# eIDAS Mittel und ihr Innovations-potential: zukunftsträchtig und vertrauenswürdig

Impulspapier zu den kurzfristigen Zielen und Potentialen der eIDAS Verordnung

www.bitkom.org

bitkom

**Herausgeber**

Bitkom e. V.
Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e. V.
Albrechtstraße 10 | 10117 Berlin

**Ansprechpartner**

Rebekka Weiß | Leiterin Vertrauen & Sicherheit
T 030 27576-161 | r.weiss@bitkom.org

**Satz & Layout**

Katrin Krause | Bitkom e.V.

**Titelbild**

© mbbirdy – istockphoto.com

# Einleitung

Mit Inkrafttreten der Verordnung über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt der Europäischen Union (eIDAS) 2014 wurde die Basis für eine europaweite, rechtsgültige elektronische Kommunikation und sichere elektronische Identifizierung geschaffen. Die EU-Signaturrichtlinie, das deutsche Signaturgesetz und Signaturverordnung wurden obsolet.

Mit Hilfe der Vertrauensdienste (elektronische Signaturen, Siegel, Zeitstempel, Zustelldienste und Zertifikate zur Authentifizierung) können sich Unternehmen, Verwaltungen und Privatpersonen digital, für unabhängige Dritte nachvollziehbar innerhalb der Europäischen Union auf einer einheitlichen Rechtsbasis austauschen. Die eIDAS schafft neue Anwendungsmöglichkeiten innerhalb und zwischen allen Ländern der Europäischen Union. Dies betrifft alle Lebenslagen. So können Verträge grenzüberschreitend rechtssicher in elektronischer Form abgeschlossen werden. Patientendaten und medizinische Kommunikation, wie Arztbriefe, sind nun europaweit auf einheitlicher Grundlage digital schützbar. Öffentliche Register, wie Handelsregister und Grundbücher, haben jetzt die Option der beweisgültigen digitalen Beauskunftung. Die öffentliche Verwaltung kann über Landesgrenzen verbindlich kommunizieren.

Das Potential der neuen Werkzeuge und der Vereinheitlichung für die Digitalisierung ist enorm und sollte dringend in Wirtschaft und Verwaltung zur Anwendung kommen. Der Einsatz der Vertrauensdienste muss deswegen vor allem von entsprechenden nationalen Rahmenbedingungen flankiert und gefördert werden. Mit diesem Positionspapier beabsichtigt der Bitkom der Bedeutung und Relevanz elektronischer Vertrauensdienste die notwendige Aufmerksamkeit zu verschaffen. Hierfür sollen die Vertrauensdienste strategisch entsprechenden Maßnahmen befördert werden.

In diesem Positionspapier werden die kurzfristigen Maßnahmen und Einsatzszenarien beschrieben.[1] Gleichzeitig liegt ein Schwerpunkt der Ausführungen darauf, welche unmittelbaren Vorteile für die deutsche Verwaltung und Wirtschaft die Verwendung der Vertrauensdienste mit sich führen. Natürlich werden auch bestehende oder angenommene Hindernisse für die unmittelbare Verwendung adressiert.

Der Bitkom sieht die nachfolgenden Anwendungen als kurzfristig umsetzbar und förderungswürdig an:

- Qualifiziertes elektronische Fernsignatur für den behördlichen Einsatz (↗**Abschnitt 1**)
- Qualifiziertes elektronisches Siegel (Q-Siegel)[2] für behördliche Dokumente (↗**Abschnitt 2**) sowie elektronische Zeugnisse (↗**Abschnitt 3**)
- Qualifizierte Webseitenzertifikate (QWACs) zum Schutz von Webseiten (↗**Abschnitt 4**)
- Fernidentifikation im Videoidentifizierungsverfahren (↗**Abschnitt 5**)
- Weiterentwicklung der Gesetzgebung zur Unterstützung der Digitalisierung empfohlen (↗**Abschnitt 6**)

1 Ergänzend dazu verweisen wir auf die weiteren Positionspapiere im Rahmen der Strategie, insb. zu den mittel- und langfristigen Zielen und Potenzialen.

2 Qualifiziertes elektronisches Siegel nach Art 3 Abs. 27 eIDAS-VO.

## Was ist ein Q-Siegel eigentlich?

### Digitalisierungsturbo: Das elektronische Siegel

**Gut zu wissen**

Es gibt in der EU-Verordnung eIDAS drei Varianten des Siegels:

- Fortgeschrittenes elektronisches Siegel (Art 3 Abs. 26)
- Qualifiziertes Zertifikat für elektronische Siegel (Art 3 Abs. 30)
- Qualifiziertes elektronisches Siegel (Art 3 Abs. 27)
  (Unterschied: Sichere Siegelerstellungseinheit + qualifiziertes Zertifikat)

Aber nur für letzteres gelten die Beweisregelungen der eIDAS, von daher sollte der Fokus auf diesem Siegel liegen.

