Das elektronische Zertifikat ist eine Basistechnologie, die in nahezu allen eIDAS-Werkzeugen zum Einsatz kommt. Dabei handelt es sich um eine Sammlung von Informationen über den Zertifikatsnehmer, den Zertifikatsaussteller (Vertrauensdiensteanbieter), Angaben zum Zertifikat selbst (Einsatzzweck, Gültigkeitszeitraum, Prüfbarkeit, zugrundeliegende Ausstellungsrichtlinien etc.) und die Angabe des öffentlichen Schlüssels des Zertifikats (Zertifikatsinhalte). Diese Zertifikatsinhalte werden durch den Vertrauensdiensteanbieter auf Richtigkeit geprüft und wiederum von ihm elektronisch unterschrieben und somit bestätigt. Auf diese Weise wird sichergestellt, dass die Zertifikatsangaben vor unbemerkter Manipulation geschützt werden.
Ein Zertifikat ist prinzipiell immer öffentlich. Ausschlaggebend für die Qualität, also gewissermaßen die Aussagekraft des Zertifikats, sind der zugrundeliegende Prozess zur Identifizierung des Zertifikatsnehmers, der Prozess der Erzeugung des Schlüsselmaterials und des Zertifikats sowie der Aufbewahrungsort des privaten Schlüssels.
Die eIDAS-Verordnung bzw. die referenzierten Durchführungsrechtsakte definieren in diesem Zusammenhang, welche Rahmenbedingungen eingehalten werden müssen, damit unter anderem das Niveau „qualifiziertes Zertifikat" erreicht werden kann.

Qualifiziertes Zertifikat für die elektronische Signatur (QES)

Eine QES beruht auf einem qualifizierten Zertifikat. Die QES wird mit der elektronischen Datei so verknüpft, dass nach Unterzeichnung keine unbemerkte Veränderung des signierten Dokuments durchgeführt werden kann. Darüber hinaus ist durch das Zertifikat ersichtlich, wer das Dokument unterschrieben hat. Eine QES wird von oder im Auftrag einer natürlichen Person erzeugt. Sie wird häufig für Willenserklärungen natürlicher Personen verwendet. Eine QES ist für die Sicherung der Anwendungsebene zuständig.

Qualifiziertes Zertifikat für das elektronische Siegel (QSiegel)

Ein QSiegel beruht ebenfalls auf einem qualifizierten Zertifikat. Die Funktionsweise des QSiegels ist vergleichbar mit der QES. Der entscheidende Unterschied liegt darin, dass ein QSiegel nicht einer natürlichen, sondern einer juristischen Person – etwa einem Unternehmen – zugeordnet wird. Die gesiegelte elektronische Datei erhält einen entsprechenden Ursprungsnachweis, nicht jedoch eine Willenserklärung. Ebenso wie die QES ist das QSiegel für die Sicherung der Anwendungsebene zuständig.

Qualifiziertes Zertifikat für die Website-Authentifizierung (QWAC)

Ein QWAC (aus dem Englischen: qualified website authentication certificate) ist der digitale Ausweis für eine Website oder Cloud-Anwendung. Auf Basis von QWACs können Betreiber von Websites sicher identifiziert werden. Diese Technologie basiert auf SSL/TLS-Verschlüsselung und wird weltweit verwendet. Hier wird allerdings – anders als bei der „reinen" SSL/TLS-Verschlüsselung, bei der die Browser- bzw. Betriebssystemhersteller die Vertrauenswürdigkeit der zugrundeliegenden Zertifikate bestimmen – die Vertrauenswürdigkeit durch die EU-Vertrauensliste bestimmt. Dies ist besonders wichtig, um vertrauenswürdige, authentisierte und verschlüsselte Kommunikationsbeziehungen etablieren zu können, zum Beispiel zwischen EU-Bürgern und Websites oder zwischen IT-Systemen. QWACs sind nicht nur serverseitig einsetzbar, sondern auch clientseitig. Somit kann sich auch ein Server gegenüber einem anderen Server als Client ausweisen. Ein QWAC ist für die Sicherung der Transportebene zuständig.

Qualifizierter Bewahrungsdienst für QES und QSiegel

Eine einmal erzeugte QES oder ein einmal erzeugtes QSiegel ist dauerhaft gültig. Die Prüfbarkeit kann über die Jahre stark eingeschränkt werden, da von der technischen Entwicklung abhängt, wie vertrauenswürdig der zugrundeliegende kryptografische Algorithmus noch ist. Deshalb konserviert der qualifizierte Bewahrungsdienst den Zustand der qualifiziert signierten und/oder qualifiziert gesiegelten Datei.

Qualifizierter Validierungsdienst für QES, QSiegel und qualifizierte Bewahrungsdienste

Diese Dienste sind auf QES und QSiegel ausgerichtet. Sie ermöglichen die unabhängige Prüfung der mathematischen und rechtlichen Gültigkeit einer QES oder eines QSiegels. Als Ergebnis wird ein spezieller Prüfbericht herausgegeben, der die Prüfschritte und -ergebnisse aufführt. Dieser Prüfbericht kann in das Dokument, sofern dies technisch unterstützt wird, eingebettet werden und ermöglicht somit über einen langen Zeitraum die Nachvollziehbarkeit des unabhängigen Prüfergebnisses.

Qualifizierter Dienst für die Zustellung elektronischer Einschreiben

Der Dienst für die Zustellung elektronischer Einschreiben bringt den postalischen Einschreibedienst in die elektronische Welt. Sowohl der Absender als auch der Empfänger werden identifiziert und die Nachricht wird vor unbemerkter Manipulation durch mindestens eine fortgeschrittene elektronische Signatur geschützt. Das Datum und die Zeit des Versands, Empfangs oder eine Änderung der Nachricht werden mithilfe eines qualifizierten Zeitstempels geschützt. Dieser Dienst ist bereits durch das De-Mail-Gesetz in vergleichbarer Form bekannt.

Qualifizierter elektronischer Zeitstempel

Die Funktionsweise eines qualifizierten elektronischen Zeitstempels ist vergleichbar mit der QES. Der Zeitstempel konserviert verbindlich den Zeitpunkt, an dem die elektronische Datei vorgelegt wurde. So ist eindeutig nachvollziehbar, wann die elektronische Datei in welchem Zustand vorlag. Hier wird kein qualifiziertes Zertifikat eingesetzt.

Die Werkzeuge des digitalen Vertrauensraums

QES
Die individuelle digitale Unterschrift

Einschreib- und Zustelldienst
Die sichere digitale Nachricht wie bei der Post oder dem Gerichtsvollzieher

QSiegel
Der verlässliche digitale Stempel für Behörden und Unternehmen

Zeitstempel
Die digitale Stoppuhr wie ein elektronischer Fotobeweis

QWAC
Die sichere Identifizierung eines Website-Betreibers

Bewahrungsdienste
Das digitale ewige Archiv

Validierungsdienst
Der automatische unabhängige Prüfer

2.2 Das Vertrauensdienstegesetz

Das Vertrauensdienstegesetz (VDG) ist Bestandteil des eIDAS-Durchführungsgesetzes.[17] Gleichzeitig hat es das SigG am 29. Juli 2017 außer Kraft gesetzt. Das VDG schafft den einheitlichen Rechtsrahmen für die vom SigG geregelten Bereiche und ergänzt diese um die von der eIDAS-Verordnung neu geschaffenen Regelungsbereiche. Damit füllt es die von der unmittelbar geltenden eIDAS-Verordnung offengelassenen Bereiche im deutschen Recht aus. Im Februar 2019 ist zudem die Vertrauensdiensteverordnung (VDV) in Kraft getreten. In der VDV werden Anforderungen an die Barrierefreiheit, die Ausgestaltung der Deckungsvorsorge qualifizierter Vertrauensdiensteanbieter, die Dokumentation bei der Zertifikatsausgabe, die dauerhafte Prüfbarkeit von Zertifikaten sowie die Anzeige von QES- oder QSiegel-Erstellungseinheiten konkretisiert.[18]

17 Gesetz zur Durchführung der Verordnung 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. 18.07.2017, aufgerufen am 01.04.2019 unter *https://bit.ly/2MlU5qG*.

2.3 Formvorschriften nach deutschem Recht

Nach aktuellem deutschen Recht sind viele Verträge formfrei möglich. Nur bestimmte Kontrakte brauchen eine besondere Form, wie die Textform, die Schriftform, die notariell beurkundete Form oder die Form der Schließung vor einer besonderen öffentlichen Stelle. Vor diesem Hintergrund definieren Formvorschriften, unter welchen Bedingungen eine Erklärung rechtliche Wirkung entfaltet. Die Systematik der Formvorschriften stammt aus dem Jahre 1896 und muss für die digitale Welt verändert werden. Denn an komplexe Maschinen oder Software wurde damals noch nicht gedacht. In wenigen Jahren wird jedoch jeder Vertrag und jede rechtserhebliche Verfahrenshandlung im Zivil- oder öffentlichen Recht digital erledigt werden. Für die Verbindung zwischen analogem Handeln und der digitalen Äußerung braucht es einen Vertrauensanker. Für bestimmte rechtserhebliche Handlungen muss sicher sein, wer was wann und zu wem digital gesagt hat.

18 Verordnung zu Vertrauensdiensten (Vertrauensdiensteverordnung – VDV). 15.02.2019, aufgerufen am 01.04.2019 unter *https://bit.ly/2wlMf5n*.

Das deutsche Recht kennt verschiedene Formvorschriften für unterschiedliche Rechtsgeschäfte. Grundsätzlich gibt es aber keine vorgeschriebene Form für Verträge und andere Rechtsgeschäfte. Deshalb können Verträge in jeder beliebigen Form geschlossen werden. Ein Vertrag wird dann eingegangen, wenn zwei zum Ausdruck gebrachte und übereinstimmende Willenserklärungen von zwei natürlichen Personen abgegeben werden und zugehen. Dies geschieht bei gegenseitigen Verträgen durch Angebot und Annahme eines Angebots. Deshalb können Verträge grundsätzlich auch per E-Mail, Messenger oder Videotelefonie geschlossen werden. Einseitige Rechtsgeschäfte werden durch die Willensäußerung mit dem jeweiligen Rechtsfolgewillen kundgetan und müssen zudem zugehen, um die jeweilige Wirkung zu entfalten (zum Beispiel Widerruf, Kündigung, Rücktritt).

Für bestimmte Rechtsgeschäfte sollten spezielle Formen vorgesehen werden. Denn besonders bedeutende Rechtsgeschäfte müssen verlässlicher sein als andere Verträge. Daran hat auch die Rechtsordnung ein besonderes Interesse. Beispielsweise wird ein Arbeitsvertrag schriftlich geschlossen, weil dieser eine wichtige Grundlage eines Arbeitnehmers ist und zudem eine soziale Bedeutung hat.

Im Laufe der Jahre wurden die jeweiligen Formerfordernisse immer wieder angepasst. Sie sollen eine besondere Funktion erfüllen, die für das jeweilige Rechtsgeschäft bzw. den jeweiligen Schutzzweck der Norm notwendig ist. Dazu zählen die Informationsfunktion, Klarstellungs- und Beweisfunktion, Kontrollfunktion, Warnfunktion und Beratungsfunktion.[19]

19 Ellenberger, Jürgen: Palandt, Kommentar zum Bürgerlichen Gesetzbuch. 71. Aufl. 2012. § 125, Rn. 2 ff.

Informationsfunktion	Klarstellungs- und Beweisfunktion	Kontrollfunktion	Warnfunktion	Beratungsfunktion
Die Parteien sollen über den Inhalt der Rechte und Pflichten informiert sein und bleiben, auch nach Vertragsschluss. Die Textform erfüllt auch diese Funktion.	Es wird der Inhalt des Rechtsgeschäfts beweisbar. Deshalb unterscheidet man weiter in Identitätsfunktion, Echtheitsfunktion und Verifikationsfunktion. Es sollen die Identität des Unterzeichners, die Echtheit der Urkunde und der Ursprung der Erklärung vom Empfänger beweisbar sein.	Auch Dritte wie Behörden können den Inhalt des Rechtsgeschäfts kontrollieren.	Vor den rechtlichen Folgen eines Rechtsgeschäfts soll gewarnt werden. Im Verbraucherrecht wird hier oft auch mit Informationspflichten und Widerrufsrechten operiert, um der Warnfunktion gerecht zu werden.	Bei notariell beurkundeten Erklärungen soll eine unabhängige Beratung durch den Notar sichergestellt werden, um die Bedeutung des Geschäfts zu vermitteln.

Die verschiedenen Funktionen von Verträgen

20 Ellenberger, Jürgen: Palandt, Kommentar zum Bürgerlichen Gesetzbuch. 71. Aufl. 2012. § 125, Rn. 2.

Ein Beispiel: Die Warnfunktion wird genutzt, um auf die Folgen eines belastenden Rechtsgeschäfts aufmerksam zu machen. Dies erfolgt heute zunehmend durch die Nutzung der Rechtsinstitute von Widerrufsrechten und Informationspflichten für Verbraucher.[20] Denn die Rechtswirklichkeit zeigt, dass das Kleingedruckte eine so hohe Aufmerksamkeit und vertieftes Spezialwissen erfordert, dass es die meisten Menschen schlicht überfordert.

Zuletzt wurde neben der Schriftform – also einer Erklärung mit eigenhändiger Unterschrift mit Tinte auf Papier – die Textform eingeführt, um Verträge zum Beispiel auch per E-Mail schließen zu können, wenn die formlose Verpflichtung nicht ausreicht bzw. ein besonderes Informationsbedürfnis besteht. Um das Jahr 1900, als das Bürgerliche Gesetzbuch (BGB) eingeführt wurde, war die Schriftform die günstigste Möglichkeit, bedeutende Verträge zu schließen. Bis in die Mitte der 1950er-Jahre wurden Verträge noch von Hand geschrieben und von dem Verpflichteten eigenhändig unterschrieben. Später wurden Verträge überwiegend durch Schreibmaschinen vorbereitet. Das geschieht heute digital. Gleichwohl behält die Schriftform ihre wesentliche Funktion im Recht der Formvorschriften. Zu Beginn des 21. Jahrhunderts wurde die QES weitestgehend der Schriftform gleichgestellt.

Auch für juristische Personen – etwa Unternehmen – gelten diese Formvorschriften. Juristische Personen sind Rechtsgebilde, die zivilrechtlich wie natürliche Personen behandelt werden. Sie sind abstrakt und können deshalb keine eigene strafrechtliche Schuld auf sich laden oder sich etwa durch einen Ehevertrag binden. Gleichwohl müssen diese juristischen Personen handeln können und tun dies durch ihre menschlichen, gesetzlichen Vertreter. Diese müssen handschriftlich unterschreiben oder qualifiziert elektronisch signieren, um die Schriftform einzuhalten.

Mangelnde Verankerung im deutschen Recht

Mit der eIDAS-Verordnung wurde nun für diese juristischen Personen das QSiegel ein-geführt. Ein QSiegel kann nur von einer juristischen Person oder von einer öffentlichen Stelle eingesetzt werden und hat eine starke Beweisfunktion. Dieses Mittel findet sich jedoch im deutschen Recht in Bezug auf die Formvorschriften nicht wieder. Hier gilt nach wie vor der „juristische Umweg", dass ein natürlicher gesetzlicher Vertreter, etwa ein Mitarbeiter, für eine juristische Person (also sein Unternehmen) signieren muss. Es wäre daher sinnvoll, das QSiegel gesetzlich in den elektronischen Geschäftsverkehr einzubinden. Ziel einer Regelung muss es sein, dass sich ein Unternehmen auf die Rechtswirkung und der Empfänger auf die Herkunft des QSiegels verlassen kann. Dazu braucht es neben der Rechtswirkung des QSiegels auch Formvorschriften im nationalen Recht, die diese Form für Unternehmen verbindlich vorsehen.

