



WHITEPAPER

Die eIDAS-Verordnung – die Basis für ein starkes digitales Europa

Effizientere Prozesse, geringere Kosten, mehr Kundenzufriedenheit



Management Summary

Der digitale Binnenmarkt hat das Potenzial, jährlich Wachstumsimpulse in zweistelliger Milliardenhöhe zu generieren und Hunderttausende neue Arbeitsplätze in Europa zu schaffen.¹ Voraussetzung dafür sind sichere und vertrauenswürdige elektronische Geschäftsprozesse zwischen Unternehmen, Behörden und Bürgern im gesamten EU-Raum.



Antonello Giacomelli, italienischer Staatssekretär für Kommunikation, der das Gesetz im Rahmen der italienischen Ratspräsidentschaft digital signierte.

„Die eIDAS-Verordnung ist der erste konkrete Schritt in Richtung digitaler Binnenmarkt.“

Dies zu erreichen, ist das Ziel der am 1. September 2014 in Kraft getretenen „Verordnung über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt“ (eIDAS-Verordnung)². Sie legt den einheitlichen, europaweit gültigen Rechtsrahmen für den elektronischen Identitätsnachweis und für Vertrauensdienste – wie zum Beispiel elektronische Signaturen, Siegel und Zeitstempel – fest. Dabei verfolgt sie einen für Innovationen offenen Ansatz und ist technologie-neutral.

Im Bereich der elektronischen Identifizierung setzt die Verordnung auf eine gegenseitige Anerkennung der verschiedenen nationalen eID-Systeme. Bei den Vertrauensdiensten wurden neue, vereinfachte Werkzeuge definiert und die Voraussetzungen für ein europaweit vereinheitlichtes Sicherheitsniveau geschaffen. Zukünftig können elektronische Transaktionen EU-weit effizient und rechtsverbindlich durchgeführt werden. Weiterhin erleichtert die eIDAS-Verordnung die Nutzung elektronischer Signaturen z. B. durch die Möglichkeit, den Signaturprozess über eine Fernsignatur standortunabhängig auszulösen. Das neu eingeführte elektronische Siegel ist nicht personenbezogen, sondern auf eine Organisation ausgestellt. Es bestätigt den Ursprung und die Unversehrtheit elektronischer Dokumente.

¹ Jean-Claude Juncker: Ein neuer Start für Europa, 15. Juli 2014 (PDF).

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 (PDF).

Die derzeit gültige EU-Signaturrechtlinie (1999/93/EG) wird durch die eIDAS-Verordnung abgelöst. Nationale Regelungen können bestehen bleiben, wenn sie der eIDAS-Verordnung nicht widersprechen. Es ist allerdings zu erwarten, dass das deutsche Signaturgesetz entsprechend angepasst wird. Anbieter von sogenannten qualifizierten Vertrauensdiensten unterliegen strengen rechtlichen und sicherheitstechnischen Anforderungen. Öffentlich einsehbare Vertrauenslisten und das EU-Vertrauenssiegel stellen sicher, dass der Dienstleister rechtskonforme Vertrauensdienste anbietet. Ein wichtiger Meilenstein auf dem Weg zur praktischen Umsetzung der eIDAS-Verordnung ist der 1. Juli 2016. Ab diesem Termin können Vertrauensdienste angeboten werden. Damit ist der Weg frei für den digitalen Binnenmarkt Europa – mit über 400 Millionen Nutzern.

Europa im Jahr 2016

Raivo, Geschäftsführer eines estnischen Kleinunternehmens, ist frustriert. Kürzlich hat er am öffentlichen Ausschreibungsverfahren einer portugiesischen Stadtverwaltung teilgenommen – ein umständlicher, zeitaufwändiger Prozess. Seine Mitarbeiter mussten Vergebendokumente ausfüllen, ausdrucken und handschriftlich ergänzen, bevor diese, mit der persönlichen Unterschrift des Geschäftsführers versehen, endlich versendet werden konnten. Auf Nachfrage stellte sich aber leider nach einigen Wochen heraus, dass die Unterlagen auf dem Postweg niemals beim Empfänger eingetroffen waren. Eine erneute Abgabe des Angebots innerhalb der verbleibenden Bewerbungsfrist war zeitlich nicht mehr zu schaffen.

Zur gleichen Zeit: Herr Meyer, Mitglied des Managementteams der Hedracell AG, ist schon einen Schritt weiter: Konnte er doch für sein Unternehmen einen Großauftrag für Maschinenbaukomponenten gewinnen. Für die effiziente Abwicklung hat ihm die Bank bereits den Kredit für zusätzliche Investitionen zugesagt. Leider gerät die Auszahlung der Kreditsumme ins Stocken, da wichtige Dokumente der Bank auf dem Postweg nicht rechtzeitig eintreffen. Einer Konventionalstrafe wegen Lieferverzugs entgeht das Unternehmen nur durch das Engagement und den Einsatz seiner Mitarbeiter.



1. WARUM DIE eIDAS-VERORDNUNG SO WICHTIG IST

Großes Potenzial

Der 1993 in Kraft getretene „analoge“ Europäische Binnenmarkt hat für große Wachstums- und Beschäftigungsimpulse gesorgt. Allein in Deutschland stieg durch das wirtschaftliche Zusammenwachsen Europas das Bruttoinlandsprodukt im Zeitraum 1992 bis 2012 um durchschnittlich 37 Milliarden Euro pro Jahr.³ Knapp 60 Prozent der deutschen Ausfuhren gehen in EU-Länder. Deutschland gehört zu den Gewinnern der europäischen Integration und hat ein ureigenes Interesse an einer weiteren Entwicklung des Binnenmarkts.

Ein weiterer zentraler Integrationsschritt ist die Etablierung eines digitalen Binnenmarkts, der neue Wachstumsmöglichkeiten bietet, die Wettbewerbsfähigkeit europäischer Unternehmen verbessert und den Verbrauchern in der EU Kosteneinsparungen und ein erweitertes Online-Angebot verspricht. Welches Potenzial darauf wartet, gehoben zu werden, zeigt der derzeitige Stand des digitalen Markts in Europa.

QUELLE:

EU-Kommission: Factsheet on Digital Single Market (PDF).

3 Prognos AG: 20 Jahre Binnenmarkt – Wachstumseffekte der zunehmenden europäischen Integration, 2014.

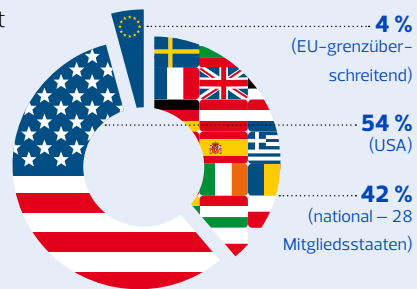
4 Europäische Kommission: Strategie für einen digitalen Binnenmarkt für Europa, COM(2015) 192 final.

5 Siehe auch Pressemitteilung der Europäischen Kommission: Die Kommission ebnet den Weg für die Digitalisierung der europäischen Industrie.