Das EU-konforme Q-Siegel schafft eine komfortable und zuverlässige Möglichkeit, um elektronische Dokumente einem schnellen Echtheits-Check zu unterziehen. Im Ergebnis kann man sich darauf verlassen

- dass tatsächlich diejenige juristische Person bzw. Organisation (Firma, Behörde, Universität etc.) das Dokument ausgestellt hat, die als Absender genannt ist (Authentizität);

- dass die Daten des Dokumentes hundertprozentig dem Original entsprechen, also nicht im Nachhinein verfälscht worden sind (Integrität).

Eine juristische Person erhält das Q-Siegel nur, wenn diese durch den Vertrauensdiensteanbieter eindeutig identifiziert werden konnte.

Im Anschluss wird das Q-Siegel der anwendenden Organisation auf einem sicheren Träger, wie z.B. einer Siegelkarte, einem Hardware Security Module (HSM) oder auch als fernausgelöstes Q-Siegel übergeben.

Das qualifizierte elektronische Siegel stellt das hochwertigste Siegel dar und der Identifizierungsprozess ist entsprechend streng. Aber es lohnt sich: ein qualifiziert gesiegeltes Dokument ist europaweit als Beweismittel vor Gericht zuzulassen.

# Was ist ein qualifiziertes Webseitenzertifikat (QWAC) eigentlich?

## TLS-Zertifikate für Transportsicherung und Identitätsbestätigung

Mit Hilfe des TLS[3]-Zertifikats werden zwei Funktionen realisiert, die Transportsicherung und die Identitätsbestätigung. Ein klassisches TLS-Zertifikat enthält für die Identitätsbestätigung Informationen zur Domain, die es absichert und kann drüber hinaus noch Informationen zur Organisation, der die Domain gehört bzw. Adress- und Kontaktinformationen enthalten. Diese Informationen werden durch einen Vertrauensdiensteanbieter überprüft, der das entsprechende TLS-Zertifikat ausstellt. Für den User ist die TLS-verschlüsselte Verbindung durch ein Schloss in der Adresszeile erkennbar. Er kann im Browser die im Zertifikat gespeicherten Informationen einsehen.

## Mit dem qualifizierten Webseitenzertifikat einen Schritt weiter

Das in der eIDAS definierte qualifizierte Webseitenzertifikat (QWAC) geht einen Schritt weiter als das klassische TLS-Zertifikat. Das QWAC bietet als Besonderheit den Aspekt der Verbindlichkeit. Die EU-Kommission hat frühzeitig erkannt, dass es neben der reinen Verschlüsselung auch notwendig ist, ein Instrument zu schaffen, welches dem Gegenüber des Webservers, unabhängig davon, ob es z.B. ein Browser, eine App oder ein Dienst ist, verbindlich Auskunft gibt, mit wem man kommuniziert.

Dies wird gewährleistet, indem nur qualifizierte VDAs ein qualifiziertes Webseitenzertifikat ausstellen dürfen. Technisch handelt es sich um ein ganz normales TLS-Zertifikat. Inhaltlich sind jedoch sämtliche Angaben in dem Zertifikat durch den qualifizierten VDA auf ihre Korrektheit geprüft worden. Der Antragsteller muss entsprechend notwendige Nachweise erbringen, die garantieren, so dass die gewünschten Einträge vorgenommen werden können.

Das Profil eines Webseitenzertifikats ist in der Norm ETSI EN 319 412-4 definiert.

Mit qualifizierten Webseitenzertifikaten ist der Aufbau und Betrieb einer sicheren Infrastruktur möglich, ein Aspekt der in der heutigen Zeit nicht zu unterschätzen ist: Sichere und vertrauenswürdige Kommunikation in unsicheren Netzen.

3 Transport Layer Security

# 1 Sicherung der Arbeitsfähigkeit von Behörden in der Pandemielage

## Ausgangslage »Pandemie«

Die Corona-Pandemie ist ein Brennglas, das aufzeigt, wo digitale Dienstleistungen in Wirtschaft und Verwaltung nicht funktionieren.[4] Dem Verwaltungsmitarbeiter und dem Bürger stehen häufig nicht die Mittel zur Verfügung, um verbindlich elektronisch zu kommunizieren.

