BearingPoint®

Berlin, 23.11.2015

Die Bedeutung der eIDAS-Verordnung für Unternehmen und Behörden

Neue Chancen und Herausforderungen für vertrauenswürdige elektronische Geschäftsprozesse in Europa

Vorwort

Der Sinn des europäischen Binnenmarkts besteht darin, Hemmnisse zu beseitigen und Vorschriften zu vereinfachen, damit Behörden, Unternehmen und Verbraucher in der EU einschließlich Island, Liechtenstein, Norwegen und der Schweiz die Chancen optimal nutzen können, die der direkte Zugang zu einem Markt mit 32 Staaten und fast einer halben Milliarde Menschen bietet.

Die wirtschaftliche und soziale Entwicklung setzt Vertrauen in das Online-Umfeld voraus. Mangelndes Vertrauen führt dazu, dass Verbraucher, Unternehmen und die öffentliche Verwaltung nur zögerlich elektronische Transaktionen durchführen oder neue Dienste einführen und nutzen. Vor allem dann, wenn sie die Befürchtung hegen, dass die Rechtssicherheit nicht gegeben ist.

Die noch junge eIDAS-Verordnung stärkt das Vertrauen in elektronische Transaktionen im Binnenmarkt nachhaltig durch Schaffung einer gemeinsamen Grundlage für eine vertrauenswürdige elektronische Interaktion zwischen Bürgern, Unternehmen und Behörden auf Basis vertrauenswürdiger elektronischer Zertifikate und europäischer Public-Key-Infrastrukturen. Vornehmliches Ziel ist die spürbare Erhöhung von Effizienz und Effektivität öffentlicher und privater Online-Dienstleistungen, des elektronischen Geschäftsverkehrs und des elektronischen Handels in Europa.

Es lohnt sich, die eIDAS-Verordnung bereits heute bei der Planung und Umgestaltung betrieblicher und behördlicher Vorgänge zu berücksichtigen. Sie bietet branchenübergreifend und über öffentliche Ebenen hinweg große Einsparpotenziale aufgrund weitreichender Standardisierungen. Sie steht für Vertrauen und Rechtssicherheit und bildet die Grundlage für die Akzeptanz elektronischer Vorgänge und Dokumente.

Stephan Weber

Partner
BearingPoint

Ziele und Inhalte der Publikation

Das Paper bietet branchenübergreifende Informationen über wesentliche Inhalte und Ziele der noch jungen eIDAS-Verordnung. Das Dokument ist hilfreich bei der Beurteilung von Vorteilen und Nutzen, Herausforderungen und Chancen. Für wen ist die eIDAS-Verordnung interessant? Welche Geschäftsprozesse sind betroffen? Und welche Vorteile bietet sie? Aber auch: Was muss berücksichtigt werden – rechtlich, technisch und organisatorisch, um den Herausforderungen bestehender Anwendungsfälle und neuer Geschäftsmodelle gerecht zu werden? Wir beschreiben den Status quo bestehender Regularien und Standards für vertrauenswürdige elektronische Prozesse in Deutschland, ziehen ein Fazit auf Basis unserer langjährigen Erfahrung und geben konkrete Handlungsempfehlungen für Anwender und Betreiber aus Behörden und Unternehmen.

Unser Ziel ist, Ihnen eine verlässliche Expertenschrift an die Hand zu geben für die sachliche Einschätzung und pragmatische Umsetzung moderner und EU-weiter eBusiness-Strategien.

Die Autoren

Tomasz Kusber ist seit mehr als zehn Jahren anerkannter Experte für Kryptographie, IT-Compliance- und IT-Sicherheit. Er ist Senior Consultant bei BearingPoint und berät in der Privatwirtschaft und im öffentlichen Sektor. Sein fachlicher Schwerpunkt ist die Umsetzung von IT-Compliance- und Digitalisierungsstrategien. Für das DIN beteiligt er sich an der Ausformulierung der technischen Durchführungsrechtsakte der eIDAS-Verordnung. Tomasz Kusber arbeitet in Berlin.

Kontakt:
tomasz.kusber@bearingpoint.com
Telefon: +49 30 88004 2039

Steffen Schwalm ist seit mehr als zehn Jahren Experte in internationalen Gremien wie ISO und ETSI. Er ist stellvertretender Leiter eines DIN-Normungsausschusses und Co-Autor der zur beweiswerterhaltenden Langzeitspeicherung veröffentlichten DIN 31647. Als Business Advisor bei BearingPoint verantwortet er zahlreiche Großprojekte zur Information Governance, E-Akte und beweissicheren Aufbewahrung elektronischer Unterlagen, unter anderem bei Behörden, in der Luftfahrt und im Health Care. Er berät in fachlichen und organisatorischen Fragen bei der Fortschreibung der BSI TR-ESOR sowie der Entwicklung von Normen im Kontext der eIDAS. Steffen Schwalm arbeitet in Berlin.

Kontakt:
steffen.schwalm@bearingpoint.com
Telefon: + 49 30 88004 9148

Alexander Dörner ist seit mehr als zehn Jahren IT-Compliance Specialist. Er berät Hersteller, Dienstleister und Anwender aus Industrie und Verwaltung in Signatur- und Digitalisierungsfragen. Er schreibt Fachkonzepte, ist Co-Autor der DIN 31647 und Mitglied im DIN, BITKOM und TeleTrust. Im Rahmen einer eAkte-Einführung entwickelte er den ersten eIDAS-konformen Signaturprozess mit Langzeitspeicherung nach BSI TR-ESOR. Er ist Geschäftsführer der itellent, die als Competence Hub und strategischer Partner der BearingPoint 'IT-Compliance & Information Governance' vorantreibt. Er arbeitet in Düsseldorf und Berlin.

Kontakt:
alexander.doerner@itellent.com
Telefon: +49 172 447 87 27

Theresa Vogt studierte Informationswissenschaften an der Fachhochschule Potsdam mit Schwerpunkt auf den Themen Records Management und digitale Archivierung. In Zusammenarbeit mit BearingPoint verfasste sie ihre Masterarbeit zum Thema "Auswirkungen der eIDAS-Verordnung auf das Records Management der öffentlichen Verwaltung in Deutschland". Bereits in ihrer Bachelorarbeit beschäftigte sie sich mit dem Thema elektronische Signaturen. Hier untersuchte sie die Möglichkeit zur elektronischen Abgabe und Speicherung von Abschlussarbeiten.

Seit Oktober 2015 ist sie als Business Analyst für BearingPoint im Bereich Public Services tätig. Theresa Vogt arbeitet in Berlin.

Kontakt:
theresa.vogt@bearingpoint.com
Telefon: +49 30 88004 9388

Inhaltsverzeichnis

1 Einführung

Das erste Kapitel beschreibt die grundsätzliche Einordnung der eIDAS-Verordnung, die Intention, den Status quo vertrauenswürdiger elektronischer Geschäftsprozesse in Europa und erläutert die wesentlichen Gründe, weshalb sich diese bisher nicht flächendeckend durchsetzen konnten. Außerdem nennen wir Mehrwerte, die sich aus der Umsetzung der eIDAS-Verordnung ergeben.

Kurz und bündig:

Die eIDAS-Verordnung bietet eine europaweit einheitliche Grundlage für vertrauenswürdige und dauerhaft nachweisbare elektronische Geschäftsprozesse in Europa. Sie ist seit Ende 2014 geltendes Recht in allen 28 EU-Mitgliedstaaten und adaptiert von Island, Liechtenstein, Norwegen und der Schweiz.

eIDAS berücksichtigt nationale Regelungen mit begrenztem Einsatzgebiet und geringer Akzeptanz (zum Beispiel der De-Mail und der qualifizierten elektronischen Signatur in Deutschland).

eIDAS verspricht spürbare Erleichterung im Scan- und Signaturprozess, zum Beispiel durch neue elektronische Siegel ohne Personenbezug und den Verzicht auf Signaturkarten. Sie sorgt für die schnelle Verbreitung von Werkzeugen und Methoden für die sichere und vertrauenswürdige elektronische Transaktion, Identifizierung und Nachweisführung - damit stets sichergestellt ist, mit welchem Vertragspartner man korrespondiert und mit wem rechtsverbindlich auf elektronischem Wege Verträge geschlossen werden können – mit weniger Papier, kürzeren Prozessen und geringeren Kosten, EU-weit.