Status quo des digitalen, europäischen Markts

Der heutige digitale Markt umfasst nationale Online-Dienste (42 %) sowie in den USA angesiedelte Online-Dienste (54 %).

Grenzübergreifende Online-Dienste in der EU machen nur 4 % aus.



Die Errichtung eines digitalen Binnenmarkts ist für die EU-Kommission deshalb eine ihrer Prioritäten.⁴ Wie dieser digitale Binnenmarkt in der Praxis aussieht, ist klar definiert:



Europäische Kommission: Strategie für einen digitalen Binnenmarkt für Europa⁵

„In einem digitalen Binnenmarkt ... können Privatpersonen und Unternehmen ... auf der Grundlage hoher Verbraucher- und Datenschutzstandards ungeachtet ihrer Staatsangehörigkeit bzw. ihres Wohn- und Geschäftssitzes nahtlos Online-Aktivitäten nachgehen und Internet-Anwendungen nutzen.“

Fundament schaffen

Der digitale Binnenmarkt ist auf einheitliche, rechtlich anerkannte Kommunikationswege im Online-Verkehr angewiesen. Unabdingbar sind Systeme und Lösungen für sichere elektronische Transaktionen und zum Identitätsnachweis, die im gesamten EU-Raum eingesetzt werden können.

Doch genau in diesem Bereich gab es in der Vergangenheit eine Vielzahl von Barrieren und Hemmnissen. So existieren in den EU-Staaten unterschiedliche technische und fachliche Standards sowie oftmals nationale Regelungen, die mangels Interoperabilität nicht grenzübergreifend angewandt werden können.



Antworten gesucht

- Wie weisen sich Mitarbeiter deutscher Unternehmen elektronisch innerhalb der EU aus?
- Wie stellen Unternehmen EU-weit Dokumente nachprüfbar und sicher auf elektronischem Wege zu?
- Wie können Online-Anbieter im EU Raum die Vertrauenswürdigkeit ihrer Website nachweisen?
- Wie unterschreiben Unternehmen im gesamten EU-Raum elektronisch Verträge, Anträge und Formulare rechtlich verbindlich?
- Wie sorgen Unternehmen im elektronischen Geschäftsverkehr mit Behörden und anderen EU-Firmen dafür, dass die zugestellten Dokumente echt und unverfälscht sind?

Neben der Überwindung funktionaler Barrieren sind für die EU-Kommission Vertrauensbildung und Rechtssicherheit von besonderer Bedeutung.⁶



eIDAS-Verordnung, Erwägungsgrund (1)

„Mangelndes Vertrauen führt dazu, dass Verbraucher, Unternehmen und öffentliche Verwaltungen nur zögerlich elektronische Transaktionen durchführen ..., vor allem, wenn sie die Befürchtung hegen, dass es an Rechtssicherheit mangelt.“

Das soll sich mit der eIDAS-Verordnung ändern. Sie schafft den rechtlichen Rahmen für eine grenzüberschreitende Anerkennung elektronischer Identifizierungssysteme und Vertrauensdienste, wie zum Beispiel elektronischer Signaturen, Siegel und Zeitstempel. Dabei stellt sie ihre Interoperabilität, Harmonisierung und rechtliche Wirksamkeit sicher.

⁶ Verordnung (EU) Nr. 910/2014, Erwägungsgrund (1).

2. DIE eIDAS-VERORDNUNG: GRUNDLAGEN UND ZIELE

Die „Verordnung über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt“ der Europäischen Union (eIDAS) ist seit dem 17. September 2014 geltendes Recht in allen 28 Mitgliedsstaaten. Sie kann von Island, Liechtenstein und Norwegen adaptiert werden. Durch die Verordnung wird die EU-Signaturrechtlinie (1999/93/EG) aufgehoben.

Die eIDAS-Verordnung bildet somit das regulatorische Dach für die Umsetzung sicherer und vertrauenswürdiger elektronischer Geschäftsprozesse in Europa. Nationale Regelungen werden zwar nicht außer Kraft gesetzt, sie dürfen aber der eIDAS-Verordnung nicht widersprechen oder müssen sich auf spezifische nationale Anwendungen beschränken. Das deutsche Signaturgesetz aus dem Jahr 2011 muss entsprechend angepasst werden. Die Europäische Kommission hat den Auftrag erteilt, verbindliche rechtliche Regelungen zu bestimmen sowie technische Normen und Standards zu definieren. Für die Umsetzung zeichnen die beiden europäischen Standardisierungsorganisationen ETSI (European Telecommunications Standards Institute) und CEN (European Committee for Standardization) verantwortlich.⁷

GUT ZU WISSEN

Verordnung und Richtlinien

Verordnungen sind vergleichbar mit europäischen Gesetzen, die in der Europäischen Union sofort nach der Verabschiedung in jedem Mitgliedsstaat gültig sind. Nationalstaaten dürfen zu den geregelten Bereichen keine eigenen Rechtsakte erlassen, darüber hinaus darf die Verordnung von keinem Land verändert werden.

Richtlinien sind dagegen Rechtssetzungen und verpflichten die Mitgliedsstaaten, bestimmte Ziele innerhalb einer definierten Zeit umzusetzen. Dabei sind Wege und Methoden zur Zielerreichung jedem einzelnen Nationalstaat überlassen.⁸

⁷ Christoph Thiel / Arno Fiedler: „Der grenzenlose Binnenmarkt“ in: Zeitschrift „Datenschutz und Datensicherheit“ 01/2013, S. 14–19. www.dud.de.

⁸ Europäische Union, offizielle Website: www.europa.eu.

Die eIDAS-Verordnung gibt Antworten auf die zentrale Frage: „Wie lässt sich der digitale Binnenmarkt realisieren?“. Zwei übergeordnete Ziele stehen dabei im Mittelpunkt:

- Bürger und Unternehmen müssen in der Lage sein, ihre nationalen elektronischen Identifikationsmittel (eIDs) für Online-Dienste in anderen EU-Ländern zu nutzen.
- Barrieren und Hemmnisse bezüglich der grenzüberschreitenden Nutzung von elektronischen Signaturen und anderen Vertrauensdiensten müssen abgebaut werden. Dabei ist sicherzustellen, dass elektronische Vertrauensdienste dieselbe rechtliche Anerkennung erhalten wie tradierte papierbezogene Prozesse.

GUT ZU WISSEN

Vertrauensdienst

Ein Vertrauensdienst ist laut eIDAS-Verordnung, Artikel 3 (16), ein elektronischer Dienst, der in der Regel gegen Entgelt erbracht wird und unter anderem Folgendes umfasst: Erstellung, Überprüfung und Validierung von elektronischen Signaturen, Siegeln oder Zeitstempeln und die Überprüfung und Validierung von Zertifikaten für die Website-Authentifizierung. Ein qualifizierter Vertrauensdienst ist ein Vertrauensdienst, der die einschlägigen Anforderungen der eIDAS-Verordnung erfüllt, Artikel 3 (17).