Hiermit ist nicht gemeint, das QSiegel der Schriftform bei einer Willenserklärung inhaltlich gleichzustellen. Dies ist gemäß der eIDAS-Verordnung nicht vorgesehen. Vielmehr muss es das Ziel sein, Unternehmen eine neue, elektronische und verbindliche Form zu ermöglichen.

Negative und positive Publizität bedeutet, dass die Eintragungen im Handelsregister als richtig und vollständig unterstellt werden dürfen, auch wenn sie nicht den tatsächlichen Umständen entsprechen. Dies ist in § 15 Handelsgesetzbuch geregelt.

Im Rechtsverkehr kann sich das Gegenüber nur auf die fiktive Wahrheit aus dem Handelsregister verlassen (negative und positive Publizität). Der dort angegebene Vertreter ist zeichnungsberechtigt. Eine Überprüfung für den Rechtsverkehr, der durch Formerfordernisse geschützt werden soll, ist also nur über diesen Kontrollumweg möglich. Bei dem QSiegel hingegen ist dies nicht mehr nötig, weil die Überprüfung der Echtheit des QSiegels elektronisch automatisiert durch das System der Vertrauensdienste geschieht. Der tatsächliche gesetzliche Vertreter muss also nicht jedes Mal selbst handeln, sondern kann delegieren.

In Unternehmen ist es möglich, dass die gesetzlichen Vertreter Vollmachten ausstellen und so auch andere Personen rechtswirksam unterzeichnen können. Mit dem QSiegel ist das auch machbar. Allerdings genießt der Rechtskreis durch das QSiegel mehr Vertrauensschutz, weil der Erklärungsursprung als gesetzlich vermutet unterstellt werden kann.[21] Dies ist bei einem Briefkopf oder einer E-Mail nicht der Fall.

Eine weitere Formvorschrift ist die elektronische Textform. Sie wurde durch die europäische Verbraucherschutzrichtlinie (Richtlinie 2011/83/EU) seit 2014 mit der Neufassung des § 126b BGB in deutsches Recht übernommen. Dort ist geregelt, dass die Textform auch dann gewahrt ist, wenn der Empfänger der in Textform abgegebenen Erklärung den Absender erkennen und die Erklärung dauerhaft speichern kann. Dies wird auch für E-Mail-Nachrichten angenommen. Noch ungeklärt ist dies für Messenger-Dienste wie Skype, WhatsApp, Snapchat, Facebook oder Instagram.

Anders verhält es sich bei De-Mail: Sie ersetzt zwar nicht die Schriftform, wie es die QES gem. § 126a BGB regelt, kann aber dennoch im Rahmen des E-Government-Gesetzes (EGovG) gleichwertig für die Kommunikation zwischen Bürger und Staat eingesetzt werden. Grund dafür ist, dass bei dem Standard De-Mail grundsätzlich nur der Diensteanbieter die QES im eigenen Namen anbringt, um die Nachrichtenvorgänge zu signieren. Sollen Dokumente elektronisch verarbeitet werden, kann die Schriftform im Privatrecht nach § 126 Abs. 3 BGB durch die elektronische Form (§ 126a BGB) ersetzt werden. Entsprechend kann im Bereich des Verwaltungsverfahrensrechts gemäß § 3a Abs. 2 Satz 1 und 2 Verwaltungsverfahrensgesetz (VwVfG) die Schriftform „soweit nicht durch Rechtsvorschrift etwas anderes bestimmt ist, durch die elektronische Form ersetzt werden. Der elektronischen Form genügt ein elektronisches Dokument, das mit einer qualifizierten elektronischen Signatur versehen ist." Um die Schriftform zu ersetzen, müsste dies der Nutzer selbst mit einer eigenen Signatur machen. Unter das Schriftformerfordernis fallen etwa Bauanträge, Baugenehmigungen, Steuerbescheide, Widersprüche gegen Verwaltungsakte gem. § 70 VwGO (Verwaltungsgerichtsordnung) oder Anträge im förmlichen Verwaltungsverfahren gem. § 64 VwVfG. Vergleichbare Regelungen finden sich im Allgemeinen Teil des Sozialgesetzbuchs (SGB I) und in der Abgabenordnung (AO). Gemäß § 36a SGB I und § 87a AO kann auch in diesen Bereichen die eigenhändige Unterschrift durch die QES ersetzt werden.

21 Die gesetzliche Vermutung aus Art. 35 Abs. 2 eIDAS-Verordnung ist umstritten und wird hier überwiegend in der etwas schwächeren Rechtsfigur des Anscheinsbeweises gesehen. Vgl.: Roßnagel, Alexander: Das Recht der Vertrauensdienste. 2016. S. 183 ff. m.w.N.

2.4 Beweisvorschriften nach deutschem Recht

Form- und Beweisvorschriften sind zwei Seiten einer Medaille. Die Formvorschriften beschäftigen sich mit der Entstehung von Rechtswirkungen, die Beweisvorschriften mit der Beweiskraft der eingesetzten Mittel. Der Vorteil eines wirksamen Vertrags ist, die Rechte und Pflichten vor einem Gericht durchsetzen zu können. Form- und Beweisvorschriften greifen ineinander und schaffen einen Vertrauensraum, in dem sich rechtserhebliches Handeln für die Beteiligten sicher abspielen kann. Ohne diesen Vertrauensraum des Rechts ist keine wirtschaftliche Entwicklung möglich. Vor diesem Hintergrund beschäftigt sich dieser Abschnitt mit der Behandlung der Vertrauensdienste der eIDAS-Verordnung im Beweisverfahren.
Die eIDAS-Verordnung sieht vor, dass bestimmten Vertrauensdiensten die Rechtswirkung

und die Zulässigkeit als Beweismittel in Gerichtsverfahren nicht allein deshalb abgesprochen werden dürfen, weil sie in elektronischer Form vorliegen oder weil sie die Anforderungen an den jeweils qualifizierten elektronischen Vertrauensdienst nicht erfüllen. Sie sind damit grundsätzlich Beweismittel im Gerichtsverfahren. Das gilt etwa für QES, QSiegel, qualifizierte elektronische Zeitstempel und qualifizierte elektronische Einschreibedienste.

Das sicherste Beweismittel im deutschen Prozessrecht ist der Urkundenbeweis durch eine öffentliche oder private Urkunde.[22] Der Inhalt der Urkundenerklärung gilt als vom Aussteller abgegeben (formelle und materielle Beweiskraft) und schränkt die freie Beweiswürdigung des Richters gem. § 286 der Zivilprozessordnung (ZPO) ein.[23] Dies gilt jedoch nur für körperliche, handschriftlich unterschriebene Urkunden. Für elektronische Urkunden bewirkt auch das qualifizierte elektronische Zertifikat eines qualifizierten Vertrauensdiensts für eine elektronische Signatur nach § 371a ZPO lediglich den Anscheinsbeweis für private elektronische Dokumente bzw. die gesetzliche Vermutung für öffentliche elektronische Dokumente nach §§ 371a Abs. 3, 437 ZPO.[24] Gleichwohl werden auf die so signierten elektronischen Dokumente die Vorschriften für die Beweiskraft von Urkunden gem. § 371a Abs. 1 Satz 1 und Abs. 3 Satz 1 ZPO entsprechend angewendet.

Art. 35 eIDAS-Verordnung
Rechtswirkung elektronischer Siegel

(1) Einem elektronischen Siegel darf die Rechtswirkung und die Zulässigkeit als Beweismittel in Gerichtsverfahren nicht allein deshalb abgesprochen werden, weil es in einer elektronischen Form vorliegt oder nicht die Anforderungen an qualifizierte elektronische Siegel erfüllt.

(2) Für ein qualifiziertes elektronisches Siegel gilt die Vermutung der Unversehrtheit der Daten und der Richtigkeit der Herkunftsangabe der Daten, mit denen das qualifizierte elektronische Siegel verbunden ist.

...

Die Beweiskraft für die Werkzeuge der eIDAS-Verordnung ist nicht im deutschen Recht geregelt (mit Ausnahme der QES, weil sie bereits im SigG vorgesehen war). Auch das VDG hat hier keine Änderungen vollzogen. Die eIDAS-Verordnung selbst soll entgegen ihrem Wortlaut in der deutschen Übersetzung keine gesetzliche „Vermutung" für die Beweiskraft des QSiegels schaffen, sondern ebenfalls den Anscheinsbeweis für die Unversehrtheit der Daten und die Richtigkeit der Herkunftsangabe der Daten bedeuten.[25] Die eIDAS-Verordnung gilt unmittelbar im deutschen Prozessrecht, da sie selbst die Behandlung als Anscheinsbeweis nach deutscher Systematik verlangen würde. Damit müsste derjenige, der sich gegen eine elektronische Urkunde wehrt, Tatsachen vortragen, die einen atypischen Geschehensablauf wahrscheinlich erscheinen lassen. Diese Anknüpfungstatsachen müssen dann bewiesen werden.

Der Anscheinsbeweis (Prima-facie-Beweis) ist ungeachtet seiner fehlenden dogmatischen Ableitung gewohnheitsrechtlich im deutschen Recht anerkannt und aus der gerichtlichen Praxis nicht wegzudenken. Nach der Rechtsprechung erlaubt er bei typischen Geschehensabläufen den Nachweis eines ursächlichen Zusammenhangs oder eines schuldhaften Verhaltens ohne exakte Tatsachengrundlage, sondern aufgrund von Erfahrungssätzen. [26]

Dies führt zu der Situation, dass elektronische Dokumente, die mit dem technisch zulässigen QSiegel eines Unternehmens oder einer anderen juristischen Person, wie einem Verein (zum Beispiel bei Spendenbescheinigungen) versehen sind, den Anscheinsbeweis

22 Geimer, Reinhold, et al.: ZPO. 30. Aufl. Vor § 415, Rn. 11.

23 Geimer, Reinhold et al.: ZPO. 30. Aufl. Vor § 415, Rn. 2ff.

24 Vgl. Geimer, Reinhold et al.: ZPO. 30. Aufl. Vor § 415, Rn. 8.

25 Roßnagel, Alexander: Das Recht der Vertrauensdienste. 2016. S. 183 ff. m.w.N.

26 Greger, Reinhard et al.: ZPO. 30. Aufl. Vor § 284, Rn. 29.

für die Unversehrtheit und Richtigkeit der Herkunftsangabe der Daten für sich in Anspruch nehmen können. Darüber hinaus gelten hier jedoch nicht die Beweiskraftregelungen für private Urkunden, weil dies eine handschriftliche (oder signierte) Unterschrift des Ausstellers erfordert. Dies biete das QSiegel nicht, weil keine Individualisierung des Erklärenden zugelassen würde.[27]

Das QSiegel bei elektronischen Dokumenten von öffentlichen Stellen entfaltet hingegen nach § 371a Abs. 3 in Verbindung mit §§ 415, 437 ZPO die Vermutung der Echtheit der Urkunde bzw. des elektronischen Dokuments, wenn es außerdem das Erscheinungsbild einer öffentlichen Urkunde hat. Denn § 371a Abs. 3 ZPO beschränkt sich nicht nur auf die Urkunde, die den individualisierten Aussteller erkennen lassen muss, sondern bezieht sich auf alle öffentlichen elektronischen Dokumente und ist entsprechend weiter gefasst. Aus dieser Perspektive des Beweisrechts ist das QSiegel für Behörden also bereits voll nutzbar.

§ 371a Abs. 3 ZPO
Die Beweiskraft elektronischer Dokumente

Auf elektronische Dokumente, die von einer öffentlichen Behörde innerhalb der Grenzen ihrer Amtsbefugnisse oder von einer mit öffentlichem Glauben versehenen Person innerhalb des ihr zugewiesenen Geschäftskreises in der vorgeschriebenen Form erstellt worden sind (öffentliche elektronische Dokumente), finden die Vorschriften über die Beweiskraft öffentlicher Urkunden entsprechende Anwendung. Ist das Dokument von der erstellenden öffentlichen Behörde oder von der mit öffentlichem Glauben versehenen Person mit einer qualifizierten elektronischen Signatur versehen, gilt § 437 entsprechend.

	Physische private Urkunde	**Physische öffentliche** Urkunde	Qualifiziert elektronisch **signierte private** Urkunde	Qualifiziert elektronisch **signierte öffentliche** Urkunde	Qualifiziert elektronisch **gesiegelte private** Urkunde	Qualifiziert elektronisch **gesiegelte öffentliche** Urkunde
Beweiswert	Vollbeweis	Vollbeweis	Anscheinsbeweis	Vermutung	Anscheinsbeweis	Vermutung
Entkräftung	Gegenbeweis	Gegenbeweis	Gegenvortrag und Beweis der Anknüpfungstatsache	Gegenbeweis	Gegenvortrag und Beweis der Anknüpfungstatsache	Gegenbeweis
Regelung	§ 416 ZPO	§ 415 ZPO	§ 371a Abs. 1 ZPO	§ 371a Abs. 3 ZPO	Art. 35 Abs. 2 eIDAS-VO	Art. 35 Abs. 2 eIDAS-VO i. V. m. §§ 371a Abs. 3 Satz 2, 437 ZPO

Die Beweiskraft qualifizierter elektronischer Zertifikate

27 Vgl.: Roßnagel, Alexander: Das Recht der Vertrauensdienste. 2016. S. 186.

3 REGELUNGSLÜCKEN IM DEUTSCHEN RECHT

Der in Kapitel zwei dargestellte europäische Rechtsrahmen bietet ein einheitliches Regelwerk für die Nutzung von Vertrauensdiensten im europäischen digitalen Binnenmarkt. Dadurch ist es möglich, komplexe digitale Anwendungen mit entsprechenden Services rechtssicher abzubilden und eine sichere digitale Infrastruktur zu nutzen.

Es bestehen jedoch zahlreiche Regelungslücken für eine erfolgreiche Digitalisierung. Dies ist angesichts des historischen Hintergrunds der gesetzlichen Systematik von Willenserklärungen und Beweisvorschriften nicht verwunderlich. Deshalb sollten die entsprechenden Lücken identifiziert und die Mittel für eine sichere digitale Kommunikation im europäischen Binnenmarkt gesetzlich verankert werden. Die eIDAS-Verordnung ist geschaffen worden, um dies europaweit einheitlich zu ermöglichen.

So wie der Euro das europäische Zahlungsmittel ist, könnten die neuen eIDAS-Werkzeuge EU-weit für alle rechtlichen Verwaltungs- und Geschäftsprozesse genutzt werden – und somit die gleiche digitale Sprache sprechen.

So erlaubt beispielsweise der Einsatz von QWACs die sichere Kommunikation einer Website. Dies ist allerdings noch nicht im Telemediengesetz (TMG) aufgenommen, das durch das IT-Sicherheitsgesetz geändert wurde und eine Verschlüsselung der Kommunikation der Website als aktuellen Stand der Technik erfordert. Hier sollten Websites, deren Kommunikation im öffentlichen Interesse ist, zusätzlich zum Einsatz von QWACs verpflichtet werden, damit der Nutzer den Betreiber einer Website sicher identifizieren kann. Websites sind so immer nach dem aktuellen Stand der Technik abgesichert, denn die technische Sicherheit der Zertifikate kann sich stets daran anpassen. Schließlich können die Kryptoalgorithmen der Zertifikate weiterentwickelt und verbessert werden.