1.1 Status quo vertrauenswürdiger elektronischer Geschäftsprozesse in Deutschland und in Europa

Trotz des bereits seit 2001 geltenden Signaturgesetzes und des E-Government-Gesetzes aus dem Jahr 2013 konnten sich elektronische Signaturen, elektronische Identifizierungsmittel sowie Zustelldienste in Deutschland nicht flächendeckend durchsetzen. Die Möglichkeit sich mit dem neuen Personalausweis zu identifizieren sowie mittels einer elektronischen Signatur Dokumente zu unterzeichnen wird weder von Bürgern noch von Behörden und Unternehmen umfassend genutzt.

1.2 Sinn und Zweck der eIDAS-Verordnung

Seit September 2014 gilt die EU-Verordnung Nr. 910/2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG. Die als eIDAS-Verordnung bezeichnete Regelung schafft europaweit einheitliche Rahmenbedingungen für vertrauenswürdige elektronische Geschäftsprozesse und Nachvollziehbarkeit von elektronischen Transaktionen zwischen Bürgern, Unternehmen und Behörden. Im Gegensatz zu einer EU-Richtlinie ist die eIDAS-Verordnung unmittelbar geltendes Recht in allen 28 Mitgliedsstaaten. Die Verordnung trifft verbindliche rechtliche Regelungen und wird durch begleitende ETSI[1]- und CEN[2]-Normen fachlich-technisch verbindlich untersetzt. Sie schafft somit eine europaweit geltende Grundlage für die vertrauenswürdige elektronische Interaktion zwischen Bürgern, Unternehmen und öffentlichen Verwaltungen, die zur Stärkung des Vertrauens in elektronische Transaktionen im europäischen Binnenmarkt beiträgt. Im Ergebnis wird die Effektivität öffentlicher und privater Online-Dienstleistungen, des elektronischen Geschäftsverkehrs und des elektronischen Handels in der Union absehbar erhöht: Beendet wird das Nebeneinander verschiedener, teilweise

[1] ETSI - das Europäische Institut für Telekommunikationsnormen (englisch European Telecommunications Standards Institute), **http://www.etsi.org/**

[2] CEN - das Europäische Komitee für Normung (französisch Comité Européen de Normalisation; englisch European Committee for Standardization), **https://www.cen.eu**

gegensätzlicher Regelungen und Standards für elektronische Transaktionen, Identifizierung, Authentifizierung und Nachweisführung. Ein wesentliches Hemmnis für übergreifende elektronische Geschäftsprozesse wird beseitigt - mit absehbarer Effizienzsteigerung und spürbaren Kosteneinsparungen bei Behörden und Unternehmen in Europa.

1.3 Wesentliche Hemmnisse bei der bisherigen Umsetzung elektronischer Prozesse

Lösungen zur Abbildung vertrauenswürdiger elektronischer Transaktionen und Identifizierung in Deutschland - wie qualifizierte elektronische Signaturen und Zeitstempel, Neuer Personalausweis oder De-Mail - sind seit langem bekannt und deren Einsatz ist bereits verbindlich geregelt. In diesem Bereich dienen die Vorgaben der eIDAS-Verordnung in erster Linie zur europaweiten Vereinfachung und Standardisierung der Werkzeuge.

Wesentliche Hemmnisse bei der Umsetzung von länderübergreifenden und innerstaatlichen elektronischen Prozessen, waren aus deutscher Sicht bislang

- rein nationale Regelungen und folglich begrenzte Einsatzgebiete z.B. für den Neuen Personalausweis, De-Mail für Deutschland oder die Amtssignatur für Österreich und damit verbundene Rechtsunsicherheit in der internationalen Kommunikation
- unterschiedliche technische und fachliche Standards in einzelnen EU-Staaten
- ausschließlicher Bezug auf eine natürliche Person und Erzeugung der qualifizierten elektronischen Signatur nur mit Signaturkarte und der hohe organisatorische wie technische Aufwand für die Einführung und Anwendung

Folglich gab es nur wenige Anwendungsfälle für übergreifende vertrauenswürdige elektronische Transaktionen in Europa oder für die nationale Anwendung der qualifizierten elektronischen Signatur in Deutschland. Hier fehlt die grundsätzliche Durchdringung und Breitenwirkung (Henne-/Ei-Problematik).
Die eIDAS-Verordnung bewirkt einheitliche EU-weite Regelungen und ermöglicht zugleich die vereinfachte Handhabung vertrauenswürdiger elektronischer Geschäftsprozesse. daraus entstehende konkrete Mehrwerte für Behörden, Unternehmen und Diensteanbieter werden im folgenden Kapitel behandelt.

1.4 Wesentliche Mehrwerte der eIDAS-Verordnung

Die Hemmnisse für die Umsetzung werden mit der eIDAS-Verordnung sowie deren *Implementing Acts* und die begleitend entstehenden europäischen ETSI- und CEN-Normen beseitigt. Diese Vereinheitlichung und

Vereinfachung unterstützt die breite Anwendung von Werkzeugen und Methoden für vertrauenswürdige elektronische Transaktionen, Identifizierung und Nachweisführung.

Wesentliche Mehrwerte der eIDAS-Verordnung sind:

- die eIDAS-Verordnung erleichtert die Umsetzung durchgängig elektronischer Prozesse
- die eIDAS-Verordnung ermöglicht branchenübergreifend eine vertrauenswürdige elektronische Kommunikation
- die Sicherheit elektronischer Prozesse wird standardisiert und damit verbessert
- die Nachweisfähigkeit und Beweissicherheit elektronischer Transaktionen von Unternehmen und Behörden wird durch einheitliche Standards vereinfacht
- durch einheitliche Standards und Regularien etablieren sich IT Compliance und Information Governance für elektronische Geschäftsabläufe in den Unternehmen
- qualifizierte elektronische Signaturen und Zeitstempel können durch die Verwendung von Organisationszertifikaten einfacher eingeführt und etabliert werden
- für IT-Dienstleister ergeben sich zusätzliche Marktchancen (sofern diese sich als qualifizierte Vertrauensdiensteanbieter notifizieren lassen)

Wie sich diese Mehrwerte konkret auf einen beispielhaften, elektronischen und EU-weiten Transaktionsprozess auswirken können, zeigt die folgende Grafik.