Die wichtigsten Bausteine für die Umsetzung der Zielvorgaben sind hier aufgeführt:

Bausteine der eIDAS-Verordnung



Elektronische ID

- Einheitliche Regeln für die Anerkennung der verschiedenen elektronischen Identifizierungssysteme in Europa.
- Technische Interoperabilität der elektronischen Identifizierungssysteme.
- Gegenseitige Anerkennung der elektronischen Identifizierungsmittel.



Vertrauensdienste

- Festlegung eines Rechtsrahmens für die betroffenen Dienste.
- Vereinfachung bestehender Verfahren und Etablierung neuer Methoden.
- Abgestimmte Formate für Signaturen, Siegel, Zeitstempel, Website-Zertifikate, E-Mail-Zustelldienste und Archivdienste.
- Gegenseitige, europaweite Anerkennung der Vertrauensdienste.
- Einheitliche Vorgaben und Regelungen für die Vertrauensdiensteanbieter (VDA).

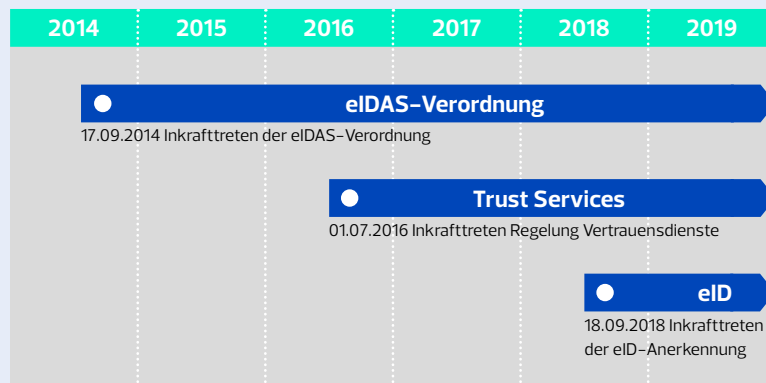


Neelie Kroes, ehemalige Kommissarin für die Digitale Agenda, bringt die Grundlagen und Zielvorstellungen der eIDAS-Verordnung mit folgendem Zitat auf den Punkt:

„Die eIDAS-Verordnung basiert auf Interoperabilität, Risikomanagement und auf Prinzipien wie Transparenz, Zuverlässigkeit und Technologieneutralität. Aber vor allem ermöglicht es viele neue Transaktionen und Interaktionen über die Grenzen hinweg. Das ist ein wesentliches Element, damit der europäische Binnenmarkt auch im digitalen Zeitalter richtig funktioniert.“

Ein bedeutsamer Meilenstein für die eIDAS-Verordnung ist der 1. Juli 2016. Ab diesem Termin löst die eIDAS-Verordnung die EU-Signaturrechtlinie (1999/93/EG) ab und es können qualifizierte Vertrauensdienste angeboten werden. Ab dem 1. Juli 2017 müssen die in der Verordnung definierten Vertrauensdienste umgesetzt sein. Zur gegenseitigen Anerkennung der elektronischen Identifizierungssysteme sind die EU-Staaten ab dem 18. September 2018 verpflichtet.

Allgemeine Roadmap der eIDAS-Verordnung



QUELLE:
 EU-Kommission, Statement: New EU regulation on eidentification (eIDAS) launched by Neelie Kroes

3. DIE eIDAS-VERORDNUNG: INHALTE

Die Regelungsinhalte der eIDAS-Verordnung teilen sich in zwei große Bereiche:



3.1 Elektronische Identifizierung

Herausforderung

Die elektronischen Identifizierungsmittel der einzelnen EU-Staaten, wie zum Beispiel der elektronische Personalausweis in Deutschland, sind nur national einsetzbar, da eine EU-weite Anerkennung fehlt.⁹ So existieren mittlerweile in sieben EU-Staaten elektronische ID-Karten und in neun EU-Staaten andere Formen der elektronischen Identifizierung (wie Smartcards und USB-Token). Doch der Nachweis und die Überprüfung der eigenen Identität finden EU-weit nicht statt, was den Online-Zugang zu öffentlichen Dienstleistungen im gesamten EU-Raum blockiert.

Definition und Ausprägungen

Elektronische Identifizierung ist der Prozess, durch elektronische Mittel die Identität einer natürlichen oder juristischen Person eindeutig festzustellen.¹⁰ Ausgestellt werden die elektronischen Mittel von einem Identifizierungssystem. Dieses prüft zusätzlich, ob die Person auch diejenige ist, für die sie sich ausgibt; man spricht in diesem Zusammenhang auch von „Authentifizierung“.¹¹ Grundlage für die europaweite Anerkennung der elektronischen Identifizierung ist die Aufnahme in die Liste notifizierter elektronischer Identifizierungssysteme.

⁹ Verordnung (EU) Nr. 910/2014, Erwägungsgrund (9).

¹⁰ Verordnung (EU) Nr. 910/2014, Artikel 3, 1.

¹¹ Verordnung (EU) Nr. 910/2014, Artikel 3, 2-5.

GUT ZU WISSEN

Notifizierung

Der Begriff der „Notifizierung“ beschreibt ein Verfahren, in dem die EU-Mitgliedsstaaten die Europäische Kommission über einen Rechtsakt in Kenntnis setzen müssen, bevor dieser als nationale Rechtsvorschrift Geltung entfalten kann. Im Fall der elektronischen Identifizierung bedeutet dies, dass die EU-Mitgliedsstaaten bei der EU-Kommission die Konformität ihrer jeweiligen nationalen Identifizierungssysteme mit den rechtlichen Vorgaben der eIDAS-Verordnung bestätigen lassen. Wer ein System erfolgreich anmeldet, muss auch alle anderen angemeldeten Systeme mit gleichem Sicherheitsniveau akzeptieren.

Praktische Umsetzung

Bei der Umsetzung konzentriert sich die eIDAS-Verordnung nicht auf eine Harmonisierung der unterschiedlichen eID-Systeme. Vielmehr geht es um eine **gegenseitige Anerkennung** verschiedener nationaler eID-Systeme. Die Verordnung erweitert also die Einsatzmöglichkeiten existierender eID-Systeme, indem sie deren Funktionalität EU-weit sicherstellt. Erreicht werden soll dies durch einen Interoperabilitätsrahmen, der auf Technologieneutralität ausgelegt ist, nach Möglichkeit europäischen und internationalen Normen folgt und Datenschutzbestimmungen strikt einhält.¹² Die Europäische Kommission hat in einem Durchführungsrechtsakt einen Mindestdatensatz festgelegt, der unterstützt werden muss, um eine natürliche oder juristische Person eindeutig identifizieren zu können.