Sowohl die Formvorschriften als auch die Beweisvorschriften erlauben es privaten und öffentlichen Stellen, das QSiegel uneingeschränkt einzusetzen. Das ist vorteilhaft, denn in der behördlichen Zusammenarbeit oder bei der Kommunikation von Gerichten und Behörden ist oft entscheidend, dass die zuständige Behörde siegelt und nicht der Mitarbeiter signiert. Die Herkunftsangabe wird nur durch das QSiegel beweisbar und nicht durch den Aussteller oder ein Attribut im Zertifikat, das zum Erteilungszeitpunkt bestand. So ergänzt das QSiegel die QES in sinnvoller Weise, um je nach Anwendungszweck Herkunft und Authentizität einer digitalen Erklärung sicherzustellen.

Warum das QSiegel in die ZPO aufgenommen werden sollte

Allerdings scheint es der eIDAS-Verordnung zu widersprechen, dass das QSiegel nicht in das BGB oder die ZPO aufgenommen wurde und es so dem Rechtsanwender überlassen bleibt, die europäischen Implikationen zu deuten. Besonders unbefriedigend ist diese Situation der Unklarheit über die prozessrechtlichen Wirkungen des QSiegels, weil auch der Anscheinsbeweis nicht legal definiert und der konkrete Bezug auf das QSiegel im deutschen Prozessrecht nicht explizit geregelt ist.

Die Rechtsfigur des Anscheinsbeweises soll die Beweisführung von Kausalitäten und Verschulden bei einem typischen, der Lebenserfahrung entsprechenden Geschehensablauf erleichtern. Es gibt aber weder besondere Erfahrungswerte zum QSiegel noch kann der Rechtsanwender sein Instrument der digitalen Kommunikation im Gesetzestext zu Beweisregeln wiederfinden. Es ist vor diesem Hintergrund sinnvoll, das QSiegel auch in die ZPO aufzunehmen und in § 371a zu verankern.

Die Maschine rückt in die Nähe des Rechts

Im vorletzten Jahrhundert ging die Systematik der Willenserklärungen und der darauf aufbauenden Beweisvorschriften für Rechtsgeschäfte davon aus, dass nur Menschen rechtserheblich handeln können. Maschinen wurden selbstverständlich nicht als Handelnde im Rechtssinne gesehen. Die digitale Transformation führt jedoch heute dazu, dass immer mehr Maschinen und Software den wirtschaftlichen Austausch von Waren und Dienstleistungen und auch Verwaltungstätigkeiten vornehmen.

Entsprechend gilt die Vorstellung, dass jeder rechtserheblichen Handlung ein Mensch zugeordnet werden muss, heute als überholt. Dieser Vorstellung wird dann nachgehan-gen, wenn weiterhin davon ausgegangen wird, dass das QSiegel keine oder weniger Beweiskraft haben kann, weil es keinem Menschen direkt zugeordnet werden kann.[28]

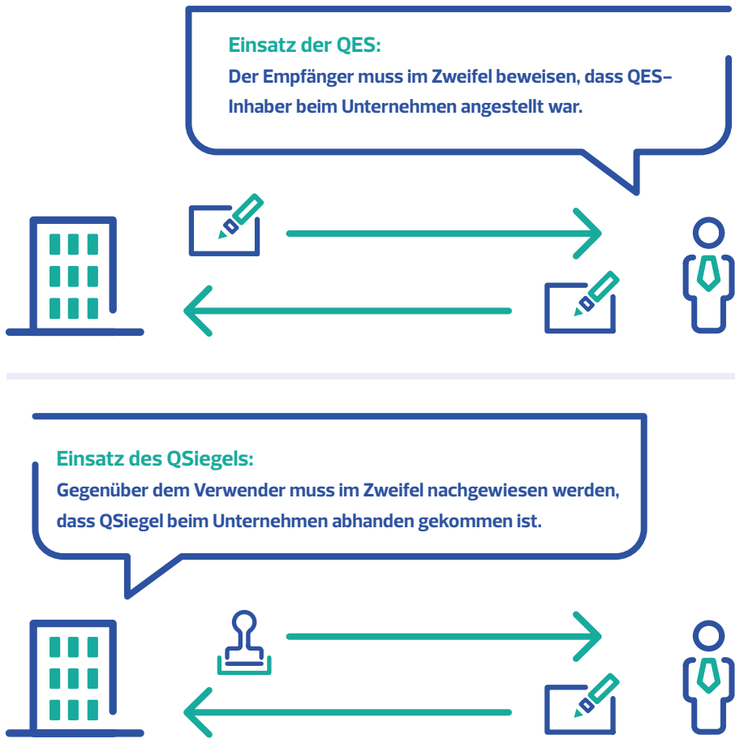
Tatsächlich braucht es nicht die sichere Zuordnung zu einem bestimmten Menschen, die Zuordnung zu einer juristischen Person reicht aus. Denn die Zuordnung bezieht sich im Zivilrecht stets auf die Haftung für eine rechtserhebliche Handlung. Haftung trifft aber nicht nur natürliche, sondern auch juristische Personen. Und in der Rechtswirklichkeit will stets der Empfänger der Willenserklärung oder rechtserheblichen Handlung etwas von dem Handelnden (etwa einen Anspruch durchsetzen wie eine Schadensersatzhaftung). Die Formvorschriften decken genau dieses Interesse durch die Warnfunktion, Beweisfunktion etc. ab.

Der QSiegel-Nutzer ist in den prozessual erheblichen Situationen der in Anspruch Genommene, der Schuldner. Da hinter dem QSiegel nur eine juristische Person stehen kann, richtet sich der Anspruch gegen eine juristische Person. Nur wenn sich diese exkulpieren, also enthaften will, muss sie nachweisen, dass die handelnde Person tatsächlich nicht in Vollmacht der juristischen Person handeln durfte und auch keine Anscheinsvollmacht vorgelegen haben kann. Das QSiegel bietet deshalb für den Rechtsverkehr mehr Rechtssicherheit, weil diese Exkulpation

28 Vgl.: Roßnagel, Alexander/Fischer-Dieskau, Stefanie/Jandt, Silke/Knopp, Michael: Langfristige Aufbewahrung elektronischer Dokumente. In: Der elektronische Rechtsverkehr. Band 17. 2007. S. 69 ff.

im Außenverhältnis für eine juristische Person schwieriger ist. Der Verbraucher oder der andere Teil nutzt entweder eine QES und ist deshalb als Gläubiger identifizierbar oder nutzt ebenfalls das QSiegel und ist als Gläubiger ohnehin Anspruchsteller, der für sich die Fiktion des § 184 Abs. 1 BGB in Anspruch nehmen kann. Demnach wirken nachträglich genehmigte Rechtsgeschäfte auf den Zeitpunkt der Vornahme des Rechtsgeschäfts zurück und das Fehlen der Vertretungsmacht ist kein Problem mehr.

Dies ist an einem Beispiel leicht nachvollziehbar: Ein Unternehmen setzt ein QSiegel ein, um einen Vertragsschluss auf eigener Seite zu tätigen oder Informationspflichten gegenüber dem Kunden zu erfüllen. In einer juristisch gestörten Rechtsbeziehung kann sich der Kunde oder andere Teil darauf berufen, dass das QSiegel von dem Unternehmen ist und dieses aus der Rechtsbeziehung haftet (etwa wenn der Kunde die Darlehensvaluta ausgezahlt bekommen möchte oder die Informationspflichten nicht erfüllt wurden und er deshalb den Vertrag später widerrufen möchte). In einem Zivilprozess darüber muss nun jede Partei die für sie günstigen Tatsachen beweisen, es sei denn, es gilt eine oben dargestellte Beweislastregelung, die etwas anderes bestimmt, etwa eine Beweislastumkehr, eine Vermutung oder der Anscheinsbeweis. Der Einsatz des QSiegels führt dazu, dass mindestens der Anscheinsbeweis für die Herkunft der Erklärung von dem Unternehmen greift. Das Unternehmen kann nun nicht einfach behaupten, das QSiegel wurde nicht von ihm genutzt, sondern von einer unbefugten dritten Person (wie bei einer QES). Für die Tatsache, dass die Erklärung von dem Unternehmen kam, kann der Kunde den Anscheinsbeweis für sich in Anspruch nehmen und muss sie nicht mit einer Urkunde, einem Zeugen, einem Gutachten oder durch Inaugenscheinnahme beweisen. Das Unternehmen muss nun durch die besondere Beweisregel des Anscheinsbeweises selbst vortragen, wie es anders gekommen sein kann, und die entsprechenden Anknüpfungstatsachen beweisen. Es muss also erklären, wie das QSiegel von einer unbefugten Person genutzt werden konnte, und beweisen, dass dies auch abstrakt funktionieren kann. Denkbar wäre etwa, dass der ehemalige Mitarbeiter die Siegeldaten mitnehmen und ein QSiegel für das Unternehmen auslösen konnte. Das Unternehmen muss dann beweisen, dass eine Fernsiegelung mit Zwei-Faktor-Authentisierung mit den Unternehmensdaten überhaupt möglich ist (wobei hier eine Haftung wegen Fahrlässigkeit im Umgang mit den QSiegel-Daten ebenfalls denkbar wäre). Dieser Beweis wird sehr schwerfallen, weil die Sicherheitsanforderungen an die Nutzung des QSiegels sehr hoch sind. Es führt also zu einem ähnlichen Beweisdilemma wie die derzeitige Signaturlösung oder das Stellvertretungsregime bei papiergebundener Kommunikation. Der einzige Unterschied ist, dass die Beweislastregeln hier zugunsten des Erklärungsempfängers ausgelegt werden. Das Beweisinteresse wird also besser verteilt. Das Unternehmen muss bei ehemaligen Mitarbeitern beweisen, dass es möglich war, Briefpapier oder Vorlagen nach Ablauf des Beschäftigungsverhältnisses zu nutzen. Sollte das Unternehmen keinen Rechtsschein gesetzt haben, also etwa die Person gar nicht beim Unternehmen gearbeitet haben, verpufft die Schutzwirkung des Anscheinsbeweises, und der Anspruchsteller muss selbst beweisen, dass die Erklärung von dem Unternehmen kam.



Die Beweisinteressen der QES und des QSiegels

Vergleicht man dies mit der QES der Erklärung, kommt man zu einem weniger zweckmäßigen Ergebnis. Hier gilt die gesetzliche Vermutung, dass die Erklärung von der darin angegebenen Person stammt. Jedoch muss der Kunde in dem Beispiel beweisen, dass der Erklärende vertretungsbefugt war oder das Unternehmen diesen lange für es hat handeln lassen und damit den Rechtsschein gesetzt hat. Dies ist ein unbilliges Ergebnis.

Auch kann jede juristische Person bzw. öffentliche Behörde den Einsatz der QSiegel-Daten selbst so protokollieren, dass sie nachvollziehen kann, wer welche Erklärung wann gesiegelt hat. Dies ist ebenfalls dem Beweis zugänglich. Wenn diese Möglichkeiten nicht genutzt werden, etwa aus Kostengründen, ist dies Sache des Siegel-Erstellers. Nach deutschem Recht wird niemand gezwungen, Beweise selbst zu sichern, wenn er dies nicht will. Die Entscheidung der Risikotragung in einem Gerichtsverfahren ist wirtschaftlich zu treffen und kann je nach Schadenshöhe auch akzeptiert werden. Transaktionen im Wert von wenigen Euro muss ein Unternehmen nicht protokollieren, wenn klar ist, dass die Beweise niemals in einem Verfahren benötigt werden.

Für die öffentliche Hand ergibt sich noch ein weiterer Umstand. Hier ist eine Durchgriffshaftung für hoheitliche Handlungen des einzelnen Beamten für den Bürger weitgehend ausgeschlossen. Art. 34 Satz 1 GG sieht für die Staatshaftung ohnehin keine Haftung des Einzelnen vor. Hier besteht also kein Interesse für den Erklärungsempfänger, die sichere Identität des individuell Erklärenden zu erfahren, sondern die Herkunft der Erklärung dem Staat zuzuordnen. Das QSiegel leistet diese sichere rechtliche Zuordnung. Die bisherige QES verweist hingegen nur auf die handelnde Person.

Im Ergebnis stellt das QSiegel, weil es zur Einhaltung bestimmter technischer Verfahren zwingt, eine höhere Sicherheit dar und schützt den Rechtskreis besser, weil derjenige, der ein Interesse an der bestimmbaren Herkunft einer Erklärung hat, durch den Anscheinsbeweis besser geschützt ist. Alle Konstruktionen der Vertretungsbefugniskette juristischer Personen dienen am Ende diesem Schutz des Rechtsverkehrs (Publizität des Handelsregisters, Unterbevollmächtigung im Unternehmen und die Rechtsscheinsvollmacht). Durch die Vertrauensdienste der eIDAS-Verordnung ist der Umweg erstmals nicht mehr notwendig. Durch sie wird es möglich, die Herkunft automatisiert im QSiegel zu hinterlegen, abzufragen, zu prüfen und im Prozess zu nutzen.

Im Ergebnis lässt sich feststellen, dass immer dann, wenn eine Handlung von juristischen Personen digital erfolgt, eine Regelungslücke besteht, weil nur für natürliche Personen mit der QES eine Anknüpfung von der physischen Handlung zur digitalen Äußerung gesetzlich geregelt ist. Das QSiegel bietet jedoch die Möglichkeit, diese Lücke gesetzlich zu schließen.

4 AKTUELLER HANDLUNGS- UND REGELUNGSBEDARF

Die bestehenden Regelungen sollten dort erweitert werden, wo bestimmte eIDAS-Werkzeuge nicht implementiert wurden und wo lediglich die Lücke zwischen altem SigG und neuem europäischen Binnenmarkt geschlossen werden muss. Neue Gesetze sollten dort geschaffen werden, wo digitale Prozesse noch nicht mitgedacht wurden. Zudem braucht es ein neues Verständnis von Formerfordernissen, wenn alle Verträge und Rechtsverhältnisse eine digitale Komponente haben. Dies hat die Bundesrepublik in der Tallinn Declaration on eGovernment 2017 für die eIDAS-Werkzeuge zugesagt und sollte mit den nachfolgenden Maßnahmen umgesetzt werden.

Ministerial Declaration on eGovernment – the Tallinn Declaration

(...) The Member States reaffirmed their commitment to progress in linking up their public eServices and implement the eIDAS regulation and the once-only principle in order to provide efficient and secure digital public services that will make citizens and businesses lives easier.

4.1 Die Vertrauensfunktion im elektronischen Rechtsverkehr

Wenn Verbraucher von zu langen Vertragstexten und Lizenzbedingungen überfordert sind und sie ungelesen unterschreiben, kann die Schriftform ihre Warnfunktion nicht mehr angemessen erfüllen. Gerade in digitalen Geschäftsprozessen wäre eine neue Art der Warnfunktion sinnvoll. Die könnte so aussehen, dass Unternehmen ihre Vertragsvorlage mit einem QSiegel versehen und der Verbraucher diese mit einer eigenen elektronischen Unterschrift zeichnen muss. So kann der Verbraucher direkt überprüfen, ob der Vertrag oder das Informationsblatt tatsächlich von dem ausstellenden Unternehmen stammt. Durch die eigene Signatur (und sei es nur die Fernsignatur mit PIN und Smartphone) kann der Verbraucher erkennen, dass sein eigenes Handeln rechtserheblich ist.