In der heutigen Lage kommt es darauf an, dass Dienstleistungen der Verwaltungen und der Unternehmen medienbruchfrei online funktionieren. Dabei stehen sie vor einigen zentralen Digitalisierungsaufgaben, wie z.B.:

- Behörden müssen auch bei eingeschränkten Öffnungszeiten und Zugangsmöglichkeiten in der Lage sein, ihre Dienstleistungen durchgehend anzubieten und dies sowohl im nationalen wie im europäischen Umfeld.

- Es müssen durchgängige digitale Workflows geschaffen werden, die funktionieren, auch wenn Behörden geschlossen sind. Dies sorgt auch für Kosteneffizienz bei den eingesetzten Fachverfahren.

## Lösung »Einsatz der qualifizierten Fernsignatur«

Der eIDAS-Vertrauensdienst qualifizierte Fernsignatur entfaltet eine große Digitalisierungswirkung. Die qualifizierte elektronische Signatur ist in der Rechtswirkung der handschriftlichen Unterschrift gleichgestellt. Mit der qualifizierten elektronischen Fernsignatur lassen sich elektronische Unterschriften auch aus der Ferne online auslösen. Qualifiziert elektronisch signierte Dokumente weisen eindeutig auf den Unterzeichner hin und schützen gleichzeitig das Dokument vor Manipulationen.

**In der Pflicht: Verwaltung und Politik**

Um die qualifizierte Fernsignatur stärker im Digitalen zu verankern, müssen sie vor allem einfach zu bedienen und integrierbar sein. Wichtige Schritte auf dem Weg dorthin wurden bereits gemacht: Fernsignaturdienste sind bereits auf dem Markt verfügbar. Diese Lösungen sind cloudbasierte Services, die die elektronische Unterschrift über eine Webanwendung ermöglichen. Zudem lässt sich der Fernsignaturdienst über ein API leicht DSGVO-konform in einen bestehenden Workflow integrieren.

Marktgängige deutsche Signaturlösungen sind bereits in einer großen Vielzahl vorhanden und können sofort genutzt werden. Damit kann die elektronische Unterschrift in einem nahtlosen Prozess direkt von der Signaturapplikation aus getätigt werden. So ist ein durchgängiges digitales Verwaltungshandeln einfach umsetzbar.

4 Die Pandemielage hat bereits zu einem deutlichen Digitalisierungssprung geführt: **↗www.bitkom.org/Presse/Presseinformation/Corona-Pandemie-beschleunigt-Digitalisierung-der-Verwaltung**. Nun muss es darauf ankommen, diesen Ausbau strategisch fortzusetzen und auf sichere Digitalisierungstools zu setzen.

# 2 Behördensiegel mit Q-Siegel

## Ausgangslage »Papier ist geduldig«

Obwohl es sich viele Bürger, Unternehmen und Verwaltungen wünschen, letztendlich wird für die meisten Verwaltungsvorgänge noch auf papiergebundene Bescheide gesetzt, obwohl die elektronische Form ebenso zulässig ist (§ 37 Verwaltungsverfahrensgesetz) und die Abwicklung hierüber deutlich vereinfacht wäre und Wartezeiten verkürzen würde. Auch Fälschungen solcher Schreiben könnten über entsprechende digitale Möglichkeiten verringert werden.

Dies zeigt sich insbesondere an folgendem Beispiel: Woran erkennt man die Echtheit eines behördlichen Schreibens? Wenn die Dokumente auf Papier vorliegen, dann ergibt sich die Echtheit oft aus dem Briefkopf, aus einem behördlichen Siegel und aus dem Briefumschlag, in dem sie enthalten sind. Sowohl Briefkopfstempel als auch entsprechende Umschläge können aber mit sehr wenig Geschick professionell nachgemacht werden.

Von daher wurden bereits 2003 im Verwaltungsrecht die qualifizierte elektronische Signatur aufgenommen, die elektronische Dokumente vor unbemerkter Manipulation schützt und Auskunft über den Unterzeichner gibt. Behörden konnten sich jedoch nie wirklich die Vorteile der qualifizierten elektronischen Signatur erschließen, da in der Vergangenheit in den häufigsten Anwendungsfeldern viele Mitarbeiter mit einer Signaturkarte ausgestattet werden mussten, an Stelle eines zentralen digitalen Signaturdienstes analog dem Amtssiegel. Dort, wo die Signaturkarten dann doch, auch in der Außenwirkung, zum Einsatz kamen, wurden die Dokumente mit einer persönlichen qualifizierten Unterschrift des Bearbeiters versehen. Sobald es eine Änderung in der Position gab, z.B. Ausscheiden, Versetzung, Umbenennung der Dienststelle, bestand die Notwendigkeit der Sperrung des Zertifikats sowie der Neubeantragung und -ausstellung.