Eine wertvolle Hilfe bei der technischen Umsetzung sind die Erfahrungen des STORK-Projekts, das die technische Machbarkeit einer grenzüberschreitenden elektronischen Identifizierung bestätigt hat. In Deutschland kann die elektronische Identifizierung anhand des neuen Personalausweises oder des elektronischen Aufenthaltstitels erfolgen. STORK ist bereits abgeschlossen, die Erkenntnisse werden in CEF-Projekten¹³ umfangreich fortgeführt.

Rechtswirkung

Die eIDAS-Verordnung verpflichtet die EU-Mitgliedsstaaten rechtlich nicht zur Einführung oder Notifizierung elektronischer Identifizierungssysteme, sehr wohl aber zur Anerkennung und Akzeptanz von in anderen Mitgliedsstaaten ausgestellten elektronischen Identifizierungsmitteln, vorausgesetzt, diese sind notifiziert.¹⁴ Ab dem 01. Juli 2018 müssen die Behörden in den EU-Mitgliedsstaaten alle notifizierten elektronischen Identifizierungsmittel anerkennen. Entsprechende organisatorische und technische Voraussetzungen zur elektronischen Annahme und Durchführung der Authentifizierung sind bis zu diesem Zeitpunkt zu treffen.

¹² Verordnung (EU) Nr. 910/2014, Artikel 12, Abs. (3).

¹³ CEF-Projekt (PDF).

¹⁴ Verordnung (EU) Nr. 910/2014, Artikel 6.

3.2 Elektronische Vertrauensdienste

Die eIDAS-Verordnung will vor allem das Vertrauen der Bürger und Unternehmen in den Binnenmarkt stärken und die Nutzung von Vertrauensdiensten fördern. Zu diesem Zweck führt sie die Begriffe „qualifizierter Vertrauensdienst“ und „qualifizierter Vertrauensdiensteanbieter (qVDA)“ ein.

Ein qualifizierter Vertrauensdienst ist ein Vertrauensdienst, der ein europaweit einheitliches Sicherheitsniveau besitzt und die in der eIDAS-Verordnung definierten Anforderungen erfüllt.

Er kann nur von einem qualifizierten Vertrauensdiensteanbieter erbracht werden. Um sich mit diesem Begriff bezeichnen zu können, muss der Anbieter sich einer sogenannten Konformitätsprüfung unterziehen, die mindestens alle 24 Monate wiederholt wird. Dabei wird untersucht, ob er die in der eIDAS-Verordnung festgelegten Anforderungen erfüllt.¹⁵

Die Prüfungen führt in der Regel eine staatlich akkreditierte Konformitätsbewertungsstelle durch. Bei erfolgreichem Verlauf erhält der qVDA ein Testat, welches er der nationalen Aufsichtsstelle vorlegt und damit seine Betriebsaufnahme beantragt.

Sind sämtliche Anforderungen nachweislich erfüllt, erfolgt die Aufnahme in öffentlich einsehbare nationale und europaweit einheitliche Vertrauenslisten. Ab diesem Zeitpunkt dürfen qVDA dann auch das EU-Vertrauenssiegel verwenden, um auf ihren Status als Anbieter qualifizierter Vertrauensdienste hinzuweisen.¹⁶

¹⁵ Verordnung (EU) Nr. 910/2014, Artikel 17, 20.

¹⁶ Verordnung (EU) Nr. 910/2014, Artikel 22, 23.

¹⁷ Verordnung (EU) Nr. 910/2014, Artikel 3, 20 und Erwägungsgrund (28).

Das EU-Vertrauenssiegel

Mit diesen Vorgaben wird eine maximale Transparenz erreicht. Anwender erkennen sofort, welcher Anbieter die Maßgaben der eIDAS-Verordnung erfüllt, zertifiziert ist und einen vertrauenswürdigen Dienst für elektronische Transaktionen anbietet.



eIDAS-Verordnung, Artikel 3, 20

„Qualifizierter Vertrauensdiensteanbieter (qVDA)“ ist ein Vertrauensdiensteanbieter, der einen oder mehrere qualifizierte Vertrauensdienste erbringt und dem von der Aufsichtsstelle der Status eines qualifizierten Anbieters verliehen wurde. Genau definierte Pflichten und Anforderungen stellen ein hohes Sicherheits- und Vertrauensniveau sicher.“¹⁷

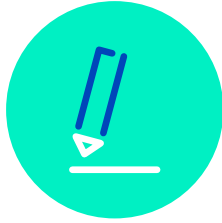
So sind Vertrauensdiensteanbieter verpflichtet, technische und organisatorische Maßnahmen (nach dem jeweils neuesten Stand der Technik) zu ergreifen, mit denen die Sicherheitsrisiken beherrscht werden. Sicherheitsverletzungen sind unverzüglich, in jedem Fall aber innerhalb von 24 Stunden, der Aufsichtsstelle und anderen direkt Betroffenen zu melden.¹⁸

Vertrauensdiensteanbieter haften für alle vorsätzlich oder fahrlässig zugefügten Schäden, die durch ihre Arbeit entstehen. Die Haftungsregelung ist für qualifizierte Vertrauensdiensteanbieter verschärft, hier wird von Vorsatz und Fahrlässigkeit ausgegangen, es sei denn, der qVDA kann das Gegenteil beweisen.¹⁹



¹⁸ Verordnung (EU) Nr. 910/2014, Artikel 19.

¹⁹ Verordnung (EU) Nr. 910/2014, Artikel 13.



Elektronische Signaturen

Herausforderung

Die bestehende Signaturrechtlinie (1999/93/EG) hat nicht zu einer EU-weiten Nutzung elektronischer Signaturen geführt. Unter anderem verhinderte der hohe organisatorische und technische Aufwand für ihre Einführung und Anwendung eine breite Nutzung. Schließlich fördert der technologieneutrale Ansatz der eIDAS-Verordnung neue Verfahren, die konsequent nutzerzentriert sind. Darunter befindet sich auch die Fernsignatur, die von der eIDAS-Verordnung ausdrücklich erwähnt wird.²⁰

Definition und Ausprägungen

Elektronische Signaturen sind Daten in elektronischer Form, die anderen elektronischen Daten beigelegt oder logisch mit ihnen verbunden werden und die der Anwender zum Unterzeichnen verwendet.²¹

Den höchsten rechtlichen Beweiswert besitzt die Qualifizierte Elektronische Signatur (QES). Sie basiert auf einem gültigen qualifizierten Zertifikat und wird mit einer Erstellungseinheit für Qualifizierte Elektronische Signaturen erstellt. Die Details zur Nutzeridentität können im Zertifikatsinhalt sichtbar sein oder auch nur im Hintergrundsystem des VDA gespeichert werden²², somit wird eine pseudonyme Nutzung ermöglicht.

Praktische Umsetzung

Auf der technischen Seite spezifiziert die eIDAS-Verordnung die Formate der Signaturen (zum Beispiel PAdES), um die EU-weite Interoperabilität sicherzustellen. Gleichzeitig beschränkt sie das Mittel zur Signaturerstellung nicht mehr auf eine Signaturkarte.