Außerdem sollte eine stärkere Verbindung von digitalem Handeln zu den tatsächlichen Auswirkungen in die physische Welt hergestellt werden. Denn Rechtsräume erstrecken sich hier auf neue Handlungsebenen. Um eine rechtssichere Verbindung der Ebenen zu ermöglichen, müssen die Identitäten aus der physischen Ebene in die digitale Ebene übersetzt werden. Diese Brücke von der digitalen in die physische Welt soll das notwendige Vertrauen in die Herkunft der Handlung schaffen. Dies ist eine Funktion, die nicht im Kanon der Funktionen der Formvorschriften vorhanden ist. Zwar gab es sogenannte Geschäfte unter Abwesenden, die durch die Schriftform zum Beispiel über große Entfernungen möglich waren. Sie blieben aber immer in der physischen Ebene. Der Empfänger konnte den Unterzeichner stets am Schriftbild oder am Druck auf das Papier identifizieren. Es gab also eine physische Verbindung von Erklärung und Form. Zwischen Tastendruck und Schriftzeichendarstellung oder der in eine App gesprochenen Sprache und der digitalen Textausgabe in der Diktierfunktion hingegen gibt es keine physische Verbindung mehr. Daten können verändert werden und verlieren jeden Bezug zum Ursprung.

Die Vertrauensfunktion

Die Brücke von der digitalen in die physische Welt kann nun durch die Vertrauensdienste der eIDAS-Verordnung geschaffen werden. Diese Brücke ist die Vertrauensfunktion, die als neues Element im deutschen Recht zu etablieren ist. Dabei handelt es sich um eine neue Funktion für Formvorschriften von Rechtsgeschäften. Anders als bei der Identitäts-, Echtheits- und Verifikationsfunktion innerhalb der bereits anerkannten Klarstellungs- und Beweisfunktion kommt die Vertrauensfunktion für die Verbindung von Physischem und Digitalem hinzu, wenn es darum geht, den Urheber zu identifizieren und zu prüfen, ob die Erklärung echt ist. Sie schafft damit Vertrauen in die Herkunft einer Handlung.

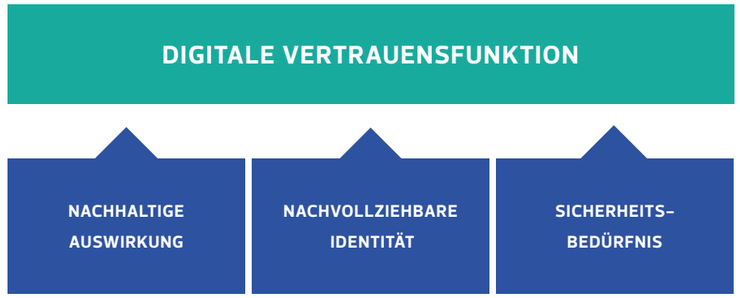
Wo müssen wir sicher sein, dass alle Beteiligten die sind, für die sie sich ausgeben?

Der Gesetzgeber muss sich dafür die Frage stellen, welche Rechtsgeschäfte und welche E-Government-Prozesse auf besonderem Vertrauen basieren und deshalb einer Absicherung durch die Vertrauensfunktion bedürfen. Die identifizierten Prozesse müssen mit geeigneten Mitteln abgesichert werden. Für alle Prozesse, die europäische Mitgliedstaaten oder EU-Ausländer betreffen, eignen sich die Vertrauensdienste der eIDAS-Verordnung.

Bei rein deutschen Sachverhalten könnten auch andere Methoden gewählt werden. Dies würde aber zu Doppelstandards mit deutlich erhöhten Kosten führen. Der entscheidende Vorteil der Interoperabilität bei europaweit einheitlichen Standards würde aufgegeben und eine Nutzung bestehender Systeme könnte nicht dynamisch erweitert werden.

Drei Merkmale bilden die Grundlage für die neue Vertrauensfunktion:

1. Die Vertrauensfunktion muss immer dann gegeben sein, wenn es sich um digitale Geschäfts- oder Verwaltungsprozesse handelt, die sich in der physischen Welt nachhaltig auswirken.
2. Die Vertrauensfunktion muss immer dann gegeben sein, wenn es um die Nachvollziehbarkeit der Identität der Beteiligten geht.
3. Die Vertrauensfunktion muss immer dann gegeben sein, wenn ein erhöhtes Maß an Sicherheit gewährleistet werden soll. Sicherheit beschreibt die Schutzziele Verfügbarkeit, Integrität und Vertraulichkeit des Geschäfts- oder Verwaltungsprozesses.



Die Merkmale der digitalen Vertrauensfunktion

Beispiel „digitaler Meldeprozess“

Ein anschauliches Beispiel für die digitale Vertrauensfunktion wäre wiederum die Ummeldung des Wohnsitzes nach den Meldegesetzen in Berlin.

Die digitale Ummeldung hat insofern Auswirkungen in der physischen Welt, als es eine neue Wohnanschrift gibt, an die beispielsweise Dokumente wie Wahlunterlagen, Steuerbescheide oder Verwaltungsakte geschickt werden. Zudem wird die Ummeldung von einer echten Person vorgenommen, der echte Vermieter bestätigt die Wohnnutzung und die echte Behörde stellt eine Meldebestätigung aus. Die Identität der Beteiligten muss also beweisbar sein. Des Weiteren ist bedeutend, dass die Kommunikation abgesichert wird, da personenbezogene Daten übertragen werden. Ein unberechtigtes Eingreifen von außen birgt zudem die Gefahr, dass eine Meldebescheinigung erschlichen werden könnte. Auch für die Behörde ist wesentlich, dass die vom Bürger beigefügten Dokumente keine Schadsoftware beinhalten. Der Vorgang selbst muss langzeitarchiviert werden, um nachvollziehbar zu bleiben. Es besteht also ein erhöhtes Sicherheitsbedürfnis für den Kommunikationsprozess.

Das wäre beispielsweise bei der Online-Reservierung einer Theaterkarte anders. Wenn man nicht rechtzeitig erscheint, verfällt die Reservierung und der Sitzplatz wird anderweitig vergeben. Der Vorgang hat keine Auswirkungen in der physischen Welt und die Identität des Besuchers ist für das Theater auch nicht von Belang. Es werden keine personenbezogenen Daten gespeichert oder Dateien ausgetauscht, die lange prüfbar sein müssen.

Zurück zum Ummelde-Beispiel. Der Vertrauensraum für den digitalen Meldeprozess sähe folgendermaßen aus: Der Bürger stellt seinen Antrag und unterzeichnet ihn mit einer fälschungssicheren QES. Die Kommunikation über das Internet wäre mit QWACs abgesichert. Der Vermieter könnte die Bestätigung mit der QES oder bei Wohnungsgesellschaften mit dem QSiegel versehen. Die Behörde würde den Meldevorgang automatisiert verarbeiten und die Meldebescheinigung mit ihrem QSiegel versehen. Über De-Mail oder andere elektronische Einschreib- und Zustelldienste könnte die Meldebescheinigung sicher zugestellt werden. Alternativ wäre es denkbar, dass der Bürger sie von einer Website, die mit einem QWAC abgesichert ist, mit seiner QES herunterlädt. Auch berechtigte Dritte könnten mit eigenen Signaturen diese Prozesse auslösen. Diese Dritten könnten auch im EU-Ausland sitzen, da die eIDAS-Vertrauensinfrastruktur europaweit einheitlich funktioniert.

Ein solcher Vertrauensraum wäre auch in anderen Fällen denkbar. So könnten Gefängnisse Insassen ummelden oder Flüchtlingsunterkünfte oder Pflegeeinrichtungen Bewohner melden. Denkbar wäre auch ein Melde- und Vermittlungssystem für freie Kindergartenplätze.

4.2 Beispiele für Regelungslücken beim Einsatz von Vertrauensdiensten

Durch die Vertrauensfunktion ergeben sich enorme Einsparungspotenziale. Schon das genannte Ummelde-Beispiel zeigt, wie ein digitaler Prozess Ressourcen der öffentlichen Hand einspart, Vertrauen ins eigene Handeln schafft und äußerst effizient ist. Die Behörde wird entlastet und der Bürger kann seine Wohnung zeitnah anmelden. Das Einsparungspotenzial gilt insbesondere auch für die Wirtschaft. Schließlich müssen Unternehmen sehr viel häufiger in Kontakt mit Behörden treten als Bürger. So kann eine digitale Verwaltung einen großen Beitrag dazu leisten, die Wettbewerbsfähigkeit deutscher Unternehmen zu verbessern. Dafür muss die Verwaltung ihre wichtigsten Dienste digital anbieten. Dieser Prozess läuft derzeit: Laut dem Online-Zugangsgesetz (OZG) müssen 575 Verwaltungsdienstleistungen bis zum Jahr 2022 online angeboten werden.

Grundsätzlich ist zu beachten: Einzellösungen, wie etwa beim besonderen elektronischen Anwaltspostfach, lohnen sich nicht. Verschiedene Standards, geschlossene Benutzersysteme und beschränkte Anwendungsfälle führen nicht dazu, dass ausbaufähige Lösungen entstehen und Aufwand gespart wird. So sind beim Anwaltspostfach nicht nur Anwälte und Gerichte mögliche Kommunikationspartner, sondern auch professionelle Verfahrensbeteiligte wie Behörden, Notare, Gerichtsvollzieher, Steuerberater, Sachverständige, Verfahrensbeistände, Jugendämter und Berufsbetreuer, Zeugen oder Arbeitgeber. Darüber hinaus braucht es eine

länderüberschreitende Kommunikation. Eine solche Kommunikation sollte deshalb alle Gruppen einschließen und eine medienbruchfreie Schnittstelle zu allen Beteiligten ermöglichen.

4.2.1 Digitale Kommunikation in der Justiz

Würden Gerichte und Behörden bei ihrem elektronischen Rechtsverkehr das QSiegel einführen, käme es zu deutlichen finanziellen und personellen Entlastungen. Die Fälle könnten schneller bearbeitet und abgeschlossen werden.

Allein die physische Zustellung beglaubigter elektronischer Abschriften kann zwei bis drei Wochen dauern. Würden sie digital zugestellt, könnten Papier, Druckertinte, Arbeitszeit und Zeit im Gerichtsverfahren gespart werden. Das QSiegel kann so in den Versendungsprozess eingebaut werden, dass nur Berechtigte darauf zugreifen können. Dies könnte beispielsweise per Fernsiegelung in einem zentralen Cloud-Service ausgelöst werden. So kann das Gerichtspersonal die Dokumente innerhalb weniger Sekunden zustellen. An den Gerichten für Zivil- und Familiensachen in Nordrhein-Westfalen kam es im Jahr 2015 im Rahmen der Verfahren zu 3.103.752 Zustellungen (acht Zustellungen pro von Rechtsanwälten geführtem Verfahren). Legt man diese Zahlen zugrunde, ergäbe das bei einer automatisierten elektronischen Siegelung allein im Servicebereich 646 ersparte Arbeitstage à acht Stunden.[29]

Ein weiterer Vorteil des QSiegels gegenüber der QES ist, dass das QSiegel einem Gericht rechtssicher zugeordnet werden kann. Und zwar ohne dass der Empfänger nachvollziehen muss, ob die Person, die die Signatur ausgestellt hat, tatsächlich bei diesem Gericht arbeitet und zuständig war. Im europäischen Kontext können Gerichtsentscheidungen ebenfalls rechtssicher zugestellt werden und Entscheidungen nach dem Übereinkommen über die gerichtliche Zuständigkeit und die Vollstreckung gerichtlicher Entscheidungen in Zivil- und Handelssachen unkomplizierter durchgeführt werden.

Das QSiegel kann vielfältig eingesetzt werden. Und zwar dort, wo es bisher nicht auf die gesetzliche Schriftform ankommt. Ideal ist es dann zu nutzen, wenn entscheidend ist, dass der Ersteller einer Organisation oder Behörde zugeordnet werden kann. Dies entspricht dem Rechtsgedanken des § 169 Abs. 3 ZPO, der die maschinelle Beglaubigung zulässt. Es kann nicht eingesetzt werden, wenn ein persönliches Signaturerfordernis vorliegt, etwa wenn ein Richter Urteile und Beschlüsse unterzeichnet.[30]

2018 wurde für die Kommunikation von Anwälten untereinander oder mit Gerichten das besondere elektronische Anwaltspostfach eingeführt. Diese Insellösung hat allerdings Nachteile für eine zukunftssichere Kommunikation: Dritte Akteure und Schnittstellen nach außen können nicht eingebunden werden. Sobald Nachrichten, Dokumente oder Dateien aus dem System in ein anderes überführt werden müssen (intersektorale Kommunikation), gehen die Vorteile des geschlossenen Systems und damit insbesondere Authentizität und Integrität verloren. Dabei gibt es – wie oben dargestellt – eine ganze Reihe möglicher Emp-

29 Seiffge, Jennifer/Henke, Eva-Maria: Zeitersparnis, Entbürokratisierung, Optimierung. e-Justice Ausgabe 01/2017. S. 13, aufgerufen am 01.02.2019 unter *https://www.e-justice-magazin.de/2017/06/28/zeitersparnis-entbuerokratisierung-optimierung/.*

30 Vgl.: Hölters, Jennifer/Henke, Eva Maria: Verwendungsmöglichkeiten und Nutzen des qualifizierten elektronischen Siegels. In: Internet-Zeitschrift für Rechtsinformatik und Informationsrecht. JurPC Web-Dok. 44/2017, Abs. 19, aufgerufen am 01.02.2019 unter *https://bit.ly/2YSZ8jp.*

fänger der jeweiligen Dokumente, zu denen professionelle Verfahrensbeteiligte, Behörden, Notare, Berufsbetreuer, Zeugen, Arbeitgeber oder der Mandant gehören.

Bei der Justiz-Kommunikation sind die drei Merkmale für die Vertrauensfunktion vorhanden:

1. Die physische Auswirkung bezieht sich auf tatsächliche Verfahrenshandlungen.
2. Die Identität der Empfänger und Absender ist wesentlich zur Sicherstellung der beruflichen Verschwiegenheitspflicht.
3. Ein erhöhtes Maß an Sicherheit muss gewährleistet sein. Die Dokumente müssen manipulationssicher sein.

Sinnvoll wäre – wie beim Beispiel des Meldeprozesses beschrieben –, die Werkzeuge der eIDAS-Verordnung für die Kommunikation aller Beteiligten zu ermöglichen. Dazu zählen die QES oder ein QSiegel für Behörden und juristische Personen. Als Kommunikationsinfrastruktur könnten Websites mit QWACs oder elektronische Einschreib- und Zustelldienste (zum Beispiel De-Mail) genutzt werden.

Dafür müssen die jeweiligen Fachgesetze (BRAO, GVG, BOStB, VwVfG, VwGO) hinreichend geändert werden. Es müsste festgehalten werden, dass der Verpflichtung zur berufsrechtlichen Verschwiegenheit Genüge getan ist, wenn Verschlüsselungstechnologien nach neuestem Stand der Technik genutzt werden. Zudem wäre zu regeln, dass die digitale Offenbarung von vertraulichen Informationen nur dann zulässig ist, wenn alle Beteiligten zuverlässig identifiziert werden können. Die Identifizierung der Beteiligten ist sichergestellt, wenn QES, QSiegel, die Online-Ausweisfunktion des elektronischen Personalausweises oder De-Mail verwendet werden.