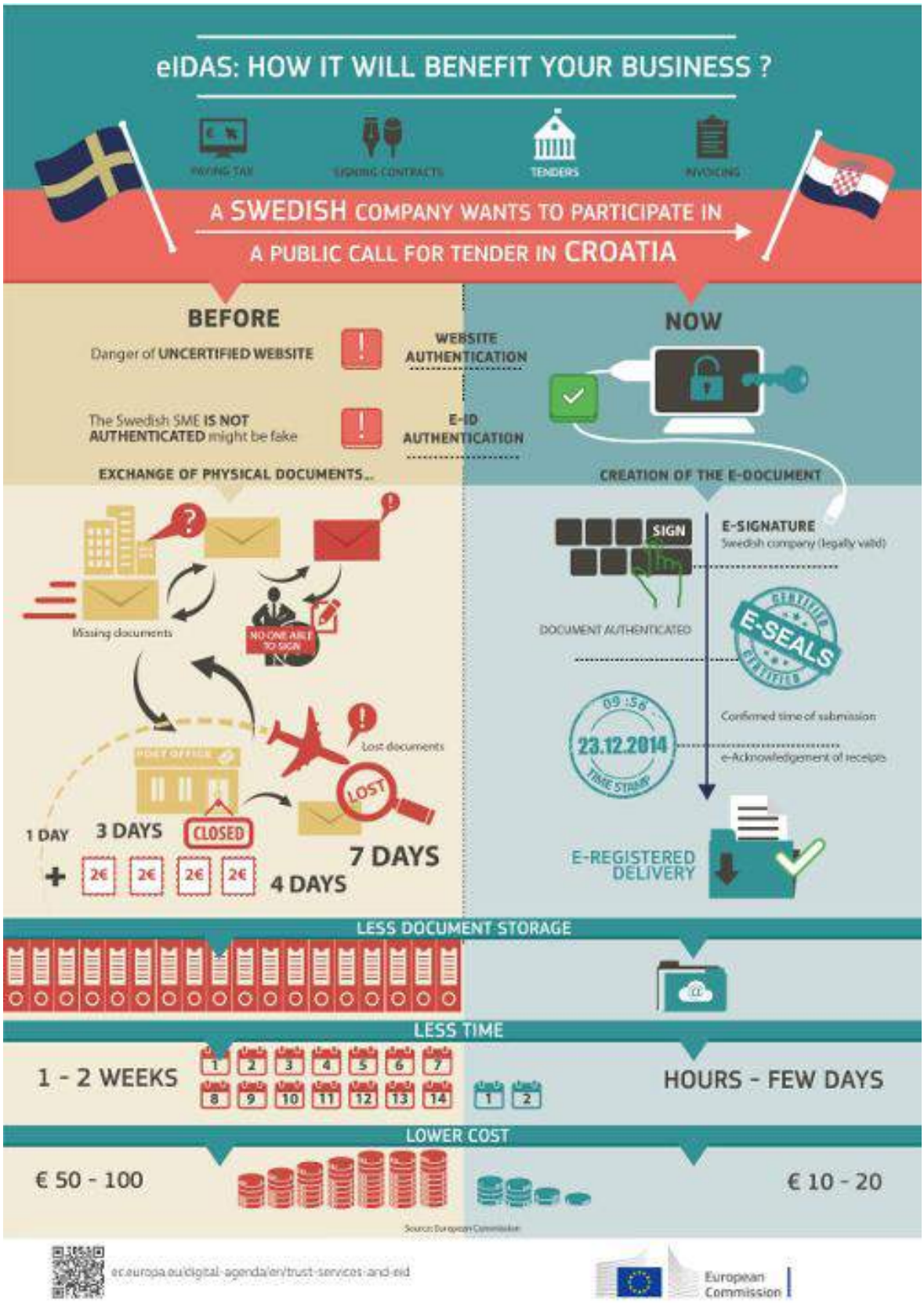


Abbildung 1: Beispielprozess zu Auswirkungen der eIDAS-Verordnung (Bildquelle: http://www.der-wid.com/wp-content/uploads/2014/10/eIDASregulationInfographic1.jpg)

2 Rechtlicher Rahmen

Das zweite Kapitel behandelt die rechtlichen Aspekte der eIDAS-Verordnung, untergliedert in die neuen Vertrauensdienste für Signaturen, Einschreib- und Zustelldienste sowie Bewahrungsdienste. Wir nennen die wichtigsten Termine im Fahrplan der eIDAS-Verordnung, die möglichen Anpassungsbedarfe in Deutschland und schließen mit einem Fazit.

Kurz und bündig:

Die eIDAS-Verordnung löst die EU-Signaturrichtlinie aus dem Jahr 1999 ab und betrifft elektronische Prozesse zwischen Behörden, Unternehmen und Bürgern. Sie gilt für die elektronische Identifizierung (eID) und die elektronischen Vertrauensdienste wie qualifizierte Signaturen und Website-Zertifikate, für elektronische Zustelldienste und Bewahrungsdienste (zum Beispiel auf Basis von BSI TR-ESOR). eIDAS betrifft Kerninhalte des EGovG Bund wie zum Beispiel die Zugangseröffnung für die elektronische Signatur, den Neuen Personalausweis und De-Mail.

Absehbare Auswirkungen auf deutsche Regularien: neue (qualifizierte) Vertrauensdienste, alternative Zustelldienste im Wettbewerb zu De-Mail, elektronische Siegel als 'Organisationssignatur' und eID. Außerdem: die beweiswerterhaltende Langzeitspeicherung auf Basis der qualifizierten eIDAS-Bewahrungsdienste und BSI TR-ESOR.

2.1 Grundsatz & Inhalte der eIDAS-Verordnung

Die eIDAS-Verordnung setzt einheitliche Maßgaben für vertrauenswürdige sowie langfristig nachweisbare elektronische Transaktionen in Europa und legt sowohl rechtliche als auch technische Rahmenbedingungen fest. Durch die Verordnung werden bestehende Richtlinien wie zum Beispiel die EU-Signaturrichtlinie (1999/93/EG) abgelöst. Die eIDAS-Verordnung ist geltendes Recht in allen EU- und EFTA-Staaten, gilt jedoch nicht für geschlossene Nutzerkreise, beispielsweise innerhalb einer Behörde oder eines Unternehmens. Der Anwendungsbereich der eIDAS ist vielmehr nach außen gerichtet - auf Prozesse zwischen Behörden, Unternehmen und Bürgern. Als Verordnung ist sie unmittelbar ab Inkrafttreten geltendes Recht und nicht erst in nationales Recht umzusetzen.

Die Regelungsinhalte sind im Folgenden beschrieben:

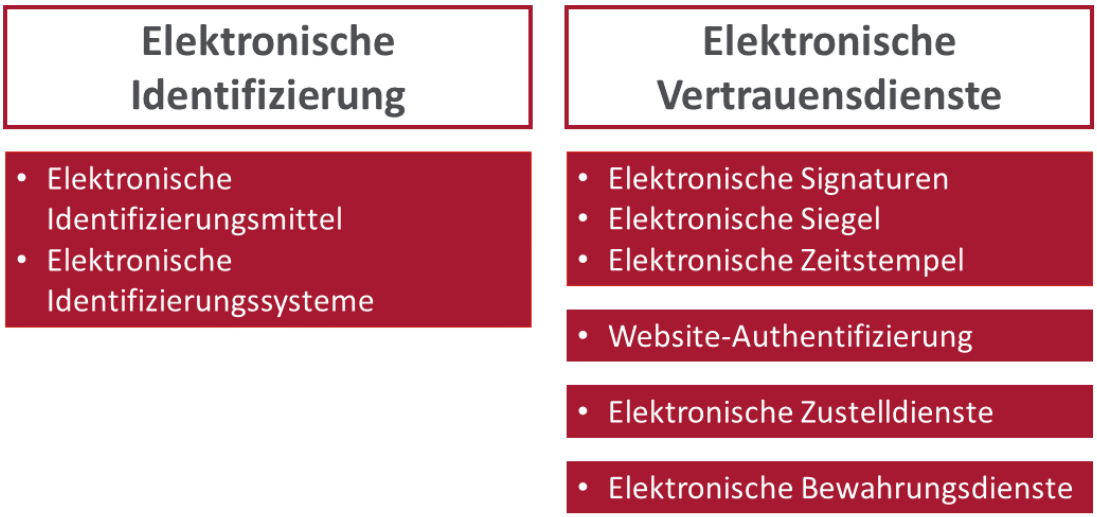


Abbildung 2: Regelungsinhalte der eIDAS-Verordnung

2.2 Elektronische Identifizierung (eID)

Hinsichtlich eID unterscheidet die Verordnung zwischen Identifizierungssystem[3] und Identifizierungsmittel[4], das in diesem System genutzt wird.