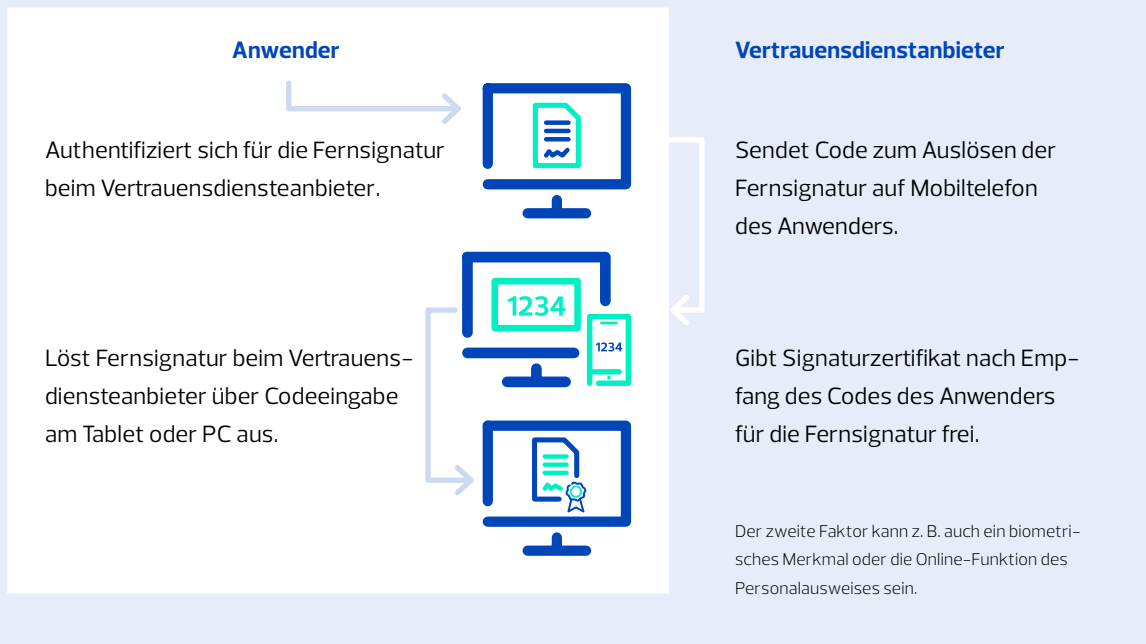
Vielmehr ist es zulässig, neben dem Zertifikat auch die elektronischen Signaturdateien (Schlüssel) auf sicheren Servern eines qualifizierten Vertrauensdiensteanbieters vorzuhalten. Damit ist die Grundlage für die Verwendung von Fernsignaturen, auch von mobilen Endgeräten aus, gegeben. Die Auslösung der QES erfolgt über eine Zwei-Faktor-Authentifizierung.

²⁰ Verordnung (EU) Nr. 910/2014, Erwägungsgrund (52).

²¹ Verordnung (EU) Nr. 910/2014, Artikel 3, 10.

²² Verordnung (EU) Nr. 910/2014, Artikel 3, 12 und Anhang I.

Die Fernsignatur im praktischen Einsatz (beispielhaft ausgelöst am Mobiltelefon)



Rechtswirkung

Die eIDAS-Verordnung gibt der QES die gleiche Rechtswirkung wie eine handschriftliche Unterschrift. Entscheidend für den EU-weiten Einsatz: Eine Qualifizierte Elektronische Signatur, die auf einem in einem Mitgliedsstaat ausgestellten qualifizierten Zertifikat beruht, wird in allen anderen Mitgliedsstaaten als QES anerkannt.²³ Und beim Zugang zu öffentlichen Online-Diensten – wie bei Ausschreibungen – darf kein höheres Sicherheitsniveau verlangt werden als das einer Qualifizierten Elektronischen Signatur.²⁴ Die bestehende Signaturrechtlinie (1999/93/EG) wird am 01. Juli 2016 aufgehoben und durch die eIDAS-Verordnung ersetzt.

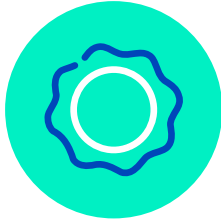
GUT ZU WISSEN

Die Zwei-Faktor-Authentifizierung

Die Zwei-Faktor-Authentifizierung dient dem Identitätsnachweis eines Nutzers mittels der Kombination zweier verschiedener und insbesondere unabhängiger Komponenten (Faktoren). Das können neben der geheimen PIN zum Beispiel biometrische Merkmale oder eine TAN-SMS auf das Mobiltelefon sein. Die Zwei-Faktor-Authentifizierung ist nur dann erfolgreich, wenn beide benötigten Faktoren korrekt eingesetzt werden.

²³ Verordnung (EU) Nr. 910/2014, Artikel 25, Abs. (2), (3).

²⁴ Verordnung (EU) Nr. 910/2014, Artikel 27, Abs. (3).



Elektronische Siegel

Herausforderung

Bisher gab es für Unternehmen und Behörden kein einheitliches, allgemein anerkanntes Verfahren, den Ursprung und die Unversehrtheit elektronischer Dokumente zu bestätigen. Dies war bislang immer an den einzelnen Mitarbeiter, das heißt an natürliche Personen, gebunden. Organisationsbezogene Lösungen, deren Nutzung mit bestimmten Rollen und Berechtigungen im Unternehmen verknüpft werden können, fehlten.

Definition und Ausprägungen

Elektronische Siegel sind Daten in elektronischer Form, die anderen Daten in elektronischer Form beigefügt oder logisch mit ihnen verbunden werden, um ihren Ursprung und ihre Unversehrtheit zu bestätigen.²⁵ Das bedeutet: Das Siegel verschmilzt mit den elektronischen Daten, die versiegelt werden, zu einer Einheit – ähnlich wie Siegellack, der auf einer Urkunde aufgetragen wird. Elektronische Siegel bieten damit eine doppelte Echtheitsgarantie:

- dass tatsächlich diejenige Organisation (Behörde, Unternehmen etc.) das Dokument ausgestellt hat, die als Absender genannt ist, und
- dass die Daten des Dokuments hundertprozentig dem Original entsprechen, also nicht im Nachhinein verändert wurden.

Das höchste Sicherheitsniveau besitzen laut eIDAS-Verordnung qualifizierte elektronische Siegel, die auf einem qualifizierten Zertifikat beruhen.²⁶

Praktische Umsetzung

Technisch betrachtet ist ein qualifiziertes elektronisches Siegel ähnlich einer Qualifizierten Elektronischen Signatur, aber mit unterschiedlichem Zertifikatstyp. Während das Siegel auf einem Organisationszertifikat basiert (also einem Zertifikat für eine Behörde, ein Unternehmen etc.), ist die Signatur immer personenbezogen. Analog zur Fernsignierung befinden sich die Schlüssel für qualifizierte elektronische Siegel virtuell auf einem sicheren Server eines qVDA. Der Anwender kann das Siegel aus der Ferne auslösen, z. B. auch über ein mobiles Endgerät.