Da viele Bescheide aber gar nicht die persönliche Unterschrift benötigen, war das »alte« Stempeln von Papier einfach leichter.

## Lösung »Elektronisches Behördensiegel«

Mit dem Q-Siegel könnten sehr viel mehr behördliche Bescheide elektronisch bereitgestellt oder verschickt werden als bisher. Denn zu einer der wichtigsten Maßgaben von Verwaltungsakten gehört es, dass sie die ausstellende Behörde erkennen lassen müssen. So lässt sich für die öffentlichen Verwaltungen insbesondere bei Massenverfahren wie Steuer- oder Rentenbescheiden eine Menge Geld einsparen[5]. Der Empfänger kann beispielsweise ein gesiegeltes PDF-Dokument mit dem Adobe Reader oder anderen frei verfügbaren Tools, wie dem digiSeal reader, öffnen und erhält sofort ein verlässliches Prüfergebnis (»Grüner Haken« oder »Rotes Ausrufezeichen«).

5 Vgl: Hölters/Henke, JurPC Web-Dok. 44/2017, Abs. 4f.: Verwendungsmöglichkeiten und Nutzen des qualifizierten elektronischen Siegels, abgerufen am 22.07.2020: ↗www.jurpc.de/jurpc/show?id=20170044

# 3 Digitale Zeugnisse / Belege / Protokolle mit Q-Siegel

## Ausgangslage »Papierdokumente«

Ein in festlichem Rahmen überreichtes oder gar eingerahmtes und aufgehängtes Zeugnis mag manchen mit Stolz erfüllen – aber wenn man bei einem neuen Arbeitgeber seine bisherigen Qualifikationen darlegen möchte, kommt es vor allem auf einfache und sichere Übermittlungsmöglichkeiten an. Gefälschte Zeugnisse bilden in der täglichen Bewerbungspraxis leider keine Seltenheit. Es gibt sogar Internet-Portale, bei denen man ein Zeugnis seiner Wahl bestellen kann – ohne eigene Leistung, dafür freilich gegen einen gewissen Obolus.

Presseberichte über Fällen des Bewerbungsbetrugs oder von Personen, die unberechtigt akademische Titel in der Öffentlichkeit führen zeigen die praktischen Auswirkungen. Das Phänomen zieht sich dabei durch alle Bewerbergruppen, ob es der Bewerber für einen Ausbildungsplatz ist oder der Studienabbrecher, der sich selbst das die Hochschulabschlüsse und die Promotionsurkunde schreibt. Es sind nicht immer derart spektakuläre Fälle, dass ein Betrüger unberechtigter Weise als Arzt[6], Lehrer[7] oder Pilot tätig wird, aber es stellt in jedem Fall eine Straftat dar und das Vortäuschen falscher Tatsachen.

Allen Dokumenten ist gemeinsam, dass sie originär auf Papier erstellt werden. Auf den ersten Blick ist es meistens nicht möglich, eine Vollfälschung zu erkennen. Mittlerweise erfolgt häufig nur noch die Vorlage von Kopien, z.B. bei der Onlinebewerbung und der zukünftige Arbeitgeber verzichtet auf die Vorlage der Originale. Nur Nachfragen bei der dokumentenausgebenden Stelle können zur Aufdeckung des Betrugs führen.

Die Fälschung von Wartungsprotokollen[8] technischer Infrastrukturen oder Verkehrsmitteln können erhebliches Schadenspotential mit sich führen. Im Skandal um gefälschte Wartungsprotokoll[9] bei der Berliner S-Bahn schätzte die Deutsche Bahn zu Beginn der Affäre das Schadenspotential auf bis zu 200 Millionen Euro.

Aber es geht nicht nur um Zeugnisse oder Protokolle. Gerade im Rahmen der Pandemie zeigte sich der Bedarf, auch so simple Dokumente wie »Hörerscheine« an Universitäten zu digitalisieren und zu siegeln. Damit würden Studenten auf einfache, aber sichere und verbindliche Art und Weise Leistungsnachweise erhalten.