4.2.2 Digitale Kommunikation in der Behörde

Mit QSiegeln können deutlich mehr behördliche Bescheide verschickt werden. Besonders bei Massenverfahren wie Steuer- oder Rentenbescheiden ergibt sich großes Einsparungspotenzial.

Behörden nutzen für viele Schreiben, die mit der Post herkömmlich versendet werden, folgenden Textbaustein: „Dieses Schreiben wurde maschinell erstellt und ist daher ohne Unterschrift gültig." Dies ergibt sich aus § 37 Abs. 5 Satz 1 VwVfG, in dem die schriftliche, mündliche oder elektronische Form für Verwaltungsakte definiert wird und damit die Namenswiedergabe und Unterschrift in einem automatisierten Verfahren verzichtbar wird. Vor diesem Hintergrund können mit einem QSiegel auf digitalem Wege sehr viel mehr behördliche Bescheide verschickt werden als bisher, weil Papier, Kosten und vor allem Zeit gespart wird. Bei Verwaltungsakten ist maßgeblich, dass die ausstellende Behörde zu erkennen ist (§ 44 Abs. 2 Nr. 1 VwVfG). Kurioserweise darf bei Schreiben auf einfach zu fälschendem Recyclingpapier dieser Textbaustein verwendet werden – nicht aber bei den deutlich sichereren elektronisch gesiegelten Dokumenten.

Das E-Government-Gesetz (EGovG) ist am 1. August 2013 in Kraft getreten und soll die Verbreitung elektronischer Verwaltungsdienstleistungen fördern. Vorher bestand ein wesentliches Hindernis für E-Government-Angebote der öffentlichen Verwaltung darin, dass als elektronisches Äquivalent der Schriftform allein die QES zugelassen war und diese keine hinreichende Verbreitung hat. Mit dem EGovG wurden daher neben der QES auch De-Mail und die Online-Ausweisfunktion (eID-Funktion) zum Beispiel des elektronischen Personalausweises als weitere sichere Technologien zugelassen, um die Schriftform im Verwaltungsverfahren elektronisch zu ersetzen. Außerdem erlaubt eine Rechtsverordnungsermächtigung der Bundesregierung mit Zustimmung des Bundesrats die rasche Anpassung an die deutschland- und europaweite technologische Weiterentwicklung (§ 3a Abs. 2 Satz 4 Nr. 4 VwVfG). Mit der Rechtsverordnung können weitere ausreichend sichere Verfahren als Schriftformersatz festgelegt werden.

An dieser Stelle muss auch das QSiegel verankert werden. Es erfüllt technisch das gleiche Sicherheitsniveau wie die QES. Zudem braucht es heute schon nicht zwingend die persönliche Unterschrift des gesetzlichen Vertreters bei Verwaltungsverfahren. Sie kann durch eine Vollmacht erteilt werden. Das QSiegel unterstellt diese Vollmacht nach §§ 164 Abs. 1 Satz 2, 167 Abs. 1 2. Alt. BGB oder nach den Grundsätzen der Rechtsscheinsvollmacht in Verbindung mit Art. 35 eIDAS-Verordnung. Denn eine Erklärung, die nach den Umständen gegenüber dem Dritten abgegeben wird, muss der Vertretene – hier der Siegel-Verwender – gegen sich gelten lassen. Das ist damit vergleichbar, dass ein Unternehmen Briefpapier und Firmenstempel in die Hände der Angestellten gibt. Eine damit abgegebene Erklärung muss das Unternehmen ebenfalls gegen sich gelten lassen. Das QSiegel bietet indes deutlich höhere Sicherheit als ein Firmenstempel, der schnell entwendet werden kann. Die oben genannten Authentisierungsmethoden gelten übrigens nur für natürliche Personen. Juristische Personen können sich nicht mit Online-Ausweisfunktion, QES oder De-Mail rechtssicher ausweisen. Unternehmen oder auch Vereine bedürfen einer zuverlässigen Authentisierungsmethode mit dem QSiegel. Deshalb muss – gesetzlich oder in der Rechtsverordnung der Bundesregierung nach § 3a Abs. 2 Satz 4 Nr. 4 VwVfG – verankert werden, dass das QSiegel juristische Personen ausreichend identifiziert und dass Behörden es nutzen können.

Öffentliche Verwaltungen können schon jetzt die Fernsignatur für alle Prozesse nutzen, bei denen die Unterschrift des Antragstellers gesetzlich gefordert ist. Dazu gehören zum Beispiel Förderanträge, Baugenehmigungen, Abfallbegleitscheine sowie Dokumentationen zum Erwerb von Zertifikaten im Emissionshandel.[31]

QSiegel stellen nicht nur den Ursprung, sondern auch die Unversehrtheit von elektronischen Daten – ein wichtiges Merkmal amtlicher Beglaubigungen – sicher. Deswegen können sie dafür verwendet werden, Urkunden jeglicher Art (Geburts-, Heirats- und Sterbeurkunden) und Zeugnisse elektronisch zuzustellen. Sie eignen sich auch für rechtswirksame öffentliche Bekanntmachungen im Internet, die gegen Löschung und Verfälschung geschützt werden müssen. Zudem sieht das eIDAS-Durchführungsgesetz ausdrücklich vor, dass QSiegel in Vergabeverfahren öffentlicher Verwaltungen neben der QES zugelassen sind.[32]

31 Bundesdruckerei-Whitepaper: Durchgängig digital – mit Fernsignatur und elektronischem Siegel. S. 12, aufgerufen am 01.02.2019 unter *https://www.bundesdruckerei.de/de/Whitepaper-Fernsignatur-und-elektronisches-Siegel.*

32 Bundesdruckerei-Whitepaper: Durchgängig digital – mit Fernsignatur und elektronischem Siegel. S. 16, aufgerufen am 01.02.2019 unter *https://www.bundesdruckerei.de/de/Whitepaper-Fernsignatur-und-elektronisches-Siegel.*

4.2.3 Digitale Kommunikation im Gesundheitswesen

eIDAS-Vertrauensdienste ermöglichen verkehrsfähige Dokumente für die intersektorale Kommunikation im Gesundheitsbereich. Die Nutzung der Vertrauensdienste spart bürokratischen Aufwand und gewährleistet einen effizienten und sicheren Umgang mit Informationen über Behandlungen und Patienten. Damit kann die Versorgung der Patienten enorm verbessert werden.

Das Gesundheitswesen weist ein besonders hohes Potenzial für Arbeitserleichterungen durch digitale Prozesse auf. Der bürokratische Dokumentationsaufwand kann weitestgehend automatisiert und Informationen über Behandlungen und Patienten können effizienter genutzt werden. Diese Prozesse müssen rechtssicher und technisch einwandfrei gestaltet werden. Die Vertrauensdienste der eIDAS-Verordnung machen das europaweit möglich.

Das QSiegel könnte beispielsweise beim Entlassbrief sinnvoll eingesetzt werden. Denn im Außenverhältnis haftet nicht zwingend der Arzt, sondern das Krankenhaus. Das gilt auch für Fachärzte, Labore und medizinische Versorgungszentren: Laborberichte und Fachuntersuchungsergebnisse könnten automatisiert mit dem QSiegel statt wie bisher mit Arztunterschrift versehen werden. Dies muss gesetzlich verankert werden. Die heutige Lösung mit lokaler Signaturkarte ist vielen Häusern zu kompliziert. Entlassbriefe müssen aber auf jedem Gerät von dem zuständigen Arzt ausgestellt und anschließend mobil versendet werden können.

Pflegedienste haben erhebliche Dokumentationspflichten, um ihre Leistungen abrechnen zu können. Die Dokumentation könnte digital auf mobilen Endgeräten erfolgen und automatisiert gesiegelt werden – sofern es keiner persönlichen Unterschrift bzw. QES bedarf. Das geht deutlich schneller und das Pflegepersonal hätte mehr Zeit für die Patientenversorgung. Daher müsste die gesetzliche Voraussetzung geschaffen werden, alle Dokumente, die einen qualifizierten Nachweis der versendenden Institution benötigen und bisher per Papier versandt wurden, auch elektronisch mit QSiegel zur Verfügung stellen zu dürfen.

Ein automatisiertes elektronisches Siegelverfahren bietet sich immer dort an, wo es darauf ankommt, den Vorgang und nicht die persönliche Verantwortlichkeit zu dokumentieren. Darunter könnten möglicherweise Mitteilungen für ambulante Versorgungsleistungen sowie Mitteilungen an und von Kammern, kassenärztlichen Vereinigungen sowie Kostenträgern fallen. Damit das QSiegel interoperabel genutzt werden kann, muss zudem eine asynchrone, elektronische Kommunikation auf Basis der Spezifikationen für elektronische Einschreib- und Zustelldienste gesetzlich verankert werden. Mit sogenannten zertifizierten Gateways können diese Dienste in und aus einem sicheren Netzwerk verwendet werden. Dies ermöglicht eine gesicherte Kommunikation, zum Beispiel mit Patienten, Betreuern oder Rechtsanwälten.

Ein Trend geht dahin, dass die Kommunikation in Netzwerken, etwa Fachanwendungen von den Ärzten, des medizinischen Diensts oder von Laboren, automatisiert abläuft. Dann stößt nicht mehr der Mensch den Austausch von Informationen an, sondern das Laborsystem kann direkt das Patienteninformationssystem des Arztes kontaktieren und notwendige Patientendaten übermitteln. Diese Art der Kommunikation sollte durch QWACs abgesichert werden. So können Berechtigte untereinander vertraulich kommunizieren. Dafür nutzen die jeweiligen IT-Systeme eindeutige Identitäten, um sich auszuweisen. Alle Kommunikationspartner können verbindlich prüfen, mit wem sie letztendlich kommunizieren. Nichtberechtigte können keine Kommunikation aufbauen. Die eingesetzte Technologie ist nicht proprietär, sondern kann europaweit von einem beliebigen Vertrauensdiensteanbieter bezogen werden.

4.2.4 Zeugnisse und Bescheinigungen

Dokumente wie Führungs-, Ausbildungs- oder Arbeitszeugnisse sowie Diplome und Meisterbriefe werden durch die eIDAS-Vertrauensdienste fälschungssicher. Dadurch steigt das Vertrauen in die digitale Welt.

Häufig werden bei Bewerbungen gefälschte Zeugnisse vorgelegt. So gibt es gar Portale, bei denen gegen Bezahlung ein Zeugnis nach Wahl bestellt werden kann.[33] Weil das Zeugnis einen Nachweis führt, der beispielsweise zu einer Anstellung verhelfen kann, besteht ein unmittelbarer Zusammenhang zwischen analoger und digitaler Welt. Unternehmen oder andere Organisationen, denen ein Zeugnis vorgelegt wird, wollen sicher sein, dass die Identität des Zeugnisausstellers und -empfängers echt ist und dass das Zeugnis nicht gefälscht wurde. Die eIDAS-Vertrauensdienste können hierfür sehr sinnvoll eingesetzt werden.

Der Regelungsinhalt ist folgender: Digitale Zeugnisse und Bescheinigungen, die im Rechtsverkehr genutzt werden, müssen den Aussteller mit hinreichender Sicherheit identifizierbar machen. Diese Sicherheit kann dadurch gewährleistet werden, dass die Dienste stets auf dem neuesten Stand der Technik sind. Die Sicherheitsanforderungen können durch die QES des Unterzeichners oder das QSiegel des ausstellenden Rechtsträgers gewährleistet werden. Durch die eIDAS-Vertrauensinfrastruktur wäre automatisiert europaweit prüfbar, ob das Zeugnis echt ist. Eigene Echtheitsrecherchen beim jeweiligen Aussteller entfallen.[34] Dieser Regelungsinhalt kann entweder an zentraler Stelle oder in allen entsprechenden Normen für die jeweiligen Aussteller verankert werden. Hier würden sich das BGB und das Verwaltungsverfahrensgesetz (VwVfG) anbieten, da sowohl für den zivilrechtlichen Bereich als auch für den öffentlichen Bereich eine allgemeingültige Regelung getroffen werden kann.

33 Vgl.: Floren, Annette/Entschew, Enrico/Fiedler, Arno: Sichere (elektronische) Dokumente. Neue Rahmenbedingungen durch die europäische eIDAS-Verordnung. White Paper des Forums elektronische Vertrauensdienste. S.7.

34 Diese werden heute vielfach datenschutzrechtswidrig durchgeführt.

4.2.5 Beglaubigung von Abschriften durch Behörden

Das QSiegel kann für die Beglaubigung von Abschriften durch Behörden eingesetzt werden. Durch den elektronischen Prozess erübrigt sich der Gang zur Behörde.

Zu den besonders intensiv nachgefragten Behördendienstleistungen zählt die Beglaubigung von Dokumenten. Es geht darum, von einem schon existierenden amtlichen Dokument, zum Beispiel einem Zeugnis oder einer Geburtsurkunde, eine Abschrift zu erstellen. Das Dokument darf aber nicht einfach kopiert werden, sondern es bedarf des verbindlichen Nachweises, dass die Zweitschrift mit dem Original übereinstimmt. Solche amtlichen Beglaubigungen können Behörden vornehmen – sowohl für Urkunden, die sie selbst ausgestellt haben, als auch für Urkunden, die von anderen Stellen stammen. Im digitalen Zeitalter werden solche Beglaubigungen immer häufiger in elektronischer Form nachgefragt.

35 Vgl.: Floren, Annette/Entschew, Enrico/Fiedler, Arno: Sichere (elektronische) Dokumente. Neue Rahmenbedingungen durch die europäische eIDAS-Verordnung. White Paper des Forums elektronische Vertrauensdienste. S.8.

§ 33 Abs. 5 Nr. 2 VwVfG
Beglaubigung elektronischer Dokumente:

Der Beglaubigungsvermerk muss zusätzlich zu den Angaben nach Absatz 3 Satz 2 bei der Beglaubigung eines elektronischen Dokuments den Namen des für die Beglaubigung zuständigen Bediensteten und die Bezeichnung der Behörde, die die Beglaubigung vornimmt, enthalten.

Das ist ein maßgeschneiderter Anwendungsfall für das QSiegel. Er setzt allerdings voraus, dass das VwVfG und das Sozialgesetzbuch dies auch zulassen.[35] Hierzu regelt § 33 Abs. 4 Nr. 4 und Abs. 5 VwVfG lediglich den Einsatz der QES, nicht aber von QSiegeln. Dabei fordert das VwVfG hier genau die Angaben zusätzlich zur Signatur, die in einem QSiegel geprüft vorhanden sind. Bei der Beglaubigung durch die Behörde ist aber für den Rechtsverkehr wichtiger, dass die Identität der Behörde geprüft wurde und nicht die des Mitarbeiters, dessen Name die Signatur enthält. Das Attribut im Zertifikat der Behörde entfaltet keine direkte Rechtswirkung mehr.

4.2.6 Ersetzendes Scannen in Unternehmen und Behörden

Scan-Vorgänge können mithilfe des QSiegels stark vereinfacht werden. Auch große Aktenbestände können effizient und sicher gescannt werden.