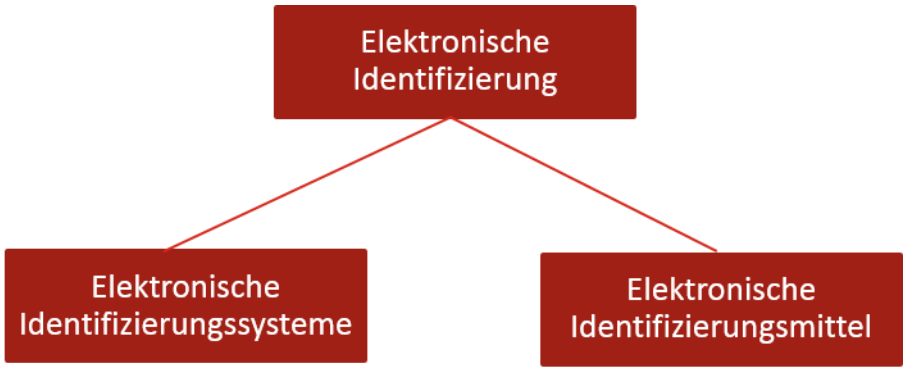


Abbildung 3: Elektronische Identifizierung (eID) in der eIDAS-Verordnung

[3] Definition: System für elektronische Identifizierung, in dessen Rahmen Entitäten elektronische Identifizierungsmittel ausgestellt werden

[4] Definition: materielle und/oder immaterielle Einheit, die Identifizierungsdaten von Entitäten enthält und zur Authentifizierung bei Online-Diensten verwendet wird

Unter elektronischer Identifizierung versteht die Verordnung die Verwendung von Personenidentifizierungsdaten in elektronischer Form (die eine natürliche oder juristische Person eindeutig repräsentieren) zur Authentifizierung gegenüber Dritten. In Deutschland kann die Authentifizierung derzeit zum Beispiel über den Neuen Personalausweis oder den elektronischen Aufenthaltstitel erfolgen.

Abbildung 4: Zweck elektronischer Identifizierung

Identifizierungssysteme steuern Verfahren zum Nachweis und zur Überprüfung der Identität natürlicher oder juristischer Personen sowie Verfahren zur Ausstellung der beantragten elektronischen Identifizierungsmittel. Sie beinhalten den Authentifizierungsmechanismus, bei dem die natürliche oder juristische Person elektronische Identifizierungsmittel verwendet, um einem vertrauenden Beteiligten gegenüber ihre Identität zu bestätigen.
Beispielsweise ermöglicht hier die Identifizierung mittels des Neuen Personalausweises berechtigten Organisationen die eindeutige Überprüfung der Identität einer natürlichen Person, z.B. bei der Anmeldung an einem Portal zur Einreichung von Anträgen oder der Erteilung von Auskünften wie bspw. aus dem Kfz-Zentralregister des KBA.

Elektronische Identifizierungsmittel werden durch festgelegte Sicherheitsniveaus europaweit klassifiziert und wie beschrieben innerhalb des eID-Systems betrieben. Die Beziehung ist nachstehend dargestellt.

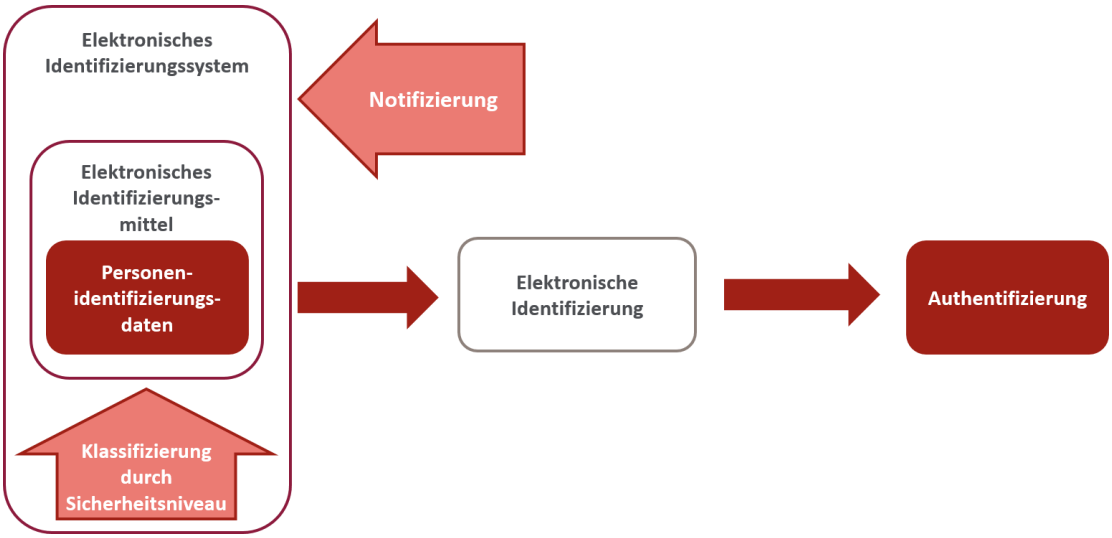


Abbildung 5: Beziehung Identifizierungssystem und Identifizierungsmittel

Die Notifizierung eines elektronischen Identifizierungssystems stellt eine elementare Grundlage für die europaweite Anerkennung des Produkts dar. Dafür sind folgende Anforderungen zu erfüllen:

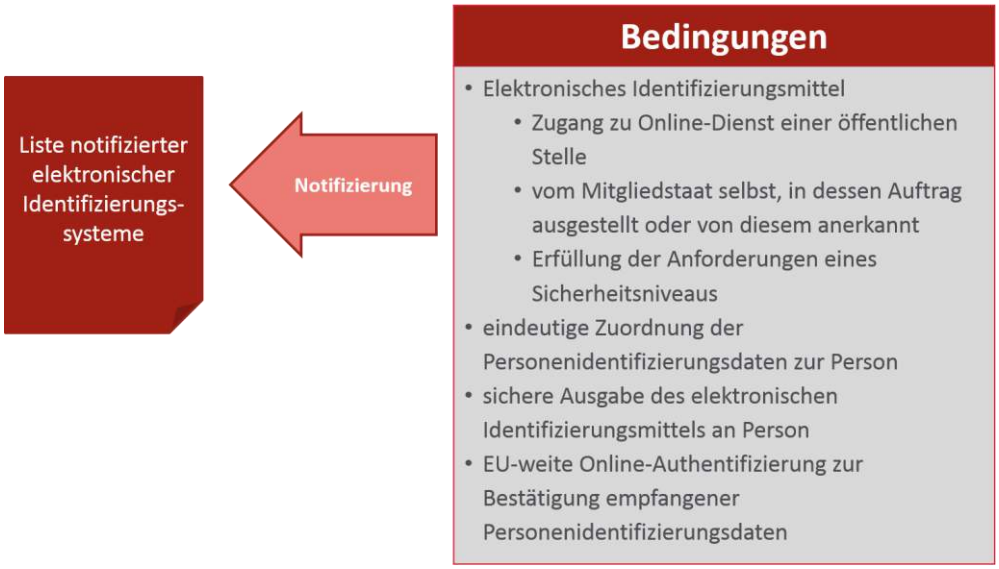


Abbildung 6: Bedingungen zur Notifizierung von eID-Systemen

Die Notifizierung selbst wird in den jeweiligen EU-Staaten vorgenommen. In Deutschland könnte dies hinsichtlich der fachlich-technischen Prüfung zum Beispiel das Bundesamt für Sicherheit in der Informationstechnik sein. Die Details hierzu werden aktuell in Ausführungsbestimmungen erarbeitet. Die Sicherheit elektronischer Identifizierungssysteme und die Verwendung der je nach Sicherheitsniveau (niedrig, substanziell oder hoch) zugelassenen materiellen und immateriellen Identifizierungsmittel (zum Beispiel Smart-Cards, USB-Token oder andere geeignete Mittel) sind ein weiterer wesentlicher Faktor für die Notifizierung als vertrauenswürdige grenzüberschreitende gegenseitige Anerkennung elektronischer Identifizierungsmittel, beispielsweise über qualifizierte Vertrauensdiensteanbieter.
Für die grenzüberschreitende Anerkennung elektronischer Identifizierungsmittel (zum Beispiel des Neuen Personalausweises) sind über die Notifizierung hinaus folgende Bedingungen zu erfüllen:

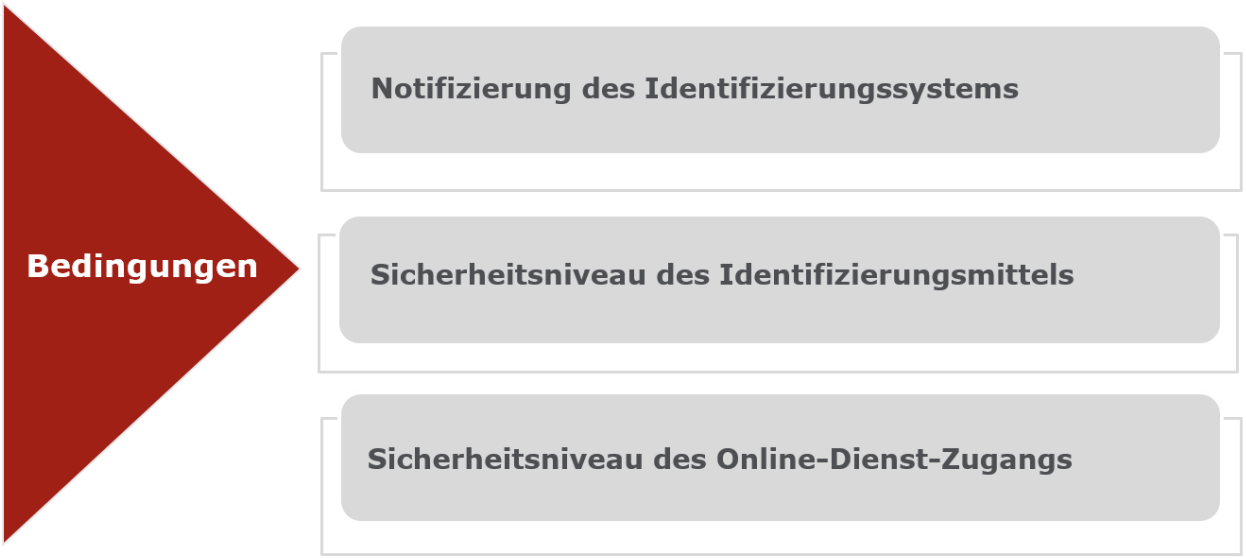


Abbildung 7: Bedingungen für die grenzüberschreitende Anerkennung von Identifizierungsmitteln

Konkret bedeutet das für Behörden, dass sie ab 1.7.2018 verpflichtet sind EU-weit alle elektronischen Identifizierungsmittel, die die oben genannten Bedingungen erfüllen, anzuerkennen. Folglich müssen organisatorische und technische Voraussetzungen zur elektronischen Annahme und Durchführung der Authentifizierung geschaffen werden. Unternehmen können diese Regelung nutzen, um die vertrauenswürdige elektronische Kommunikation mit ausländischen Behörden zu vereinfachen.

2.3 Elektronische Vertrauensdienste

Gemäß der Verordnung stehen neben elektronischen Identifizierungssystemen und -mitteln folgende elektronische Vertrauensdienste zur Abwicklung vertrauenswürdiger elektronischer Transaktionen zur Verfügung.

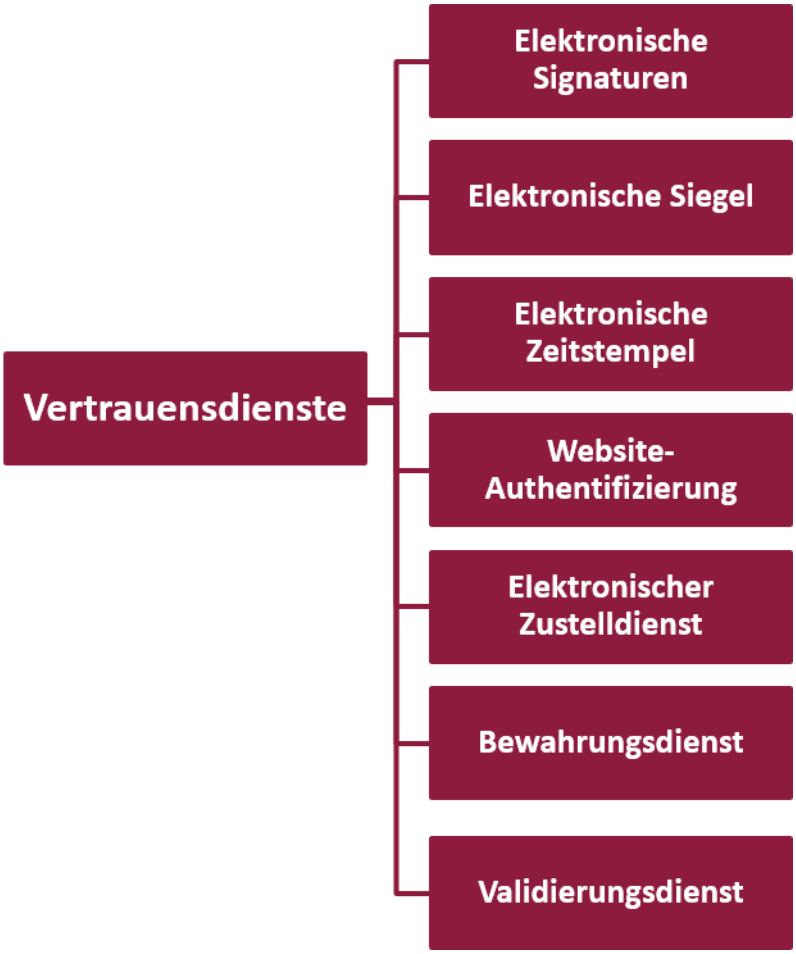


Abbildung 8: Vertrauensdienste gemäß der eIDAS-Verordnung

Als elektronischer Vertrauensdienst gilt ein IT-Service, der

- die Erstellung, Überprüfung und/oder Validierung elektronischer Signaturen, Zeitstempel, Siegel sowie elektronischer Einschreiben und/oder von Website-Zertifikaten und/oder
- die beweissichere Bewahrung qualifiziert elektronisch signierter Dokumente in der Regel gegen Entgelt ermöglicht

Dabei ist zu beachten, dass qualifizierte elektronische Siegel technisch eine qualifizierte elektronische Signatur tragen. Sie sind folglich bei den Bewahrungsdiensten ebenso relevant wie Nachweise für elektronische Einschreiben, sofern diese, wie aktuell bei De-Mail, qualifiziert elektronisch signiert sind.

Somit unterstützt die eIDAS-Verordnung vertrauenswürdige elektronische Geschäftsprozesse und Dokumentation im vollständigen Lebenszyklus geschäftsrelevanter elektronischer Dokumente.