6 ↗www.aerzteblatt.de/archiv/48041

7 ↗www.lto.de/recht/nachrichten/n/ag-kiel-kurioses-lehrerin-urkundenfaelschung-betrug

8 ↗https://de.wikipedia.org/wiki/L%C3%ADneas_A%C3%A9reas_Nacionales

9 ↗www.t-online.de/nachrichten/panorama/buntes-kurioses/id_19941724/berlin-wartungsprotokolle-der-s-bahnen-waren-gefaelscht.html

## Lösung »Gesiegeltes PDF-Zeugnis«

Gegen die Veränderung eines elektronischen Dokuments (Zeugnis, Protokoll etc.) hilft ein elektronisches Siegel der Institution (wie z.B. der Schule, der Universität oder der Firma), die die Bescheinigung ausgestellt hat und sich damit für die Echtheit verbürgt.

Im Bildungsbereich wären die folgenden Szenarien denkbar: Ausbildungszeugnisse, die die Industrie- und Handelskammern oder die Handwerkskammern ausstellen, könnten in elektronischer Form mit einem Siegel der Kammer abgesichert werden. Auf Sachkundenachweise, die die IHK ausstellt, ließe sich das Verfahren ebenfalls anwenden. Nicht nur bei Bewerbungsverfahren könnten solche elektronisch gesiegelten Zeugnisse die Vertrauenswürdigkeit erhöhen. Es wäre auch zum Beispiel möglich, Zulassungsverfahren an Hochschulen komplett elektronisch abzuwickeln. Umständliche Parallelverfahren, wie zum Beispiel nach der Online-Einschreibung noch ein Abiturzeugnis beglaubigen zu lassen und in Papier nachzureichen, würden dann der Vergangenheit angehören. Denn die amtliche Beglaubigung ist im elektronisch gesiegelten Zeugnis quasi immer schon integriert und es bedarf zukünftig keiner Echtheitsrecherche mehr beim Aussteller.

Diese Verfahren sind auf alle Bereiche in der Wirtschaft und Verwaltung übertragbar, in denen in irgendeiner Art und Weise etwas bescheinigt werden muss. Die Prüfung der gesiegelten Bescheinigung durch den Empfänger oder unabhängige Dritte erfolgt beispielsweise einfach mit dem Adobe Reader oder sonstigen freien Tools.

## Erforderliche Maßnahmen und Erfolgsfaktoren

Um Q-Siegel in der deutschen Behörden- und Unternehmenswelt zu etablieren, ist der Boden europaweit bestellt. Dank eIDAS-Verordnung und den Vorbereitungen der Vertrauensdiensteanbieter stehen der Verbreitung der neuen organisationsbezogenen Zertifikate keine Hindernisse im Weg. Die Attraktivität dieses neuen Produkts für deutsche Anwender ergibt sich dadurch aber noch nicht von selbst: Nicht alles, was an Einsatzmöglichkeiten für elektronische Siegel denkbar wäre, ist heute allerdings auch schon rechtlich zulässig. Aus diesem Grund muss auch der deutsche Gesetzgeber seinen Beitrag leisten. Hier geht es nicht nur um einen symbolischen »Ritterschlag«, sondern auch darum, die elektronischen Siegel in Einzelgesetzen und -verordnungen für konkrete Verwaltungsakte als geeignet, zulässig oder vielleicht sogar verbindlich zu erklären.

## Behördliche Bescheide und Dokumente

- **E-Government-Gesetz des Bundes** (§ 2, § 6, § 7): Behörden sollten verpflichtet werden, elektronische Dokumente auch mit elektronischem Siegel (nicht nur mit qualifizierter elektronischer Signatur) entgegennehmen zu können.

- **Verwaltungsverfahrensgesetz** (§ 3a): Behörden sollten neben der qualifizierten elektronischen Signatur auch das qualifizierte Siegel nutzen dürfen.

- **Verwaltungsverfahrensgesetz** (§ 33): Schon in der jetzigen Form schreibt das Gesetz vor, dass jede Behörde von Urkunden, die sie selbst gefertigt hat, elektronische Dokumente und elektronische Beglaubigungen ausfertigen können soll. Was läge hier näher als die Maßgabe, eine solche Abschrift/Beglaubigung auch mit einem qualifizierten elektronischen Siegel abzusichern?

- **Verwaltungsverfahrensgesetz** (§ 37): Ausdrücklich ist schon jetzt festgeschrieben, dass auch ein elektronischer Verwaltungsakt die erlassende Behörde erkennen lassen muss. Genau diese Anforderung erfüllt das elektronische Siegel perfekt und sollte darum folgerichtig hier auch Erwähnung finden.