Im Zuge der digitalen Transformation überführen Unternehmen und Verwaltungen nach und nach ihre analogen Dokumente in die digitale Welt. Dazu braucht es zwingend einen rechtssicheren Prozess, in dem nachvollziehbar wird, dass das gescannte Dokument das Original ersetzt bzw. bereits gescannte Dokumente den Status des Originals erhalten. Durch den Scan-Vorgang können Lager- und Verwaltungskapazitäten dramatisch eingespart werden. Behörden, Unternehmen, Krankenhäuser, Anwälte, Steuerberater und andere Institutionen wenden deutschlandweit enorme Kosten für die Miete von Archivräumen und für Personal zur Verwaltung des Papierarchivs auf. Viele der Akten müssen 30 Jahre und länger aufbewahrt werden. Ersetzendes Scannen wird durch die eIDAS-Vertrauensdienste – in Verbindung mit der technischen Richtlinie zum rechtssicheren ersetzenden Scannen des Bundesamts für Sicherheit in der Informationstechnik (BSI, TR RESISCAN) – rechtssicher möglich.

Das QSiegel in der TR RESISCAN

Die TR RESISCAN erwähnt das QSiegel in A.AM.IN.H.1: „Mit einer fortgeschrittenen elektronischen Signatur (...) oder einem elektronischen Siegel gemäß Art. 3 Nr. 25 der Verordnung (EU) Nr. 910/2014 kann neben der Integrität auch die Authentizität der entsprechenden Datenobjekte (zum Beispiel Scanprodukt, Transfervermerk) sichergestellt werden."

Lange herrschte die Vorstellung, dass öffentliche Urkunden von Hand eingescannt und einzeln mit der Signaturkarte unterschrieben werden müssen. So regelt es auch § 371b ZPO. Zukunftssicher sind aber nur Prozesse, die es zulassen, große Aktenmengen effizient und automatisiert zu digitalisieren. Und zwar ohne dass ein Mitarbeiter einzeln seine Signaturkarte und PIN vielfach nacheinander eingeben muss. Das QSiegel sollte hier anwendbar werden und diese Dienstleistung auch durch spezialisierte Dritte erlaubt werden, um die ohnehin belastete Justiz und Verwaltung zu schonen.

Das QSiegel darf an dieser Stelle grundsätzlich eingesetzt werden. Das BSI spricht dem QSiegel technisch die Fähigkeit des notwendigen Integritätsschutzes und der Authentizität zu. Auch wenn der europäische Anwendungsvorrang der eIDAS-Verordnung bei einer rein deutschen Lösung nicht greift, bleibt die technische Zulässigkeit der Nutzung des QSiegels erhalten. Zwar darf eine rein deutsche Lösung oder ein geschlossener Benutzerkreis eigene Standards setzen, das QSiegel bleibt trotzdem immer ein legitimes Mittel der Vertrauensdienste. Bisher gibt es keine entgegenstehende deutsche Regelung. Auch das Argument, aus der Verwendung des QSiegels sei ein Rückschluss auf die scannende, natürliche Person nicht möglich, greift hier nicht.

Die TR RESISCAN sieht in 4.2.1 eine Verfahrensdokumentation vor.[36] In der Musterverfahrensdokumentation wird der Dienstleister oder Scannende verpflichtet, die jeweiligen personellen Verantwortlichen zu benennen.[37] Damit ist immer sichergestellt, wer für den Prozess verantwortlich ist. Eine QES bietet damit keinen Vorteil gegenüber dem QSiegel. Im Gegenteil, die QES dürfte sogar zeitintensiver sein, weil hier viele Signaturkarten oder Fernsignatur-Accounts im Vergleich zu wenigen Siegelkarten verwendet werden müssten.

36 Bundesamt für Sicherheit in der Informationstechnik: BSI Technische Richtlinie 03138 – Ersetzendes Scannen. 15.06.2018, aufgerufen am 01.02.2019 unter *https://bit.ly/2M7KrYm.*

37 Bundesamt für Sicherheit in der Informationstechnik: BSI Technische Richtlinie 03138 – Ersetzendes Scannen. 15.06.2018, aufgerufen am 01.02.2019 unter *https://bit.ly/2M7KrYm.*

4.2.7 Cloud-Dienste und -Anwendungen

Es besteht ein öffentliches Interesse an einer sicheren öffentlichen digitalen Infrastruktur. So können Rechenzentren durch die eIDAS-Vertrauensdienste abgesichert oder miteinander vernetzt werden.

Derzeit gibt es keine rechtsverbindlichen Vorgaben für die Nutzung von Cloud-Diensten. Entsprechend werden auch Netzwerkdienste, die Rechenleistung auf Servern in Rechenzentren anbieten, noch nicht reguliert. Gleichwohl hat das BSI verschiedene internationale Standards und deren Zusammenfassung in den BSI-Anforderungskatalog Cloud Computing bzw. Cloud Computing Compliance Controls Catalogue (C5) aufgenommen. Um Cloud-Dienste nutzen zu dürfen, braucht es aber eine regulatorische Ermöglichung: Es bedarf Rahmenbedingungen und Rechtsgrundlagen.

Die Vertrauensdienste ermöglichen eine rechtsverbindliche und sichere Vertrauensinfrastruktur. So kann etwa der Kommunikationskanal von Anwendung und Rechenzentrum durch QWACs nach Art. 45 eIDAS-Verordnung abgesichert werden. Die Identität der Anwendungssoftware selbst oder der Datenbanken sowie der Nutzer kann durch die QES oder ein QSiegel geschützt werden. Mit den technologieoffenen Vertrauensdiensten – und ergänzt durch C5 – kann das Rechenzentrum physisch und elektronisch gesichert und die Qualität der Anwendung erhöht werden.

Auf diese Weise könnten gemeinsame Rechenzentren für eine polizeiliche Massendatenauswertung sicher betrieben werden. In den vergangenen Jahren wurde die Bevölkerung immer mal wieder – etwa nach terroristischen Anschlägen – aufgerufen, private Smartphone-Bilder und -Videos von den Ereignissen bei Behörden einzusenden. Dadurch kommen gigantische Datenmengen und Tausende Stunden Bildmaterial zusammen, die nicht mehr zeitnah durch Polizeibeamte ausgewertet werden können. Hier werden automatisierte Hochleistungsrechner und Spezialsoftware benötigt, die gemeinsam als Cloud-Anwendung betrieben werden können. Diese Systeme dürfen in keinem Fall mit Schadsoftware infiziert werden und es muss sichergestellt sein, dass Unberechtigte nicht auf sie zugreifen können. Hier können Vertrauensdienste das Zugriffsmanagement absichern. So könnten QWACs eine eindeutige Identifizierung von Kommunikationspartnern sowie eine verschlüsselte Verbindung ermöglichen. Mit ihrer Hilfe wäre auch eine sichere Vernetzung verschiedener Rechenzentren möglich.

4.2.8 Technische Überwachung von Tachoständen

Mit den Werkzeugen der eIDAS-Verordnung und der Tachodatenbank können die Kilometerstände von Gebrauchtwagen europaweit erstmals gerichtsfest nachvollzogen werden.

Das letzte Beispiel zu Regelungslücken bei Vertrauensdiensten beschäftigt sich mit dem „liebsten Kind" der Deutschen: dem Auto. Im europäischen Recht gibt es eine Umsetzungsverpflichtung, die Tachostände von Gebrauchtwagen zu überwachen. Die Tachostände sollen in eine europaweite Datenbank eingetragen werden. Damit soll die Laufleistung von Gebrauchtfahrzeugen nachvollziehbar und Betrug durch Manipulation bekämpft werden.[38] Die Einträge könnten ideal mit dem QSiegel abgesichert werden. Dazu muss Art. 16 der Richtlinie 2014/45/EU des Europäischen Parlaments und des Rates vom 03.04.2014 europäisch einheitlich umgesetzt werden.

38 Europäische Union: Änderung der Verordnung Nr. 1014/2010 zur Festlegung eines Verfahrens für die Ermittlung der Korrelationsparameter, die erforderlich sind, um der Änderung des Regelprüfverfahrens Rechnung zu tragen, aufgerufen am 01.02.2019 unter *https://eur-lex.europa.eu/legal-content/DE/TXT/ELI/?eliuri=eli%3Areg_impl%3A2017%3A1153%3Aoj&locale=sl.*

4.3 Vorschläge notwendiger Gesetzesanpassungen

Es gibt zahlreiche Beispiele dafür, wie die Digitalisierung in Deutschland durch fehlende Rechtssicherheit verzögert wird. Wie in dieser Studie dargestellt, gibt es zudem einige deutsche Gesetze, bei denen die digitale Dimension noch gar nicht mitgedacht wurde. Wie man es bei neuen Regelungen besser macht, zeigt die zweite Payment Services Directive (PSD2) der EU. Hier wurde die Digitalisierung im Gesetzgebungsverfahren gleich mit berücksichtigt.

Das Positivbeispiel Payment Services Directive 2 (PSD2)

Mit der PSD2 wird der Online-Zahlungsverkehr zwischen Marktteilnehmern innerhalb der EU geregelt. Die PSD2 verpflichtet unter anderem Banken mit Geschäftstätigkeit in der Europäischen Union, Drittanbietern Zugang zu Kundenkonten zu gewähren. Damit die Drittanbieter automatisiert auf das Bankkonto zugreifen können, müssen sie sich mit einem oder mehreren Zertifikaten identifizieren. Auch Banken weisen sich mittels Zertifikat gegenüber den zugreifenden Zahlungsdienstleistern aus. Das Zertifikat gilt als „Unternehmensausweis" im elektronischen Geschäftsverkehr. Art. 34 der Delegierten Verordnung (EU) 2018/389 schreibt vor, dass QWACs oder QSiegel verwendet werden müssen. Dieser sichere Prozess ermöglicht neue Geschäftsmodelle zwischen Firmen, die ursprünglich keine Vertragsbeziehungen miteinander hatten. Die Aufnahme der eIDAS-Vertrauensdienste in die PSD2 eröffnet damit vollkommen neue und sichere Möglichkeiten der Kommunikation.

Grundsätzlich geht es bei neuen Gesetzen um eine regulatorische Ermöglichung und nicht um eine restriktive Regulation. Ein Vorbild dafür ist die „Better Regulation Toolbox"[39] der Europäischen Kommission. Die Toolbox#23 gibt auf 17 Seiten wertvolle Hilfestellung, um digitale Prozesse zu regulieren, überflüssige Regulierung zu verhindern und Konsistenz zu fördern. Die Berücksichtigung reduziert zudem die Gefahr möglicher Sanktionen eines EU-Vertragsverletzungsverfahrens wegen mangelnder Implementierung der eIDAS-Verordnung.

Es gibt zudem das Projekt „Bessere Rechtsetzung" des Bundesministeriums des Innern, für Bau und Heimat. Dieses Projekt sollte um eine Folgenabschätzung von Gesetzen für die digitale Transformation ergänzt werden, die wie auf EU-Ebene die Berücksichtigung von eIDAS-Vertrauensdiensten als wichtiges Mittel digitalisierungsfreundlicher Gesetzgebung anerkennt.

39 Europäische Kommission: „Better Regulation Toolbox", aufgerufen am 01.02.2019 unter *https://bit.ly/2QtI15V*

Regelungsbedarf in elf Anwendungsbeispielen nach aktueller Gesetzgebung

Regelungsbedarf	Beispiel	Gesetzanpassung	Zuständig
Formerfordernis für besondere digitale Geschäftsprozesse	Einführung einer eigenen **Form für die Digitalisierung.** Maschine-zu-Maschine- und digitale Mensch-zu-Maschine-Kommunikation	BGB: neue Formvorschrift § 126c	BMJV
Selbstfahrende Fahrzeuge/ autonome Maschinen: Einführung digitaler Kommunikation	**Identifizierung von autonomen Fahrzeugen** untereinander und bei Nutzern durch sichere Kommunikation mit Vertrauensdiensten: QSiegel für die Maschine und die Software	StVZO: Kommunikation und Identifikation von Fahrzeugen und Prüfung Vergabe von vernetzten Maschinen	BMVI
Einführung des elektronischen QSiegels	Vorteile des QSiegels im Vergleich zur QES: **rechtssichere Zuordnung zu Gericht oder Behörde**	VwVfG, VwGO, GVG: Einführung der QSiegel-Anforderungen in die Verfahrensgesetze	BMJV
Bürgerkonten	**Die eIDAS-Werkzeuge** konsequent für den Bürger und Unternehmen in der Kommunikation anbieten. Interoperabilität und Technologieoffenheit gewährleisten	EGovG: Einführung des QSiegels und anderer Werkzeuge entsprechend dem VDG	BMI, IT-Planungsrat
Digitale Zeugnisse von Arbeitgebern und öffentlichen Trägern (Universitäten, Kammern)	**Digitale Zeugnisse und Bescheinigungen,** die zur Nutzung im Rechtsverkehr bestimmt sind, müssen den Aussteller mit hinreichender Sicherheit identifizierbar machen	BGB, VwVfG: Sicherheit durch Stand der Technik von QES oder QSiegel des Rechtsträgers	BMJV
Juristische Kommunikation: Erweiterung ERV durch Einführung digitaler Kommunikation	Schaffung sicherer und vertrauensvoller Kommunikation von **Anwälten zu Mandanten und gerichtlichen oder behördlichen Partnern.** Übermittlung von digitalen Originalen und verschlüsselten Dokumenten an verschiedenste Teilnehmer	BRAO, BOStB: Einführung einer offenen eIDAS-Kommunikationsstruktur	BMJV
Einführung einer Tachostand-Datenbank zur Überwachung des Gebrauchtwagenmarkts	Datenbank, die sicherstellen soll, dass **die Laufleistung von Gebrauchtfahrzeugen nachvollziehbar** wird, und so den Betrug durch Manipulation bekämpfen soll	StVZO und Richtlinie 2014/45/EU des Europäischen Parlaments und des Rates vom 03.04. 2014, Art. 16	BMVI
E-Health mit intelligenten QSiegeln und Signaturlösungen erweitern	Einführung des **elektronischen Entlassbriefs, des elektronischen Eingangsstempels und der elektronischen Prozessdokumentation** in Pflege und Ambulanz	Prüfen, ob die Unterschrift bzw. QES notwendig ist. Im Zweifel automatisierte Verfahren fördern	BMG, gematik
Ersetzendes Scannen mit QSiegel ausdrücklich ermöglichen	Große **analoge Aktenmengen** müssen in den kommenden Jahren digitalisiert werden. Hier muss das QSiegel einsetzbar sein	Anpassung VwVfG, VwGO, ZPO	BMI, BMJV, IT-Planungsrat
Erweiterung digitale Beglaubigung durch QSiegel	**Wichtig ist die Identität der Behörde, nicht des Beamten.** Einführung des QSiegels auch für Beglaubigungen, um physische Dokumente digital verkehrsfähig zu machen	§ 33 Abs. 4 Nr. 4 und Abs. 5 VwVfG ermöglichen lediglich den Einsatz von QES, nicht aber von QSiegeln	BMI, BMJV
Absicherung von Websites mit öffentlichem Interesse erweitern	**Die Manipulation durch Fake-Seiten muss bekämpft werden.** Wasserwerke, Banken, Behörden, Krankenhäuser, Schufa usw. müssen nachvollziehbar die echten Betreiber der Website sein	TMG: Einsatz von QWACS für die Herkunftsangabe des Betreibers einer Website	BMI, BMVI

4.3.1 Einführung der Vertrauensdienste

Es wurde bisher deutlich, dass eine zukunftssichere Kommunikationsinfrastruktur auf Grundlage der europäischen Binnenmarktregulierung etabliert werden muss. In erster Linie geht es dabei um die Einführung des QSiegels und der QWACs in die deutsche Gesetzgebung. Die E-Government-Gesetze des Bundes und der Länder müssen entsprechend angepasst werden. Dafür muss ein bundeseinheitlicher Rahmen geschaffen werden, der aber auch in den Ländern umgesetzt wird. Damit können Behörden, Kommunen und sonstige öffentliche Stellen die Vertrauensdienste der eIDAS-Verordnung rechtssicher einsetzen.