Rechtswirkung

Rechtlich geht man bei Daten, mit denen das qualifizierte elektronische Siegel verbunden ist, immer von der Vermutung aus, dass sie unversehrt sind und die Herkunftsangabe richtig ist.²⁷ Qualifizierte elektronische Siegel, die in einem Mitgliedsstaat auf Grundlage eines qualifizierten Zertifikats ausgestellt wurden, werden automatisch in allen anderen EU-Staaten anerkannt.²⁸

²⁵ Verordnung (EU) Nr. 910/2014, Artikel 3, 25.

²⁶ Verordnung (EU) Nr. 910/2014, Artikel 3, 27.

²⁷ Verordnung (EU) Nr. 910/2014, Artikel 35, Abs. (2).

²⁸ Verordnung (EU) Nr. 910/2014, Artikel 35, Abs. (3).



Elektronische Zeitstempel

Herausforderung

In elektronischen Geschäftsprozessen gibt es Situationen, in denen es entscheidend ist, wann ein elektronisches Dokument eingegangen ist und dass es seit diesem Zeitpunkt nicht mehr verändert wurde. Beispiele dafür sind Angebotsunterlagen bei öffentlichen Ausschreibungen, das fristgerechte Eintreffen elektronischer Nachrichten in Gerichtsverfahren oder – im Industrieumfeld – Prüf- und Testdokumentationen, bevor sie im Archiv abgelegt werden.

Definition und Ausprägungen

Elektronische Zeitstempel sind Daten in elektronischer Form, die andere Daten in elektronischer Form mit einem bestimmten Zeitpunkt verknüpfen und dadurch den Nachweis erbringen, dass diese anderen Daten zu diesem Zeitpunkt vorhanden waren.²⁹

Als einzige Ausprägung sieht die eIDAS-Verordnung den qualifizierten elektronischen Zeitstempel vor. Dieser ist ein elektronischer Zeitstempel, der Datum und Zeit so mit den Daten verknüpft, dass die Möglichkeit der unbemerkten Veränderung der Daten nach vernünftigem Ermessen ausgeschlossen ist. Ferner basiert er auf einer korrekten Zeitquelle, die mit der koordinierten Weltzeit verknüpft ist.

Praktische Umsetzung

Der Betrieb eines qualifizierten Zeitstempeldiensts liegt ausschließlich in der Hand des Vertrauensdiensteanbieters. Dieser betreibt einen Server, der für Anwendungsprogramme einen signierten Zeitstempel ausstellt. Die Softwareapplikation schickt dafür die Prüfsummen des Dokuments an den Zeitstempelserver, der mittels Funkuhr und einer zusätzlichen internen Zeitquelle die aktuelle Zeit ermittelt.

Die Zeitangabe und die Prüfsumme des Dokuments werden mit dem Zertifikat des Zeitstempelservers signiert und an die Anwendung zurückgesendet. Der Austausch der Daten erfolgt nach der internationalen Spezifikation RFC 3161.

Rechtswirkung

Für qualifizierte elektronische Zeitstempel gilt die Vermutung der Richtigkeit des Datums und der Zeit, die darin angegeben sind, sowie der Unversehrtheit der mit dem Datum und der Zeit verbundenen Daten.³⁰ Als Beweis vor Gericht haben sie deshalb einen hohen Stellenwert.

Ein qualifizierter elektronischer Zeitstempel, der in einem EU-Mitgliedsstaat ausgestellt wurde, besitzt in allen anderen Mitgliedsstaaten Gültigkeit.³¹

²⁹ Verordnung (EU) Nr. 910/2014, Artikel 3, 33.

³⁰ Verordnung (EU) Nr. 910/2014, Artikel 41, Abs. (2).

³¹ Verordnung (EU) Nr. 910/2014, Artikel 41, Abs. (3).



Elektronische Einschreib- und Zustelldienste

Herausforderung

Eine verschlüsselte E-Mail stellt nur die Nachrichtenintegrität und die Vertraulichkeit elektronischer Informationen sicher, aber nicht deren Zustellung. Elektronische Einschreiben mit Zustelldienst bieten daher zusätzliche Vorteile wie die Identifizierung des Absenders und Empfängers sowie eine Zustellgarantie.

Definition und Ausprägungen

Qualifizierte Dienste für die Zustellung elektronischer Einschreiben ermöglichen die Übermittlung von Daten zwischen Dritten mit elektronischen Mitteln. Dabei weisen sie die Handhabung der übermittelten Daten nach, darunter den Nachweis, dass die Daten abgeschickt und empfangen wurden. Und sie schützen die übertragenen Daten vor Verlust, Diebstahl, Beschädigung oder unbefugter Veränderung.³²

Praktische Umsetzung

Qualifizierte elektronische Einschreib- und Zustelldienste werden von qualifizierten Vertrauensdiensteanbietern erbracht. Aktuell wird ein sogenanntes Framework an europäischen Normen und Spezifikationen definiert, das für die Interoperabilität der Dienste sorgen soll. Zentrale Anforderungen sind der Einsatz elektronischer Signaturen beziehungsweise elektronischer Siegel und das Aufbringen eines qualifizierten Zeitstempels.³³

Rechtswirkung

Die Rechtswirkung eines qualifizierten Diensts für elektronische Einschreiben umfasst die Vermutung:

- dass die Daten unversehrt sind,
- dass die Daten durch einen identifizierten Absender sicher gesendet und durch einen identifizierten Empfänger sicher empfangen wurden, und
- dass Versand und Empfang zum korrekten Zeitpunkt stattfanden.³⁴

³² Verordnung (EU) Nr. 910/2014, Artikel 3, 36.

³³ Verordnung (EU) Nr. 910/2014, Artikel 44, Abs. (1) d), f).

³⁴ Verordnung (EU) Nr. 910/2014, Artikel 43, Abs. (2).



Elektronische Validierungs- und Bewahrungsdienste

Herausforderung

Elektronische Validierungs- und Bewahrungsdienste sind die Grundlage für eine dauerhafte, rechtssichere Nutzung elektronischer Signaturen und Siegel. Sie sorgen EU-weit für die vertrauenswürdige Prüfung der Gültigkeit von Signaturen und Siegel sowie für einen rechtsverbindlichen elektronischen Langzeitspeicher.

Definition und Ausprägungen

Validierungs- und Bewahrungsdienste beziehen sich ausdrücklich auf Qualifizierte Elektronische Signaturen und qualifizierte elektronische Siegel. Sie können deshalb nur von qualifizierten elektronischen Vertrauensdiensteanbietern erbracht werden.

Ein qualifizierter Bewahrungsdienst verwendet Verfahren und Technologien, die es ermöglichen, die Vertrauenswürdigkeit der Qualifizierten Elektronischen Signatur und des qualifizierten elektronischen Siegels über den Zeitraum ihrer technologischen Geltung hinaus zu verlängern.³⁵

Praktische Umsetzung

Elektronische Validierungs- und Bewahrungsdienste lassen sich optimal miteinander kombinieren. Sie ermöglichen die gemeinsame Speicherung der signierten Unterlagen und der Signatur selbst mit dem dazugehörigen Zertifikat sowie die Speicherung des positiven Prüfprotokolls mit der Signatur des Validierungsdienstes.