## Zeugnisse

Verankerung in allen entsprechenden Normen für die Aussteller oder an zentraler Stelle (BGB und VwVfG): Aussteller von digitalen Zeugnisse und Bescheinigungen, müssen diese qualifiziert elektronisch signieren oder siegeln, sofern die Dokumente für die Nutzung im Rechtsverkehr bestimmt sind.

# 4 Sichere Behördenwebseiten in einem unsicheren Netz

## Ausgangslage »Gefälschte Webseiten, z.B. Corona-Hilfeantragsseiten«

Im April 2020 musste das Land Nordrhein-Westfalen die Internet-Antragstellung für die Corona-Soforthilfen kurzfristig stoppen. Betrüger hatten Fake-Webseiten gebaut und die Antragsteller dorthin umgeleitet. Ahnungslos gaben viele Antragsteller ihre Daten preis, darunter die Registernummer der Firma, Steuernummern, Personalausweisdaten und Kontoverbindungen. Mit diesen Daten stellten die Cyberkriminellen dann auf den Originalseiten Anträge und kassierten Gelder ab. Der Westdeutsche Rundfunk (WDR) berichtete von über 90 Fake-Webseiten; zwischen 3.500 und 4.000 Antragsteller waren vom Datenmissbrauch betroffen.

Was sind die Lehren aus diesem Vorfall? Nur wenn Personen sich zweifelsfrei elektronisch identifizieren können und eine Webseite als echt zu erkennen ist, entsteht ein Vertrauensraum für elektronische Interaktionen und Transaktionen.

## Lösung »Absicherung von Webseiten durch qualifizierte Webseitenzertifikate (QWAC)«

**1. Absicherung von Verwaltungswebseiten**

Wer schon einmal eine Reise außerhalb der EU vorbereitet hat und für sein Zielland im Vorfeld des Reiseantritts ein Visum benötigte, wird das Problem kennen. Welche Webseite ist eigentlich die Richtige, auf der offiziell der Antrag vorbereitet werden kann? Es gibt häufig neben der einen wirklichen Webseite, viele Agenturwebseiten bzw. Fake-Webseiten, die ausschließlich an der Zahlung einer Gebühr interessiert sind.

Aber auch innerhalb der EU ist es häufig nicht so eindeutig, ob die aufgerufene Domain tatsächlich die Webseite der Behörde darstellt. Das beste Beispiel hierfür sind die Corona-Hilfe-Antragsseiten[10]. Hier ist ein QWAC ein wichtiger Anker, der neben der Verschlüsselung auch die wahre Identität des Webseiteninhabers offenlegt und somit Vertrauen schafft. Davon profitieren alle Einwohner Deutschlands und der EU.

**2. Absicherung von behördlichen Diensten**

Momentan laufen intensive Anstrengungen, die unbedingt notwendige digitale Vernetzung von Registern, Realität werden zu lassen. Eine mögliche Umsetzung der Vernetzung kann über die QWACs erfolgen, geben sie doch eindeutig Auskunft darüber, welches Register sie vertreten. QWACs können so ermöglichen, dass auch Register miteinander Daten austauschen können, die noch nie zuvor mit einander kommuniziert haben. In der Praxis würde jedes Register ein eigenes QWAC besitzen, welches es als Register ausweist. Sollen zwei Register miteinander Daten austauschen, dann würden sie sich gegenseitig mit Hilfe ihrer QWACs ausweisen und im Anschluss über vorher definierte Protokolle kommunizieren. Ein Dienst, der kein Register ist, würde niemals ein QWAC erhalten mit dem Eintrag, ein Register zu sein.

10 ↗www.polizei-beratung.de/startseite-und-aktionen/corona-straftaten/betrug-im-internet

Gleiches kann für Dienste gelten, die Open Data bereitstellen. Auf dieser Weise können Anwendungen ihren Informationsquellen vertrauen, Datenqualität und Datenherkunft kann belegt werden. Eine Verwendung des QWAC würde es auch ermöglichen, dass die behördlich bereitgestellten Dienste nicht nur in Deutschland sondern in ganz Europa nutzbar wären.

**3. Payment Service Directive 2 (PSD2)**

Ein sehr konkretes und in seiner Umsetzung weit fortgeschrittliches Beispiel wie zukünftig QWACs grenzüberschreibend innerhalb Europas eingesetzt werden, stellen die Anforderungen der PSD 2 dar. Seit September 2019 werden kontoführende Banken und Fintechs (sogenannte Third Party Payment Provider (TPP)) europaweit verpflichtet werden, für die Absicherung ihres Datenaustausches untereinander, QWACs einzusetzen. Dies ermöglicht den FinTechs Europas neue und DSGVO konforme Geschäftsmodelle und besseren Service für Bankkunden. Eine Erweiterung in den Versicherungsbereich wäre sehr leicht möglich und würde den aufstrebenden InsureTechs ebenfalls einen Schub an neuen Geschäftsmodellen ermöglichen.