E-Government-Gesetz (EGovG)

Das EGovG des Bundes (§§ 2, 6, 7) sollte eine Verpflichtung enthalten, dass die Instrumente der eIDAS-Verordnung genutzt werden müssen. Behörden sollten verpflichtet werden, elektronische Dokumente auch mit QSiegel (nicht nur mit der QES) entgegenzunehmen. Außerdem sollte das EGovG des Bundes (§§ 6, 7) auch um die Vorschriften zur elektronischen Akte erweitert werden: Das QSiegel könnte als geeignete technisch-organisatorische Maßnahme fungieren, um die elektronische Aktenführung und die Vernichtung von Papieroriginalen bei der Einführung elektronischer Archive abzusichern. Zwar enthält die TR RESISCAN einen Hinweis darauf, aber die gesetzliche Verankerung schafft für die öffentlichen Anwender mehr Rechtssicherheit als der veraltete Bezug ausschließlich auf die Signatur.

Bürgerliches Gesetzbuch (BGB)

Das Beispiel der digitalen Zeugnisse macht deutlich, dass auch das BGB angepasst werden muss. Wie im Beispiel beschrieben, müssten QES und QSiegel eingeführt werden. Die Regelungen könnten entweder im Allgemeinen Teil des BGB oder zu den jeweiligen spezialgesetzlichen Regelungen (Bildungseinrichtungen, Arbeitsverhältnisse usw.) hinzugefügt werden. Darüber hinaus wäre es sinnvoll, ein neues Formerfordernis für die QSiegel für juristische Personen einzuführen. Ähnlich wie die Textform mit zunehmender Verbreitung des Computers ins BGB Einzug fand, sollte das QSiegel als „Schriftform für Unternehmen" verankert werden. Dies wäre zum Beispiel bei der Ausgabe elektronischer Zeugnisse sinnvoll.

Verwaltungsverfahrensgesetz (VwVfG)

Bei der Implementierung des QSiegels in das VwVfG geht es nicht nur um einen symbolischen „Ritterschlag", sondern auch darum, die QSiegel in Einzelgesetzen und -verordnungen für konkrete Verwaltungsakte als geeignet, zulässig oder vielleicht sogar verbindlich zu erklären.[40]

Zeugnisse und Bescheinigungen können auch im öffentlichen Recht vorkommen und durch Universitäten, Behörden und Kammern ausgestellt worden sein. Hier bedarf es einer Regelung mit obigem Inhalt, wobei sich hier ein QSiegel ebenfalls wiederfinden muss.

Das QSiegel sollte in § 3a VwVfG verankert werden und die QES ergänzen. Dadurch können zukünftig Kosten für Signaturkarten und Infrastruktur gespart und gleichzeitig alte Signaturkarten bis zu ihrem Ablauf genutzt werden.

Auch damit Behörden QSiegel von Unternehmen akzeptieren, muss das VwVfG geändert werden. Dann können auch Unternehmen, Vereine, Stiftungen und andere europäische juristische Personen sicher elektronisch mit der Verwaltung kommunizieren.

Der Entwurf des „Gesetzes zum Abbau verzichtbarer Anordnungen der Schriftform im Verwaltungsrecht des Bundes" listet 586 Rechtsvorschriften des Bundes auf, bei denen auf die Schriftform verzichtet werden kann. Sie können entweder ersatzlos gestrichen oder durch einfache elektronische Verfahren ersetzt werden.[41] Das Gesetz ist schließlich mit 464 Änderungen am 30. März 2017 in Kraft getreten. Das QSiegel könnte hier eingesetzt werden, weil schon die strengere Schriftform nicht erforderlich ist. Gleichwohl braucht es eine ausdrückliche gesetzliche Klarstellung, um den Behörden die rechtssichere Nutzung zu ermöglichen. In diesem Fall steht nicht die Verbindlichkeit der Herkunft oder, im Falle der Signatur, die Willenserklärung im Vordergrund, sondern der Integritätsschutz (Schutz vor unbemerkter Veränderung).

§ 33 VwVfG regelt schon jetzt, dass jede Behörde von Urkunden, die sie selbst gefertigt hat, elektronische Dokumente und elektronische Beglaubigungen ausfertigen können muss. Diese elektronischen Abschriften und Beglaubigungen müssen auch mit einem QSiegel möglich sein, damit sich der Rechtskreis darauf verlassen kann und ein Beweis vorliegt, dass die Urkunde von dieser Behörde stammt.

In § 37 VwVfG muss ausdrücklich festgeschrieben werden, dass auch bei einem elektronischen Verwaltungsakt die erlassende Behörde durch ein QSiegel zu erkennen sein muss. Denn diese Anforderung erfüllt das QSiegel im Gegensatz zum Attributszertifikat und sollte darum folgerichtig erwähnt werden.

Zivilprozessordnung (ZPO)

Die Darstellung der Beweisregeln hat gezeigt, dass das QSiegel uneingeschränkt eingesetzt werden kann, solange es nicht die Schriftform ersetzen soll. Gleichwohl wird es von der ZPO nicht erwähnt und kann so für den Rechtsverkehr nicht bedeutend werden. Die deutschen Gerichte und Rechtsanwendenden müssen sich auch mit dem europäischen QSiegel auseinandersetzen, weil es im europäischen digitalen Binnenmarkt künftig zunehmend genutzt wird. Schon vor diesem Hintergrund erscheint es sinnvoll, das QSiegel in § 371a ZPO ergänzend aufzunehmen. Regelungsinhalt könnte sein, das QSiegel beweisrechtlich so zu behandeln wie die QES. So kann für eine elektronische Nachricht oder ein elektronisches Dokument der Anschein der Echtheit nur durch Tatsachen erschüttert werden, die ernstliche Zweifel daran begründen, dass die Nachricht von dieser juristischen Person mit diesem Inhalt versandt wurde. Probleme zur Vertretungsmacht lassen sich im Übrigen nach diesen Vorschriften und den Grundsätzen der Stellvertretung lösen.

Darüber hinaus ergibt sich ein Problem bei dem Beweiswert nach § 371b ZPO. Dieser sieht vor, dass eine ehemals physische öffentliche Urkunde nur dann eine elektronische öffentliche Urkunde mit der Echtheitsvermutung wird, wenn die scannende mit der bestätigenden Person identisch ist und eine öffentliche Funktion hatte bzw. mit öffentlichem Glauben versehen ist und zudem ihre persönliche QES anbringt. Allerdings können große Archivbestände so nicht effizient digitalisiert werden, weil die Person am Scanner jedes Dokument mit ihrer Signatur versehen muss. Für effiziente und gleichwohl sichere Digitalisierungsprozesse muss das QSiegel hier ebenfalls möglich sein. Durch diese Brücke zwischen der papiergebundenen und der digitalen Welt wird zukunftsgewandtes Handeln überhaupt erst ermöglicht.

Außerdem müsste § 169 Abs. 4 ZPO um die Verwendung des QSiegels ergänzt werden, damit die Bescheinigung und Beglaubigung der Zustellung von Schriftsätzen automatisiert und eine effiziente Nutzung der technologischen Möglichkeiten erfolgen kann.

Verwaltungsgerichtsordnung (VwGO)

Ebenso wie in der ZPO müssen die eIDAS-Vertrauensdienste auch in der VwGO und den anderen Gerichtsordnungen verankert werden. Nur so sind einheitliche, interoperable und zukunftssichere IT-Lösungen möglich. In § 55a VwGO ist die elektronische Übermittlung bereits geregelt – insbesondere der Ersatz durch die QES bei bisherigem Schriftformerfordernis. Das QSiegel ist hier noch nicht berücksichtigt. Allerdings kann neben der QES auch ein anderes sicheres Verfahren zugelassen werden, das die Authentizität und die Integrität des übermittelten elektronischen Dokuments sicherstellt. Dies sollte durch eine neue Rechtsverordnung der Bundesregierung bestimmt werden. Für ein zukunftssicheres Verfahren muss auch hier das QSiegel eingeführt werden, da es auf derselben Technologie der Zertifikate für QES aufsetzt.

Telemediengesetz (TMG)

Im TMG müsste es ermöglicht werden, dass Websites mit öffentlichem Interesse – dazu zählen etwa die Websites von Behörden und künftigen Bürgerkonten, Arbeitsämtern, dem Auswärtigen Amt, Krankenhäusern, Feuerwehr oder Polizei – sicher dem tatsächlichen Betreiber zugeordnet werden können. Der Nutzer muss automatisiert prüfen können, dass es sich um eine vom Aussteller stammende Website oder Internetanwendung handelt. Dazu sollte der Einsatz von QWACs eine verpflichtende Absicherung werden. Dies ist in § 13 Abs. 7 TMG bereits für die Verschlüsselung der Kommunikation der Website festgelegt und kann technologieoffen auch für die verlässliche Betreiberherkunft erfolgen.

40 Vgl.: Floren, Annette/Entschew, Enrico/Fiedler, Arno: Sichere (elektronische) Dokumente. Neue Rahmenbedingungen durch die europäische eIDAS-Verordnung. White Paper des Forums elektronische Vertrauensdienste. S.22.

41 Drucksache des Deutschen Bundestags 18/11007 vom 25.01.2017: Beschlussempfehlung und Bericht des Innenausschusses (4. Ausschuss) zu dem Gesetzentwurf der Bundesregierung, Entwurf eines Gesetzes zum Abbau verzichtbarer Anordnungen der Schriftform im Verwaltungsrecht des Bundes. S. 2, aufgerufen am 01.02.2019 unter *http://dip21.bundestag.de/dip21/btd/18/110/1811007.pdf*.

Sozialgesetzbuch (SGB) I, IV, V, X, XI

Für den Austausch von Daten und Dokumenten im Gesundheitswesen sollte auf die vorhandenen eIDAS-Standards zurückgegriffen werden. Dafür bedarf es einer Reihe von Änderungen im SGB. Generell bietet sich hier ein Normenscreening an, um eine vollständige Übersicht über den Anpassungsbedarf zu erhalten und einen stärkeren eIDAS-Bezug im SGB herzustellen.

Im Ersten Sozialgesetzbuch sollte als elektronisches Mittel im § 36a (Elektronische Kommunikation) das QSiegel aufgenommen werden, zum Beispiel indem ein neuer Absatz hinzugefügt wird:

Vorschlag für eine Ergänzung des SGB I § 36a

(1) Die Übermittlung elektronischer Dokumente ist zulässig, soweit der Empfänger hierfür einen Zugang eröffnet.

(2) (neu) *Die intersektorale Kommunikation und Datenübertragung im Gesundheitswesen ist als elektronischer Datenaustausch von personenbezogenen Behandlungs- und Gesundheitsdaten über die Grenzen der klassischen Sektoren hinaus, wie niedergelassene Ärzte, Kliniken, Nachsorge- und Rehabilitationsbereiche, die Selbstverwaltungen, Kranken-/Ersatzkassen, Behörden und öffentliche Einrichtungen des Gesundheitswesens, über vom Gesetzgeber zugelassene Infrastrukturen (Telematikinfrastruktur, KV-SafeNet etc.), die Nutzung standardisierter Übertragungstechnologien zur Sicherstellung des gesetzlich vorgeschriebenen Datenschutzes und Datensicherheit sowie die mit geeigneten standardisierten Methoden zur Identifikation, Authentifikation und Integrität nach der Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates vom 23. Juli 2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt (eIDAS) sicherzustellen.*

Für die Transportsicherung beim Austausch von Daten zwischen den Primärsystemen im Gesundheitswesen und für die Identifikation der Teilnehmer oder teilnehmender Systeme der Kommunikation sind QWACs gemäß oben genannter Verordnung zu verwenden. Für die Sicherung der Authentizität von medizinischen Dokumenten und Daten (Anwendungsebenen) sind qualifizierte Siegel gemäß genannter Verordnung zu verwenden, sofern die Schriftform nicht gewahrt werden muss.

...

Im Vierten Sozialgesetzbuch (§ 110, SGB IV) ist die Aufbewahrungspflicht für Sozialversicherungsträger festgehalten. Hier sollte für die elektronische Form der Aufbewahrung ausdrücklich auch die Absicherung mithilfe von QSiegeln vorgesehen werden. So werden automatisierte Ablagesysteme ermöglicht. Im Fünften Sozialgesetzbuch (§ 291a ff. SGB V) legt die „gematik Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH" im Einvernehmen mit dem BSI die Standards für die Nutzung der Telematikinfrastruktur fest. Auch dort kann das QSiegel Anwendung finden.

Im Zehnten Sozialgesetzbuch (§§ 25, 33 SGB X) sollten elektronische Auszüge oder Abschriften aus Akten, für die eine Akteneinsicht zu gewähren ist, ebenfalls mit dem QSiegel abgesichert werden. Denn bei der Abschrift kommt es nicht auf die Person desjenigen an, der die Abschrift auslöst oder verschickt, sondern auf die Authentizität des Dokuments, von dem die Abschrift gefordert wird.

Darüber hinaus sollte geprüft werden, ob im Elften Sozialgesetzbuch zur Pflegeversicherung (§§ 7, 105 SGB XI) QWACs und QSiegel für die Abrechnungs- und Dokumentationssysteme sowie für sonstige Mitteilungen genutzt werden können. Derzeit ist in § 105 Abs. 2 SGB XI geregelt, dass für die Übertragung elektronischer Dokumente neben der QES auch ein anderes sicheres Verfahren vorzusehen ist, das den Absender authentifiziert und die Integrität des Datensatzes gewährleistet. Eine Verankerung des QSiegels bietet sich hier immer dann an, wenn es auf die Dokumentation des Vorgangs ankommt und nicht auf die persönliche Haftung.

4.3.2 Neue Regelungen für den sicheren elektronischen Rechtsverkehr

Einige Bereiche des Rechtsverkehrs benötigen gänzlich neue Regelungen, um digitale Geschäftsprozesse einführen zu können.

Das BGB und die Herausforderung völlig neuer Kommunikationsformen

In das BGB muss eine Regelung zu neuen Kommunikationsbeziehungen, die im Zuge der Digitalisierung auftauchen, aufgenommen werden. Denn ein separates Gesetzeswerk zu schaffen, würde der Bedeutung der Digitalisierung nicht gerecht. Durch die Aufnahme ins BGB können die zahlreichen Verweisungen von Fachgesetzen sinnvoll genutzt werden.

So wird das selbstfahrende Fahrzeug selbstständig an eine Ladesäule fahren und dort Strom tanken oder einen Parkplatz im automatischen Parkhaus mieten und zu Reparaturen in eine Werkstatt fahren. Wenn das smarte Haushaltsgerät eine Bestellung abgibt, automatisierte Internethändler darauf reagieren und ebenso automatisiert eine Transportdienstleistung bestellen, die eventuell von einem automatisierten Lieferroboter ausgeführt wird, müssen diese vertraglichen Beziehungen manipulationssicher gestaltet und nachvollziehbar dokumentiert werden können.

Inhaltlich müsste die Regelung verschiedene Bereiche abdecken: (1) Welche Definition für eine maschinelle Kommunikation zu finden ist. (2) Die Form, die eine Maschine bzw. Software einhalten muss, um sie im Nachhinein auch menschlich nachzuvollziehen. (3) Wer für Handlungen der Maschine haftet. (4) Wer anspruchsberechtigt wird.