Zur Beweiswerterhaltung ist eine periodische Signatur- und Hasherneuerung notwendig, wenn die Sicherheitseignung der zugrundeliegenden Algorithmen nicht mehr gegeben ist. Mit den vorhandenen nationalen und internationalen Standards und Normen – wie ISO 14721 oder TR-ESOR (Version 1.2) – sind die Vorgaben der eIDAS-Verordnung umsetzbar.³⁶

³⁵ Verordnung (EU) Nr. 910/2014, Artikel 34, 40.

³⁶ Siehe BearingPoint: Die Bedeutung der eIDAS-Verordnung für Unternehmen und Behörden, eBook 2015, S. 46, 47 (PDF).



Website-Authentifizierungsdienste

Herausforderung

Website-Authentifizierungsdienste geben dem Besucher die Sicherheit, dass hinter der Website eine echte und vertrauenswürdige Einrichtung steht. Zwar bestehen bereits Vorgaben durch die Browser-Anbieter, doch gab es bisher keine qualifizierten Website-Zertifikate, die von europäischen Zertifizierungsstellen ausgestellt werden und die Zugehörigkeit der Website zu einer Organisation oder Person bestätigen.³⁷

Definition und Ausprägungen

Die Authentifizierungsdienste für Websites basieren auf einem qualifizierten Zertifikat. Dieses ermöglicht die Authentifizierung einer Website und verknüpft sie mit der natürlichen oder juristischen Person, der das Zertifikat ausgestellt wurde.

Die eIDAS-Verordnung definiert Anforderungen an qualifizierte Zertifikate für die Website-Authentifizierung und nennt die Vorgaben, denen ein solches Zertifikat entsprechen muss. Dazu gehören unter anderem Name und Adresse des Betreibers sowie die von ihm betriebenen Domain-Namen.³⁸

Ausgestellt werden qualifizierte Zertifikate für die Website-Authentifizierung von qualifizierten Vertrauensdiensteanbietern.³⁹

Praktische Umsetzung

Die Verbreitung vertrauenswürdiger Website-Zertifikate und die damit verbundene Umstellung der Webkommunikation auf sichere Protokolle wird in der Praxis mithilfe von TLS (Transport Layer Security) umgesetzt.

In bestehenden europäischen Normen sind wesentliche Anforderungen an einen Zertifikatsanbieter und für den Aufbau eines qualifizierten Website-Zertifikats enthalten (EN 319 411-1 und EN 319 412-4).⁴⁰

³⁷ Verordnung (EU) Nr. 910/2014, Artikel 3, 38.

³⁸ Verordnung (EU) Nr. 910/2014, Anhang IV.

³⁹ Verordnung (EU) Nr. 910/2014, Artikel 3, 39.

⁴⁰ Siehe BearingPoint: Die Bedeutung der eIDAS-Verordnung für Unternehmen und Behörden, eBook 2015, S. 43 (PDF).

GUT ZU WISSEN

TLS/SSL

Transport Layer Security (TLS, deutsch Transportschichtssicherheit), ist ein Verschlüsselungsprotokoll zur sicheren Datenübertragung im Internet. Es ist auch bekannt unter der Vorgängerbezeichnung **Secure Sockets Layer (SSL)**. Seit einiger Zeit wird das SSL-Protokoll unter dem neuen Namen TLS weiterentwickelt und standardisiert. TLS-Verschlüsselung wird heute vor allem mit HTTPS eingesetzt.

4. DIE eIDAS-VERORDNUNG: MEHRWERTE UND NUTZEN

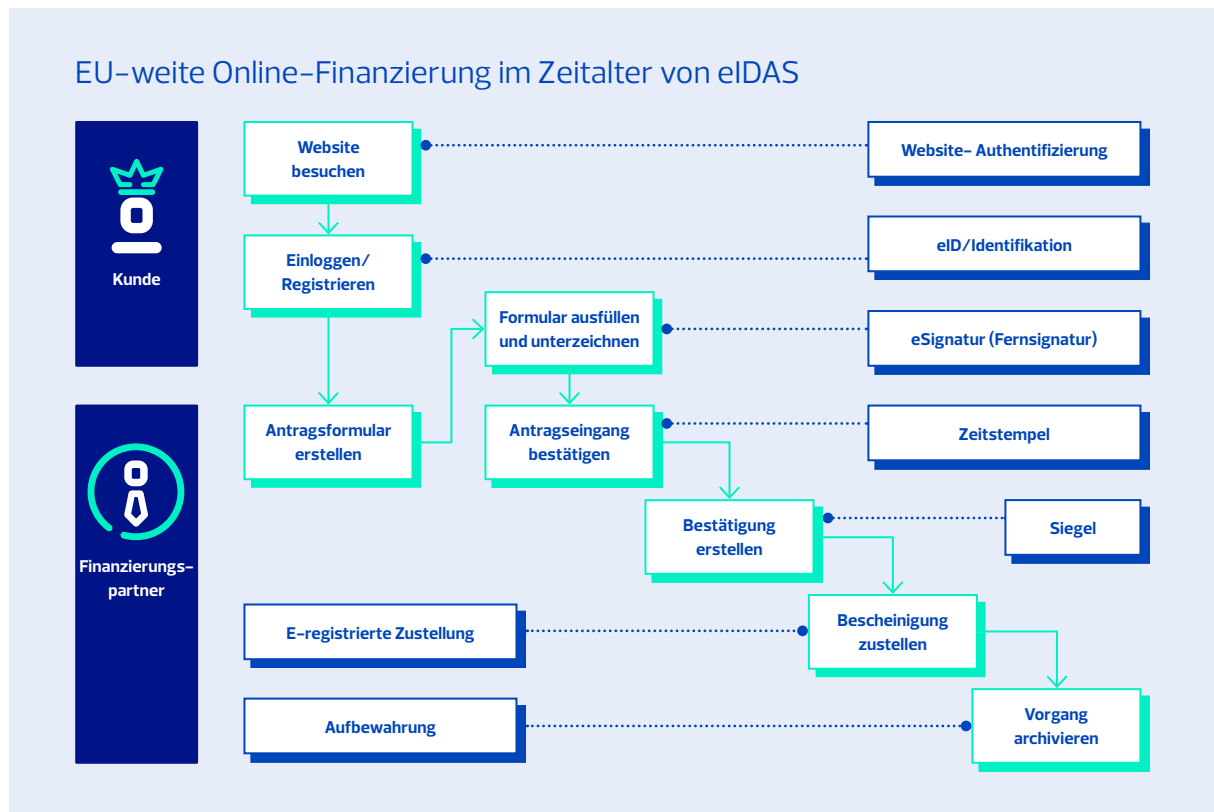
Die eIDAS-Verordnung bildet den rechtlichen und organisatorischen Rahmen für einen sicheren und vertrauenswürdigen elektronischen Geschäftsverkehr im gesamten EU-Raum. Die EU-weite Interoperabilität der elektronischen Identifizierung, die Harmonisierung und Standardisierung von Signaturen sowie die Etablierung von neuen Vertrauensdiensten – wie dem elektronischen Siegel – bieten Chancen für eine schnelle Verbreitung und hohe Anwenderakzeptanz.