# 5 Harmonisierung der Anerkennung des Videoidentifizierungsverfahren als Fernidentifizierungsverfahrens

## Ausgangslage »Modernere Identifikationsverfahren nötig«

Mit der Anwendung der Regelungen aus dem Kapitel III der eIDAS-Verordnung kann das Videoidentifizierungsverfahren für die Beantragung von qualifizierten Zertifikaten gemäß Artikel 24 Absatz 1 Unterabsatz 2 Buchstabe d Satz 1 der Verordnung (EU) Nr. 910/2014 eingesetzt werden. Erste Vertrauensdienste nutzten diese Möglichkeiten in Deutschland bereits seit 2017[11]. Heute werden in mehreren EU-Mitgliedsstaaten Videoidentifizierungsverfahren mit »Künstlicher Intelligenz« (KI) für die Beantragung qualifizierter Zertifikate eingesetzt. Auf nationaler, deutscherer Ebene werden mit Ausnahmegenehmigung auch Videoidentifizierungsverfahren mit KI eingesetzt.[12] Damit sind bereits heute Ungleichheiten in den Anforderungen der Videoidentifizierungsverfahren, nicht nur auf europäischer, sondern sogar auf nationaler Ebene festgeschrieben und daraus resultierende Wettbewerbsnachteile für Vertrauensdiensteanbieter eingetreten.

Eine Vergleichbarkeit der Qualität der Dienstleistung der Vertrauensdiensteanbieter kann unter diesen Gegebenheiten ist in Frage gestellt, was dem Gedanken der eIDAS widerspricht. Beispielsweise ist der Standort Deutschland für einen qualifizierten Vertrauensdiensteanbieter ist zu einen entscheidenden Wettbewerbsnachteil geworden.

## Lösung »Harmonisierung von Videoidentifikationsverfahren«

Eine Harmonisierung der Anerkennung des Videoidentifizierungsverfahrens als Fernidentifizierungsverfahren muss auf europäischer Ebene erfolgen. Es hat sich erwiesen, dass die bisherigen Regelungen auf nationaler Ebene zu einem starken Ungleichgewicht in dem möglichen Dienstleistungsangebot der nationalen Vertrauensdiensteanbieter führen.

Standardisierungsorganisationen wie ETSI sind hervorragend geeignet, um die gemeinsame, europäische, technischen Rahmenbedingungen zu definieren. Dies kann auch für das Videoidentifizierungsverfahren erfolgen.

Diese Maßnahmen stellen sicher, dass die Nutzung des Videoidentifizierungsverfahrens europaweit einheitlich möglich ist und eine Differenzierung durch das Angebot sowie die Qualität der Leistungserbringung nicht aber durch den Standort erfolgt.

11 2018 wurde auf Basis des deutschen Vertrauensdienstegesetzes (VDG) der Erlass einer Erstverfügung, die die Anwendung der Fernidentifikation mittels Videoidentifizierungsverfahrens regelt (Erstverfügung i.S.d. § 11 Abs. 1 VDG / Nationale Anerkennung alternativer Identifizierungsmethoden).

12 Dies erfolgt zwar nicht für die Beantragung qualifizierter Zertifikate, aber dient dem Nachweis der persönlichen Vor-Ort-Identifizierung.

# 6 Gesetzliche Anpassungen notwendig

## Ausgangslage »Digitalisierungsbehinderung durch fehlende Unterstützung der eIDAS-Mittel«

Die Werkzeuge für diese Digitalisierung sind vorhanden. Gleiches gilt für den benötigten rechtlichen Rahmen. Dieser Rahmen ist durch die EU-Verordnung in allen Mitgliedstaaten gleichermaßen wirksam.

In der Breite werden allerdings die in der Verordnung definierten eIDAS-Werkzeuge noch nicht genügend eingesetzt.