Für die Form der Kommunikation können die Ergebnisse aus der Untersuchung zur Vertrauensfunktion genutzt werden. Es muss eine Formvorschrift greifen, wann immer es zu einer nachhaltigen Auswirkung durch das Maschinenhandeln kommt, ein Interesse an der Identifikation der Maschine und dem dahinterstehenden Rechtsträger entsteht und ein Bedürfnis an der Sicherheit der Kommunikationsbeziehung besteht.

Hier ist das QSiegel die passende Form. Es identifiziert eine juristische Person, die hinter der Maschine und Software als Rechtsträger steht. Außerdem kommuniziert die Maschine im Zweifel als eigene, ebenfalls virtuelle Entität. Für das QSiegel spricht zudem der Bedarf nach einer Abgrenzung zur menschlichen Kommunikation. Es bietet die notwendige Manipulationssicherheit und Dokumentationsfähigkeit. So kann vermieden werden, dass derartige Abläufe durch „falsche" Maschinen ausgelöst werden oder die Kommunikation manipuliert wird. Neben der Identität der Maschine muss aber auch der Kommunikationsweg abgesichert werden. Dies kann durch QWACs erfolgen. Sie sorgen dafür, dass von einer Maschine oder Software verschlüsselte Daten den richtigen Server oder die richtige Kommunikationsplattform erreichen. Um den kausalen Ablauf festzuhalten, können elektronische Zeitstempel eingesetzt werden.

Gleiches kann auch für die Mensch-zu-Maschine-Kommunikation gelten. Hier wurden zur Benutzung von mechanischen Automaten schon Grundsätze entwickelt. Allerdings wird erstmals auch in die andere Richtung (ergebnisoffene Software mit dem Menschen) rechtserheblich kommuniziert, zum Beispiel in Chatbots, bei Telefonhotlines oder wenn die Software einen menschlichen Lieferanten zu einer Dienstleistung beauftragt oder ein Pflegeroboter Leistungen erbringt. Hier muss der Mensch ebenso wissen, welche Maschine oder Software etwas bestellt oder leistet.

Berufsgeheimnisträger: BRAO und BOStB

Hier besteht Erweiterungsbedarf bei § 42 BRAO und § 5 BOStB. Die bisherigen Regelungen betreffen nur die Verpflichtung des Dienstleisters, nicht aber den Mandantenkontakt. Hier sind die Berufsstände noch auf sich gestellt. Es wäre förderlich, digitale Prozesse durch einen gesetzlichen Rahmen zu unterstützen. Geregelt werden sollte, dass Verschlüsselungstechnologien nach dem Stand der Technik ausreichen, um der Verpflichtung zur berufsrechtlichen Verschwiegenheit nachzukommen. Zudem sollte geregelt werden, dass die Offenbarung, Weitergabe oder Einsicht von vertraulichen Informationen digital nur bei sicherer Identifizierung der Kommunikationsbeteiligten zulässig ist. Diese Anforderungen sind insbesondere

bei der Nutzung von eIDAS-Vertrauensdiensten gegeben. Zu begrüßen ist, dass mit der Reform des § 203 StGB und des § 2 BORA die Dienstleister bereits miteinbezogen wurden und hier die Problematik der Verschwiegenheit der digitalen Serviceprovider gelöst werden soll. Dies beinhaltet aber nur in Ausnahmefällen die Kommunikation und den Erhalt oder die Weitergabe von Dokumenten an die oben aufgezählten Gruppen. Diese sind gerade nicht Dienstleister des Rechtsanwalts, sondern im Zweifel Verfahrensbeteiligte. Deshalb braucht es eine technologieoffene, europaweit standardisierte Vertrauensinfrastruktur.

EU-Richtlinie zur technischen Überwachung von Kraftfahrzeugen

Art. 16 der Richtlinie 2014/45/EU des Europäischen Parlaments und des Rates vom 03. April 2014 muss europäisch einheitlich umgesetzt werden. Die Datenbank kann durch QWACs gegen Manipulation abgesichert werden und der Zugriff berechtigter Benutzer (Werkstätten und TÜV-Prüfstandorte) mit QSiegeln bestätigt werden. Der Abruf von Informationen zu den Laufleistungen kann durch die Mittel des EGovG und der eIDAS-Verordnung sinnvoll geleistet werden (zum Beispiel De-Mail, QES und QSiegel für Versicherungen).

Regulatorische Ermöglichung von öffentlichen Cloud-Diensten

Die öffentliche Hand wird durch Cloud-Dienste effizienter und kann künftig digitale Prozesse besser bewältigen. Für derartige Dienste und Anwendungen braucht es aber die erforderliche Rechtssicherheit der Anwender und Hersteller dieser Lösungen. Es fehlt bisher ein Rahmen zur regulatorischen Ermöglichung dieser Dienste. Dazu müssen die eIDAS-Vertrauensdienste für die Kommunikation eingesetzt werden. Auch hier greifen die Merkmale der Vertrauensfunktion. Dies muss gleichwohl mit den bisherigen Überlegungen des BSI-Anforderungskatalogs C5 kombiniert werden. Dadurch wird die physische Sicherheit und Qualität der Dienstleistung gewährleistet. Zudem wird die kommunikative Sicherheit der Nutzer und Anwendungen durch den Einsatz qualifizierter Vertrauensdienste rechtsverbindlich sichergestellt. Es braucht eine bundesweit verbindliche regulatorische Lösung, um Kommunen, Ländern und den Bundesbehörden zu erlauben, Cloud-Dienste effizient einzusetzen.

5 AUSBLICK

Die Digitalisierung stellt die deutsche Wirtschaft und Verwaltung vor große Herausforderungen. Es ist zwingend erforderlich, die deutschen Gesetze, Verordnungen und Richtlinien anzupassen, um auf die Veränderungen zu reagieren.

Die vorgeschlagenen Rechtsänderungen und die Einführung der eIDAS-Vertrauensdienste können Deutschland im Wettbewerb um die besten digitalen Standorte wieder ganz vorn platzieren. Gleichzeitig können sie das Vertrauen der Bürger in den Staat stärken, da ihnen teil- oder vollautomatisierte Verwaltungsvorgänge die Funktionsfähigkeit der öffentlichen Verwaltung aufzeigen.

Bei allen juristischen Überlegungen dürfen die faktischen Veränderungen der Gesellschaft nicht außer Acht gelassen werden. Digitale Bedrohungen, wie Cyber-Angriffe auf Unternehmen oder Personen, nehmen zu und werden schwerwiegender. Deutschland muss diesen neuen digitalen Gefahren mit einer erhöhten Resilienz begegnen. Es ist unumgänglich, digitale Sicherheitsmechanismen einzuführen und zu fördern. Hier liegt ein Mehrwert der eIDAS-Verordnung: Mit ihren Vertrauensdiensten kann sie gegen digitale Bedrohungen schützen – sei es im Gesundheitswesen, im digitalen Rechtsverkehr oder in der Verwaltung. So können behördliche Server gegen Überlastausfälle dadurch geschützt werden, dass nur fälschungssichere Zertifikate durch die Filtermechanismen gelassen werden. Gleichzeitig ließe sich beispielsweise auch der Softwareschutz verbessern. Der Einsatz vertrauenswürdiger Software ist aufgrund der umfassenden Bedrohungen durch Schad-, Ausspäh- und Erpressungsprogramme äußerst wichtig. Bereits heute gibt es zum Schutz von Softwareprogrammen Prüfmechanismen, die auf QES beruhen. Zukünftig könnten QSiegel zum Schutz vor bösartiger Manipulation eingesetzt werden. Vor Installation oder Ausführung der Software würde der Herausgeber mittels des QSiegels identifiziert. Ist die Prüfung erfolgreich, kann die Software genutzt werden. Zusätzlich könnten QSiegel in Kombination mit QWACs auch für automatisierte elektronische Kommunikationsprozesse (zum Beispiel Maschine-zu-Maschine-Kommunikation), zur Device-Authentisierung oder zum asynchronen Integritätsnachweis eingesetzt werden.

6 HANDLUNGSEMPFEHLUNGEN

Die eIDAS-Verordnung ermöglicht einheitliche digitale Geschäfts- und Verwaltungsprozesse in der Europäischen Union. Die darin enthaltenen Vertrauensdienste wurden allerdings noch nicht sinnvoll in das deutsche Recht integriert und entfalten daher noch keine große Wirkung.

Es ergeben sich konkrete Handlungsempfehlungen für die Politik:

1. Die Bundesregierung sollte die Defizite bei der Umsetzung der eIDAS-Verordnung schnellstmöglich aufarbeiten. Insbesondere in Bezug auf das qualifizierte elektronische Siegel und qualifizierte Website-Zertifikate braucht es neue gesetzliche Regelungen, wie sie beispielweise bereits in der Payment Services Directive 2 (PSD2) vorhanden sind. Die PSD2 kann als Vorbild dienen, um weitere Anwendungsfelder zu erschließen und dort ähnliche Regelungen zu treffen. Eine Orientierung dazu bieten die gesetzlichen Änderungsvorschläge dieser Studie. Erste konkrete Schritte sollten bis zum 1. Halbjahr 2020 – wenn die Europäische Kommission eine Evaluation der eIDAS-Verordnung durchführt – sichtbar sein. Dabei sollte die Bundesregierung die Umsetzung der eIDAS-Verordnung und die Nutzung der darin standardisierten Vertrauensdienste auch als wichtigen Beitrag für mehr Daten- und Verbraucherschutz in Deutschland verstehen.
2. Im Rahmen der „digitalen Gesetzgebung" sollte eine Orientierung an der „Better Regulation Toolbox #23" der Europäischen Kommission erfolgen. Dazu gibt es bereits das Projekt „Bessere Rechtsetzung" des Bundesministeriums des Innern, für Bau und Heimat. Dieses Projekt sollte um eine Folgenabschätzung von Gesetzen für die digitale Transformation ergänzt werden, die wie auf EU-Ebene die Berücksichtigung von eIDAS-Vertrauensdiensten als wichtiges Mittel digitalisierungsfreundlicher Gesetzgebung anerkennt.
3. Im Rahmen der deutschen EU-Ratspräsidentschaft im Jahr 2020 sollte die Bundesregierung die Weiterentwicklung der eIDAS-Verordnung als Priorität behandeln und die Präsidentschaft nutzen, um die Verhandlungsführung im Rat bei der Überarbeitung der Verordnung zu übernehmen. Dabei geht es vor allem um die Einführung neuer Instrumente (z. B. eine eID-Funktion für Unternehmen), eine stärkere Verbindlichkeit bei der Nutzung und Anerkennung der Vertrauensdienste sowie eine weitere Harmonisierung der Voraussetzungen für die Zertifizierung und Zulassung von eIDAS-Vertrauensdiensten.

Die folgende Liste enthält Beispiele für gesetzgeberische Maßnahmen, um die eIDAS-Vertrauensdienste sinnvoll in das deutsche Recht zu integrieren:

Gesetz	Erweiterung Vertrauensdienst	Anwendungsbeispiele	Zuständigkeit Ministerium
ZPO	QSiegel, Zeitstempel	Zustellung Schriftsätze, Beglaubigung, Beweismittel	BMJV
StVZO	QSiegel, Zeitstempel, Zustell-dienste	Tachostand- Datenbank für TÜV- und KFZ-Werkstätten	BMVI
VwVfG	QSiegel	Anträge und Erklärungen an Behörden durch Unternehmen, § 3a VwVfG	IT-Planungsrat, BMJV
	QSiegel	Elektronisches Äquivalent für Beglaubigungen und Dienstsiegel, §§ 3a, 33 Abs. 5, 37 VwVfG	IT-Planungsrat, BMJV
	QES, QSiegel	Führungszeugnisse	BMJV
EGovG Bund	Verankerung aller Standards der eIDAS-Verordnung	Grundlage für die Einführung im E-Government: Zustellungs- und Empfangsverpflichtung, E-Akte mit QSiegeln	IT-Planungsrat, BMI
EGovG Länder	Verankerung aller Standards der eIDAS-Verordnung	Grundlage für die Einführung im E-Government: Zustellungs- und Empfangsverpflichtung, E-Akte mit QSiegeln	IT-Planungsrat, IMK
BGB	QSiegel	Digitale Unternehmens-informationen	BMJV
	QES, QSiegel	IHK-Zeugnisse, Arbeitgeberzeug-nisse, Diplome, Meisterbriefe	BMJV
	QSiegel, QWACs, Zeitstempel	Mensch-zu-Maschine-Kommuni-kation und Mensch-zu-Mensch-Kommunikation	BMJV
TMG	QSiegel, QWACs	Sichere Kommunikation, § 13 Abs. 7	BMI, BMVI
BRAO, BOStB	QSiegel, Zeitstempel, Zustell-dienste	Nutzung der eIDAS-Vertrauens-dienste für Verfahrenskommuni-kation	BMF, BMJV
EStG	QSiegel	Nutzung des QSiegels für Banken, § 45a Abs. 2 EStG	BMF
Eu-RiLi technische Überwachung von Kraftfahrzeugen	QSiegel, QWACs	Gesetz zur Datenbankerstellung und -nutzung	BMVI
SGB I	QSiegel	Absicherung der elektronischen Kommunikation	BMG
SGB XI (Pflege)	QSiegel, QWACs	Mitteilungen, Abrechnung, Dokumentation in der Pflege	BMG
SGB IV, X (E-Health)	QSiegel, QWACs	Mitteilung der Träger, Speicherung und Abschriften	BMG

7 ABKÜRZUNGSVERZEICHNIS

AO	Abgabenordnung
BGB	Bürgerliches Gesetzbuch
BMG	Bundesministerium für Gesundheit
BMI	Bundesministerium des Innern, für Bau und Heimat
BMJV	Bundesministerium der Justiz und für Verbraucherschutz
BMVI	Bundesministerium für Verkehr und digitale Infrastruktur
BORA	Berufsordnung für Rechtsanwälte
BOStB	Berufsordnung der Bundessteuer-beraterkammer
BRAO	Bundesrechtsanwaltsordnung
EGovG	Gesetz zur Förderung der elektronischen Verwaltung (E-Government-Gesetz)
eIDAS-Verordnung	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
ERV-Gesetz	Gesetz zur Förderung des elektronischen Rechtsverkehrs mit den Gerichten
EStG	Einkommenssteuergesetz
GG	Grundgesetz für die Bundesrepublik Deutschland
GGO	Gemeinsame Geschäftsordnung der Bundesministerien
GVG	Gerichtsverfassungsgesetz
IMK	Innenministerkonferenz
PSD2	Payment Services Directive 2
QES	Qualifizierte elektronische Signatur
QSiegel	Qualifiziertes elektronisches Siegel
SGB	Sozialgesetzbuch (mit römischer Zahlenbezeichnung)
SigG	Signaturgesetz (außer Kraft getreten)
StGB	Strafgesetzbuch
StVZO	Straßenverkehrs-Zulassungs-Ordnung
TMG	Telemediengesetz
TR RESISCAN	Technische Richtlinie zum rechtssicheren ersetzenden Scannen des Bundesamts für Sicherheit in der Informationstechnik
VDG	Vertrauensdienstegesetz
VDV	Verordnung zu Vertrauensdiensten
VwGO	Verwaltungsgerichtsordnung
VwVfG	Verwaltungsverfahrensgesetz
ZPO	Zivilprozessordnung

Bundesdruckerei GmbH
Kommandantenstraße 18 10969 Berlin
Tel.: +49 (0)30 2598-0 Fax: +49 (0)30 2598-2205
info@bdr.de www.bundesdruckerei.de