Welche Mehrwerte sich daraus konkret in der Praxis ergeben, zeigt das kleine baltische Land Estland. Dort lässt sich mit der eID-Card in weniger als einer halben Stunde online ein Unternehmen gründen. Die Abgabe einer Jahresbilanz durch Unternehmen konnte von einem dreimonatigen papiergebundenen Verfahren auf einen 20-minütigen elektronischen Prozess reduziert werden. Und 98 Prozent aller Finanztransaktionen werden in Estland elektronisch durchgeführt.⁴¹ Die Vorteile und Nutzeneffekte der eIDAS-Verordnung ziehen sich durch alle Branchen und Wertschöpfungsprozesse. Am Beispiel öffentlicher Ausschreibungen hat die Europäische Kommission den Nutzen der eIDAS-Verordnung detailliert beziffert. Demnach reduziert sich der Zeitaufwand für den gesamten Prozess von ein bis zwei Wochen auf Stunden bzw. wenige Tage. Wo vorher mehrere Aktenordner im Archiv verstaut werden mussten, sind jetzt alle Dokumente elektronisch abgespeichert. Und die Kosten betragen in einem elektronischen Workflow ein Fünftel bis ein Zehntel der Ausgaben, die durch den Austausch von Papierdokumenten entstanden wären.

⁴¹ European Commission: Electronic identification, signatures and trust services: Questions & Answers (Memo).

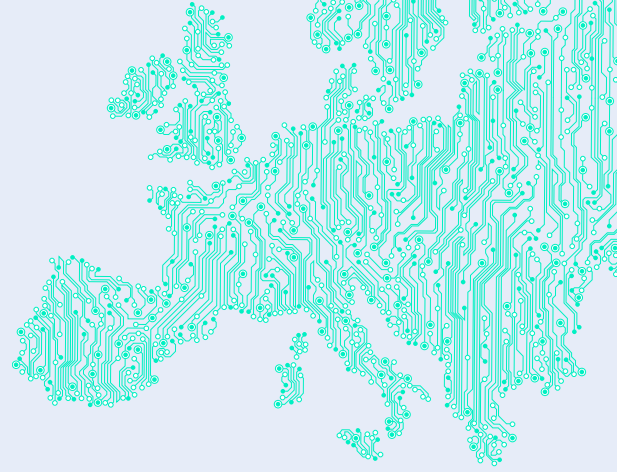


Wie eIDAS ganzheitlich in einem typischen eTransaktions-Workflow wirkt, zeigt auch das zweite Beispiel aus dem Finanzumfeld.



Zusammengefasst bietet die konsequente Umsetzung der eIDAS-Verordnung folgende Mehrwerte und Chancen:

- Gesteigerte Sicherheit elektronischer Prozesse durch EU-weit anerkannte vertrauenswürdige Identifizierung.
- Die Nachweisfähigkeit und Beweissicherheit elektronischer Transaktionen von Unternehmen und Behörden wird durch einheitliche Standards gestärkt.
- Durchgängige elektronische Geschäftsprozesse ohne Medienbrüche führen zu:
 - Kosteneinsparungen, indem Ausgaben für den Transport (Papier, Briefumschläge, Porto) und die Archivierung (Ordner, Regale, Räumlichkeiten) wegfallen,
 - schnelleren Prozessdurchlaufzeiten sowie Geschäftsabschlüssen in Echtzeit und
 - einer erhöhten Kundenzufriedenheit durch schnellere Reaktionen auf Kundenanfragen.
- Wettbewerbsvorteile für europäische Unternehmen durch neue Produkte, Dienstleistungen und Geschäftsmodelle.



Europa im Jahr 2021

Der digitale Binnenmarkt ist Wirklichkeit. Erstmals in der Geschichte der Europäischen Union lassen sich über alle Grenzen hinweg elektronische Interaktionen und Transaktionen zwischen Bürgern, Unternehmen und öffentlicher Verwaltung sicher, vertrauenswürdig und rechtsverbindlich durchführen.

Raivo ist hochzufrieden. Erst letzte Woche hat der Geschäftsführer eines estnischen Kleinunternehmens von einer öffentlichen Ausschreibung in Frankreich erfahren. Fünf Jahre zuvor hätte sich eine Teilnahme aufgrund des Aufwands und der bestehenden Unsicherheit bei der Zustellung nicht gelohnt. Doch seither hat sich viel geändert. Über seine elektronische ID-Karte wird Raivo von der Behörde eindeutig identifiziert. Alle eingereichten Dokumente sind elektronisch gesiegelt. Damit ist die Unversehrtheit der Informationen sichergestellt und das estnische Unternehmen eindeutig als Absender bestätigt. Das Ausschreibungsformular unterschreibt Raivo mit seiner elektronischen Signatur. Die Behörde versieht die Unterlagen mit einem elektronischen Stempel, was den Zeitpunkt der Abgabe beweiskräftig bestätigt. Die Bescheinigung, dass alle Unterlagen ordnungs- und fristgerecht abgegeben wurden, erhält Raivo per elektronischem Einschreibzustelldienst.

Und auch für Herrn Meyer von der Hedracell AG ist vieles einfacher geworden. In den Geschäftsbeziehungen mit Kunden und Zulieferern lassen sich Verträge und andere wichtige Vereinbarungen komplett elektronisch abbilden. Das fängt bei der Erstellung an und hört beim elektronisch unterschriebenen Dokument auf. Und erhält Herr Meyer kurzfristig einen größeren Auftrag, kann er gelassen bleiben. Online-Kredite für notwendige Kapazitätserweiterungen werden EU-weit innerhalb weniger Tage bearbeitet. Dabei findet der gesamte Prozess online statt – vom Nachweis der elektronischen Identität über die elektronisch geleistete Vertragsunterschrift bis hin zur finalen Kreditbescheinigung.



Die eIDAS-Verordnung legt das Fundament für den digitalen Binnenmarkt. Unternehmen profitieren von einer gesteigerten Wettbewerbsfähigkeit, Behörden von effizienteren Arbeitsabläufen und Verbraucher von günstigen Preisen und erweiterten Online-Services. Jetzt gilt es, die Chancen auch zu ergreifen ...

Bundesdruckerei GmbH

Kommandantenstraße 18 10969 Berlin

Tel.: +49 (0)30 25 98-0 Fax: +49 (0)30 25 98-22 05

info@bdr.de www.bundesdruckerei.de