## Lösung »Evaluation und Ratspräsidentschaft nutzen und eIDAS-Mittel stärker gesetzlich berücksichtigen«

Eines ist sicher: Die rasche Umsetzung der EU-Verordnung ist ein wichtiger Baustein, um die Folgen einer erneuten Krise abzufedern. Die anstehende eIDAS-Evaluation durch die EU-Kommission wird Aufmerksamkeit schaffen. Zusätzlich bietet die deutsche Präsidentschaft des EU-Rats im zweiten Halbjahr 2020 eine gute Möglichkeit, eIDAS auf die politische Agenda zu setzen. Auf jeden Fall muss für alle Akteure – Marktanbieter, Behörden und Politik – die Devise gelten: Mehr eIDAS wagen!

Wichtig ist nun vor allem, dass die Nutzung der eIDAS Werkzeuge in der Breite gefördert wird und neben dem Einsatz im öffentlichen Sektor auch Anwendungen in der Privatwirtschaft flächendeckend eingesetzt werden. Hierbei muss insbesondere der breite Anwendungsbereich und die Mehrwerte für den täglichen Gebrauch stärker in den Vordergrund gestellt werden. Ein weiterer wichtiger Impuls wäre die Förderung von eIDAS als Regelung für Single-Sign-on Verfahren. Mehr Reichweite und Harmonisierung des europäischen Marktes kann durch die Einführung einer obligatorischen Akzeptanz und Einführung in Dienste und Apps erreicht werden:  Damit sich europäisches ID System durchsetzt und Relevanz beim Nutzer geschaffen wird, ist eine **Ausweitung der täglichen Nutzung durch die Einbeziehung von Anwendungsmöglichkeiten auf Identifizierung und / oder Authentifizierung in allen Vertrauensniveaus notwendig**.

Gerade Verwaltungen können dazu beitragen, das »Henne-Ei-Problem« zu lösen. Viel wäre bereits erreicht, wenn Behörden flächendeckend eIDAS-Werkzeuge und die Online-Ausweisfunktion des Personalausweises akzeptierten[13]. Einen großen Schub kann die Politik geben: Eine aktuelle Studie der Bundesdruckerei zur eIDAS-Verordnung kommt zu dem Schluss, dass die eIDAS-Vertrauensdienste gesetzlich stärker zu berücksichtigen sind[14]. Beispielsweise sieht das Verwaltungsverfahrensgesetz momentan nur den Einsatz einer qualifizierten elektronischen Signatur vor. Werden diese Vorgaben auf qualifizierte elektronische Siegel erweitert, können Behörden in Zukunft Beglaubigungen von Dokumenten noch einfacher ausstellen. Die Studie schlägt zudem vor, das E-Government-Gesetz um eine Regelung zu ergänzen, nach der die eIDAS-Werkzeuge von Behörden genutzt werden müssen. Ministerien, Ämter und Co. könnten dann nicht nur elektronische Dokumente mit der qualifizierten elektronischen Signatur, sondern auch mit Siegel annehmen.

13 Siehe auch hier: ↗**www.bitkom.org/Presse/Presseinformation/10-Jahre-elektronischer-Personalausweis-Grosses-Potenzial-kaum-genutzt**

14 ↗**www.bundesdruckerei.de/de/Newsroom/Pressemitteilungen/Bundesdruckerei-Studie-zur-eIDAS-Verordnung**

Bitkom vertritt mehr als 2.700 Unternehmen der digitalen Wirtschaft, davon gut 2.000 Direktmitglieder. Sie erzielen allein mit IT- und Telekommunikationsleistungen jährlich Umsätze von 190 Milliarden Euro, darunter Exporte in Höhe von 50 Milliarden Euro. Die Bitkom-Mitglieder beschäftigen in Deutschland mehr als 2 Millionen Mitarbeiterinnen und Mitarbeiter. Zu den Mitgliedern zählen mehr als 1.000 Mittelständler, über 500 Startups und nahezu alle Global Player. Sie bieten Software, IT-Services, Telekommunikations- oder Internetdienste an, stellen Geräte und Bauteile her, sind im Bereich der digitalen Medien tätig oder in anderer Weise Teil der digitalen Wirtschaft. 80 Prozent der Unternehmen haben ihren Hauptsitz in Deutschland, jeweils 8 Prozent kommen aus Europa und den USA, 4 Prozent aus anderen Regionen. Bitkom fördert und treibt die digitale Transformation der deutschen Wirtschaft und setzt sich für eine breite gesellschaftliche Teilhabe an den digitalen Entwicklungen ein. Ziel ist es, Deutschland zu einem weltweit führenden Digitalstandort zu machen.

**Bundesverband Informationswirtschaft,**
**Telekommunikation und neue Medien e.V.**

Albrechtstraße 10
10117 Berlin
**T** 030 27576-0
**F** 030 27576-400
bitkom@bitkom.org
**www.bitkom.org**