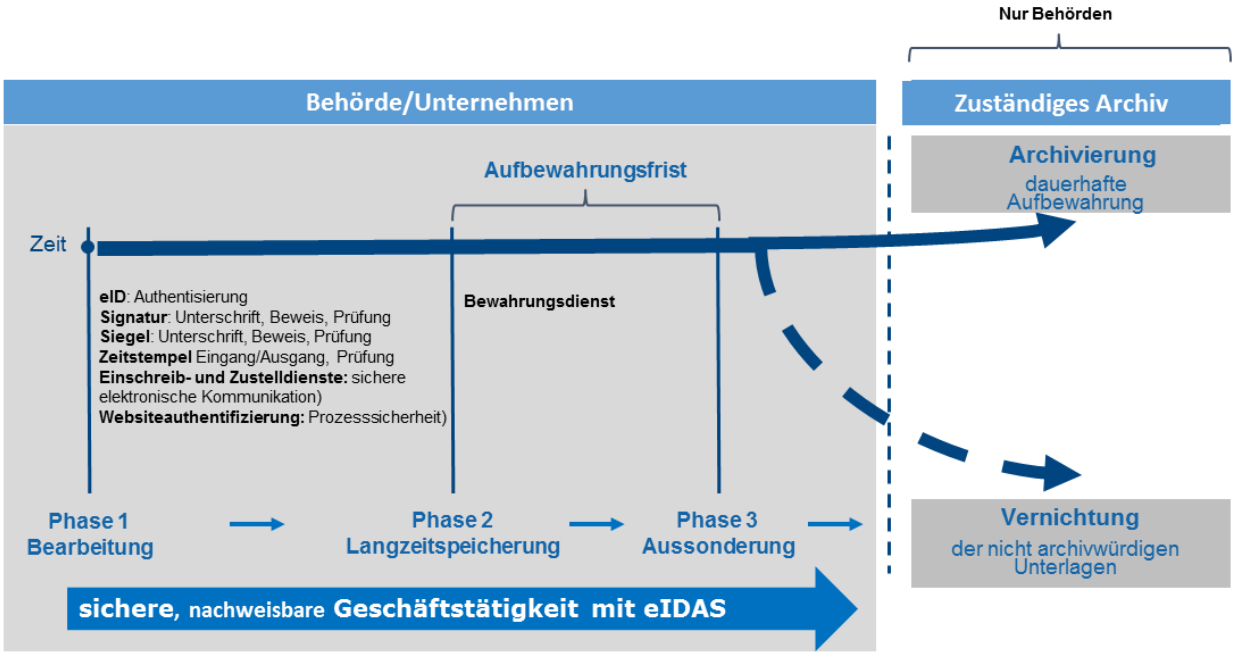


Abbildung 9: Anwendungsbereich der eIDAS-Verordnung

Die genannten Vertrauensdienste werden von sogenannten Vertrauensdiensteanbietern (VDA) erbracht. Dabei kann es sich um natürliche oder juristische Personen handeln, die Vertrauensdienste anbieten. Ein VDA, der sich einer Konformitätsprüfung durch eine unabhängige Zertifizierungsstelle gegen die Anforderungen der eIDAS-Verordnung beziehungsweise der zugrundeliegenden Standards und Normen erfolgreich unterzieht (Notifizierung), wird als qualifizierter Vertrauensdiensteanbieter bezeichnet. Wesentliche Vorteile sind:

- europaweit verpflichtende Anerkennung der Produkte des Vertrauensdiensteanbieters durch öffentliche Stellen (Ausnahme: Einschreib- und Zustelldienste)
- Eintragung in öffentlich einsehbare Vertrauenslisten (Trusted List) national sowie europaweit
- Verleihung des europäischen Vertrauenssiegels

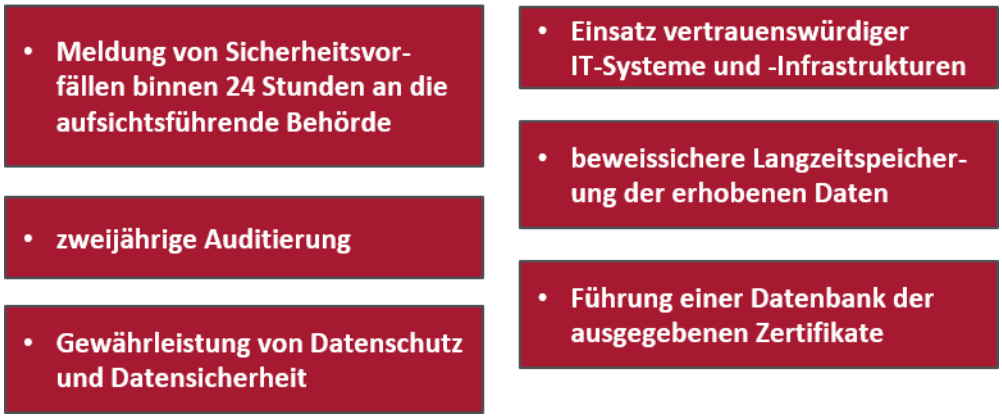
Folgende Vertrauensdienste sind nur für qualifizierte Vertrauensdiensteanbieter möglich:

- **Validierungsdienste**
  → Prüfung von (qualifizierten elektronischen) Signaturen, Siegeln und Zeitstempeln
- **Bewahrungsdienste**
  → beweissichere Langzeitspeicherung
- **Einschreib- und Zustelldienste**
  → vertrauenswürdige Kommunikation und nachweisbare Zustellung

Erst nach der erfolgreichen Zertifizierung und Eintragung in die Vertrauensliste darf das Vertrauenssiegel genutzt und der Betrieb als qualifizierter Vertrauensdiensteanbieter aufgenommen werden. Somit wird für Anwender transparent, welcher Anbieter die Maßgaben der eIDAS-Verordnung erfüllt und **zertifiziert** einen vertrauenswürdigen Dienst für vertrauenswürdige elektronische Geschäftsprozesse anbietet.

Für den qualifizierten Vertrauensdiensteanbieter gelten weiterhin folgende Anforderungen:

- Haftung für alle vorsätzlich oder fahrlässig erzeugten Schäden gegenüber natürlichen oder juristischen Personen
- Gewährleistung der Sicherheitsanforderungen an den Dienstbetrieb, die faktisch einer Zertifizierung nach ISO 27001 entsprechen und folgende Aspekte umfassen:



Die Beweislast liegt beim qualifizierten Vertrauensdiensteanbieter!

Je EU-Land wird eine Aufsichtsinstanz, ein sogenannter Supervisory Body, geschaffen. Diese trägt insbesondere die Verantwortung für:

- Aufsicht und Überwachung der qualifizierten Vertrauensdiensteanbieter
- Aufsicht und Überwachung der unabhängigen Zertifizierungsstelle für Konformitätsprüfungen gemäß eIDAS-Verordnung zur Erlangung des Status eines qualifizierten Vertrauensdiensteanbieters

Die folgende Grafik zeigt die Aufgaben der Aufsichtsinstanz im Überblick:

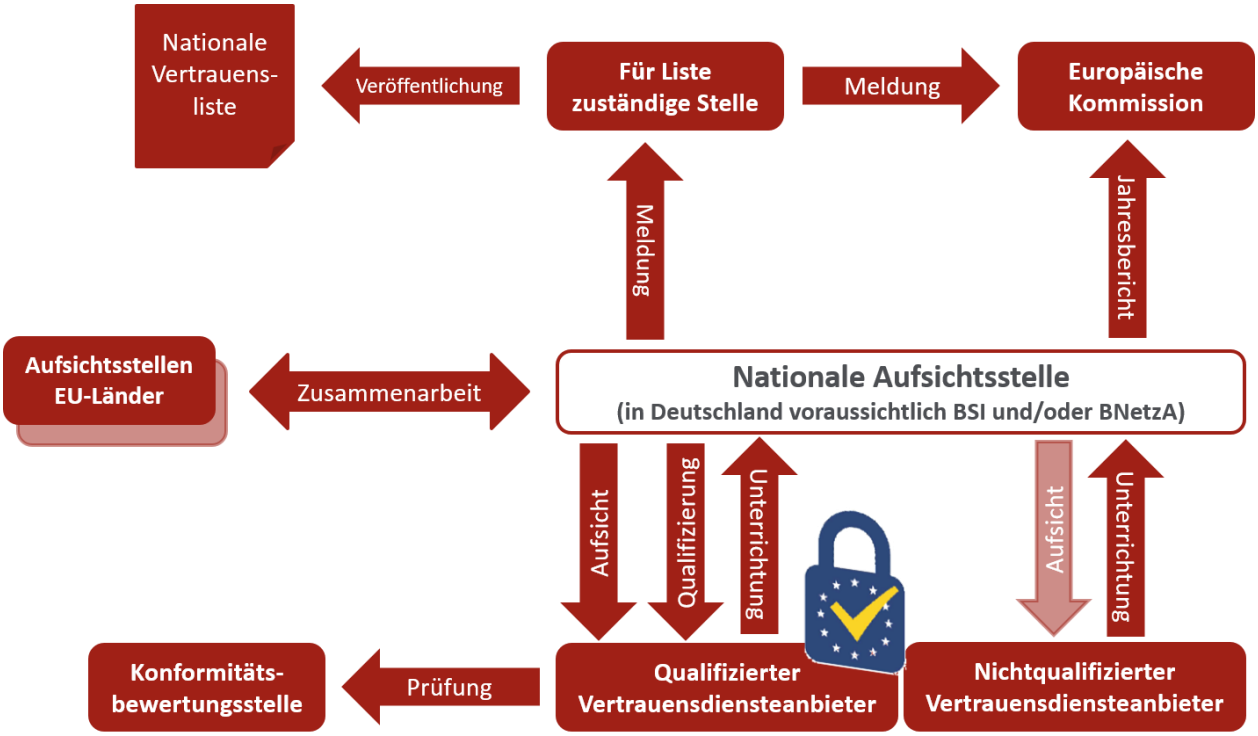


Abbildung 10: Stellung und Aufgaben der nationalen Aufsichtsstelle gemäß eIDAS-Verordnung

In Deutschland werden dies voraussichtlich das BSI und/oder die Bundesnetzagentur sein.

2.3.1 Vertrauensdienste für (qualifizierte) elektronische Signaturen

Elektronische Signaturen sind Daten in elektronischer Form, die anderen elektronischen Daten beigefügt oder logisch mit ihnen verbunden werden und die der Unterzeichner zum Unterschreiben verwendet. Eine qualifizierte elektronische Signatur stellt eine fortgeschrittene elektronische Signatur dar, die mit einer qualifizierten elektronischen Signaturerstellungseinheit generiert wurde und auf einem qualifizierten Zertifikat für elektronische Signaturen eines qualifizierten Vertrauensdiensteanbieters beruht. Die eIDAS-Verordnung spezifiziert die Formate der Signaturen (zum Beispiel CAdES, XAdES etc.)[5], um die EU-weite Interoperabilität zu gewährleisten, beschränkt aber das Medium (das Qualifizierungsmittel) nicht mehr auf eine Chipkarte. Vielmehr ist es zulässig, die elektronischen Daten auch softwareseitig beziehungsweise in Hardware Security Modules (HSM) vorzuhalten, was die Anwendung von Signaturen und ihren Prozessen enorm erleichtert.

[5] Vgl. Kap. 3.1.1

Die qualifizierte elektronische Signatur wird als einziges Pendant zur elektronischen Unterschrift anerkannt und genießt den vollen Beweiswert.

Für elektronische Signaturen sind folgende Dienste vorgesehen:

- Erzeugung und Überprüfung elektronischer Signaturen (sowie Siegel und Zeitstempel)
- Validierung qualifizierter elektronischer Signaturen (sowie Siegel und Zeitstempel)

Die Validierung der qualifizierten elektronischen Signatur (wie auch des Siegels) darf nur durch qualifizierte Vertrauensdienste erbracht werden. Dies schafft eine zusätzliche Sicherheit und Vertrauenswürdigkeit.

2.3.2 Vertrauensdienste für (qualifizierte) elektronische Siegel

Elektronische Siegel sind Daten in elektronischer Form, die anderen Daten in elektronischer Form beigefügt oder logisch mit ihnen verbunden werden, um deren Ursprung und Unversehrtheit sicherzustellen. Qualifizierte elektronische Siegel sind fortgeschrittene elektronische Siegel, die von einer qualifizierten elektronischen Siegelerstellungseinheit erstellt werden und auf einem qualifizierten Zertifikat für elektronische Signaturen eines qualifizierten Vertrauensdiensteanbieters beruhen. Technisch ist ein qualifiziertes elektronisches Siegel somit eine qualifizierte elektronische Signatur basierend auf einem Organisationszertifikat – also ein Zertifikat für eine Behörde, ein Unternehmen, etc. Die eIDAS-Verordnung spezifiziert die Formate der Siegel, um die EU-weite Interoperabilität zu gewährleisten, beschränkt aber das Medium (Qualifizierungsmittel) nicht mehr auf eine Chipkarte. Es ist zulässig, die elektronischen Daten auch softwareseitig beispielsweise in Hardware Security Modules (HSM) vorzuhalten, was die Anwendung von Siegeln und ihren Prozessen enorm erleichtert.

Das qualifizierte elektronische Siegel ist eine qualifizierte elektronische Signatur, beruhend auf einem Zertifikat für eine komplette Organisation. Rechtlich entspricht es der qualifizierten elektronischen Signatur, ersetzt also Schriftform und genießt den vollen Beweiswert.

Für elektronische Siegel sind folgende Dienste vorgesehen:

- Erzeugung und Überprüfung elektronischer Siegel
- Validierung qualifizierter elektronischer Siegel

2.3.3 Vertrauensdienste für (qualifizierte) elektronische Zeitstempel

Elektronische Zeitstempel bezeichnen Daten in elektronischer Form, die andere Daten in elektronischer Form mit einem bestimmten Zeitpunkt verknüpfen und nachweisen, dass diese anderen Daten zu diesem Zeitpunkt vorhanden waren. Qualifizierte elektronische Zeitstempel sind elektronische Zeitstempel, die Datum und Zeit in der Form mit Daten verknüpfen, dass die Möglichkeit der unbemerkten Veränderung der

Daten nach vernünftigem Ermessen ausgeschlossen ist. Außerdem beruhen sie auf einer korrekten Zeitquelle, die mit der koordinierten Weltzeit verknüpft ist. Qualifizierte elektronische Zeitstempel tragen eine fortgeschrittene elektronische Signatur oder ein fortgeschrittenes elektronisches Siegel des qualifizierten Vertrauensdiensteanbieters. Die eIDAS-Verordnung spezifiziert lediglich die Formate der Signaturen und. Zeitstempel (wie RFC3161), um die EU-weite Interoperabilität zu gewährleisten.

Für elektronische Zeitstempel sind folgende Dienste vorgesehen:

- Erzeugung elektronischer Zeitstempel
- Prüfung/Validierung elektronischer Zeitstempel

Wesentliche Maßgaben zu qualifizierten Zeitstempeln sind:

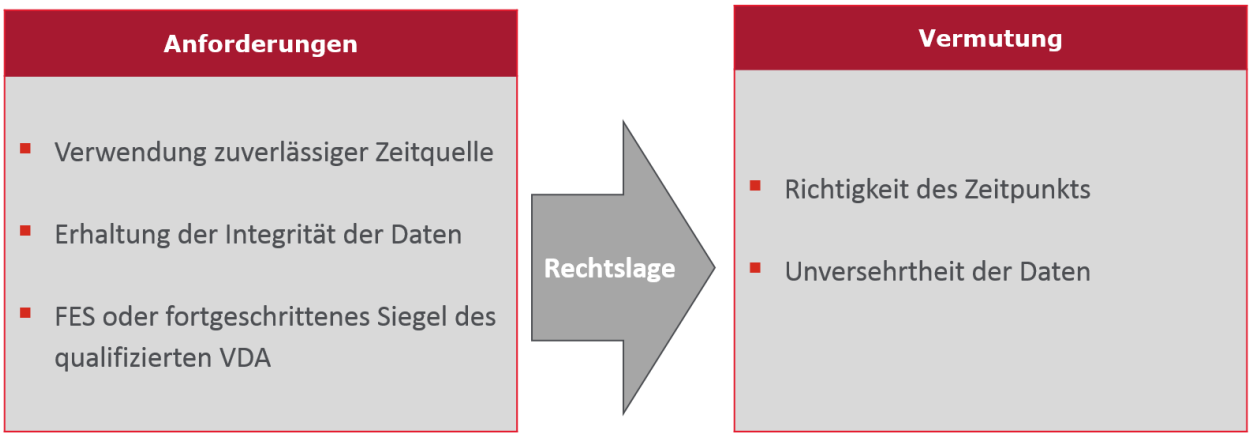


Abbildung 11: Wesentliche Maßgaben qualifizierter Zeitstempel

2.3.4 (Qualifizierte) elektronische Einschreib- und Zustelldienste

Dienste für die Zustellung elektronischer Einschreiben sind Dienste, die die Übermittlung von Daten zwischen Dritten mit elektronischen Mitteln ermöglichen und einen Nachweis der Handhabung der übermittelten Daten erbringen, darunter den Nachweis der Absendung und des Empfangs der Daten. Die Dienste schützen die übertragenen Daten vor Verlust, Diebstahl, Beschädigung oder unbefugter Veränderung. Qualifizierte Dienste für die Zustellung elektronischer Einschreiben sind Dienste, die von mindestens einem qualifizierten Vertrauensdiensteanbieter bereitgestellt werden und die Identifizierung des Absenders mit einem hohen Maß an Vertrauenswürdigkeit sowie die Identifizierung des Empfängers noch vor der Zustellung der Daten gewährleisten. Sie sichern das Absenden und Empfangen der Daten durch eine fortgeschrittene elektronische Signatur oder ein fortgeschrittenes elektronisches Siegel eines qualifizierten Vertrauensdiensteanbieters in der Form ab, dass die Möglichkeit einer unbemerkten Veränderung der Daten ausgeschlossen ist. Datum und Zeitpunkt des Absendens, Empfangens oder eine Änderung der Daten

werden durch einen qualifizierten elektronischen Zeitstempel angezeigt. In Deutschland wird dies derzeit durch den De-Mail-Dienst realisiert.

Wesentliche Maßgaben für Einschreib- und Zustelldienste sind:

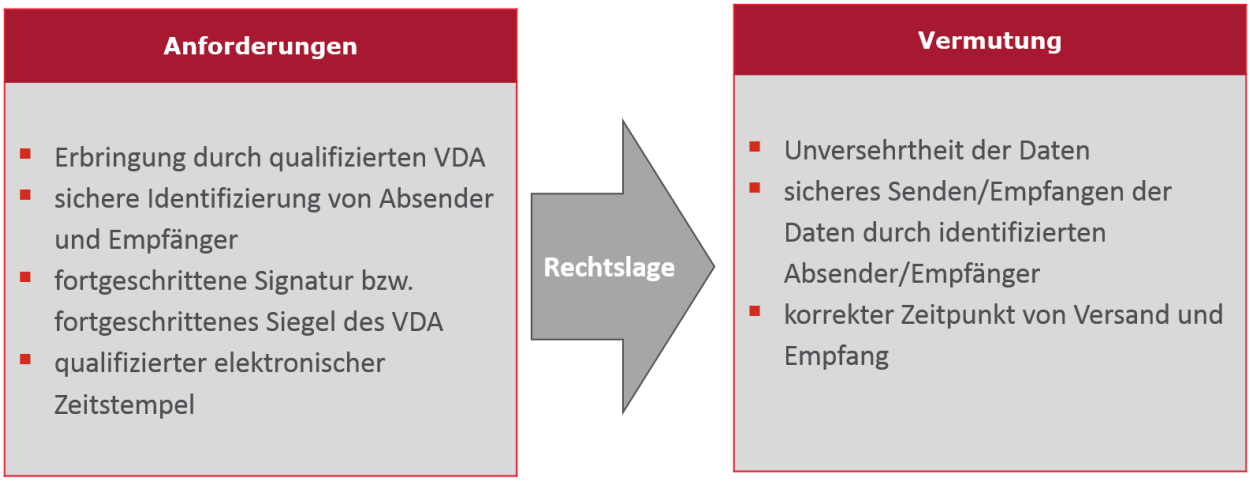


Abbildung 12: Wesentliche Maßgaben qualifizierter Einschreib- und Zustelldienste

2.3.5 (Qualifizierte) elektronische Bewahrungsdienste für (qualifizierte) elektronische Signaturen

Elektronische Bewahrungsdienste gewährleisten die Speicherung von elektronischen Signaturen, Siegeln und Zertifikaten. Zur Beweiswerterhaltung fordern die eIDAS-Verordnung und ihre untersetzenden Ausführungsbestimmungen die periodische Signatur- und Hasherneuerung, sobald die Sicherheitseignung der zugrundeliegenden Algorithmen nicht mehr gegeben ist. In Deutschland entspricht die Bewahrung nach BSI TR-ESOR-Standard dem aktuellen Stand der Technik.

Der Dienst selbst kann nur von qualifizierten Vertrauensdiensteanbietern erbracht werden. Betreiben Behörden oder Unternehmen selbst einen Bewahrungsdienst so bezieht sich dieser auf einen geschlossenen Benutzerkreis und liegt somit nicht im Geltungsbereich der eIDAS-Verordnung. Dennoch ist es ratsam die Vorgaben der Verordnung einzuhalten, um einen möglichst hohen Beweiswert zu erhalten.

2.3.6 Vertrauensdienste für (qualifizierte) Zertifikate für die Website-Authentifizierung

Zertifikate für die Website-Authentifizierung ermöglichen die Authentifizierung einer Website und verknüpfen sie mit jener natürlichen oder juristischen Person, für die das Zertifikat ausgestellt wurde. Qualifizierte Zertifikate für die Website-Authentifizierung werden von einem qualifizierten Vertrauensdiensteanbieter

ausgestellt und für Website-Authentifizierungsdienste verwendet, die dem Besucher einer Website gewährleisten, dass hinter der Website eine echte und rechtmäßige Einrichtung steht.
Die eIDAS-Verordnung legt Anforderungen an qualifizierte Zertifikate für die Website-Authentifizierung fest und nennt die Angaben, die ein solches Zertifikat enthalten muss. Dazu zählen u.a. Name und Adresse des Betreibers sowie Namen der Domänen, die von ihm betrieben werden.

2.4 Fahrplan für die Umsetzung der eIDAS-Verordnung

Derzeit sind die wesentlichen Ausführungsbestimmungen (Durchführungsrechtsakte, bzw. *engl.: Implementing Acts*) zur Detaillierung der grundlegenden Vorgaben der eIDAS-Verordnung in der Erarbeitungsphase. Mit dem Mandat M460 wurden die europäischen Normungsinstitute ETSI und CEN beauftragt, die notwendigen begleitenden technischen Normen zu entwickeln. Nicht alle in der Regelung definierten Vertrauensdienste sind von den Durchführungsrechtsakten in gleicher Weise betroffen. Die nachstehende Tabelle zeigt den Fahrplan für die Umsetzung der eIDAS-Verordnung:

Maßnahme	Datum/Zeitraum
Befugnis zum Erlass delegierter Rechtsakte/Durchführungsrechtsakte	Seit 17.09.2014
Gestaltung EU-Vertrauenssiegel	Seit 01.07.2015
Notifizierung von Vertrauensdiensten möglich[6]	Seit September 2015
Erstellung der verpflichtenden Durchführungsrechtsakte durch die EU	
Sicherheitsniveaus	Liegen seit 18.09.2015 vor
Detaillierung hinsichtlich Vertrauenslisten	Liegen seit 18.09.2015 vor
Formate für fortgeschrittene elektronische Signaturen beziehungsweise Referenzverfahren, sofern andere Formate genutzt werden	Liegen seit 18.09.2015 vor

[6] Voraussetzung: Durchführungsrechtsakte (Implementing Acts) zu den Sicherheitsniveaus und Interoperabilitätsrahmen liegen vor

Maßnahme	Datum/Zeitraum
Formate für fortgeschrittene elektronische Siegel beziehungsweise Referenzverfahren, sofern andere Formate genutzt werden	Liegen seit 18.09.2015 vor
Erstellung der notwendigen ETSI/CEN-Normen	Ende 2015
Geltung der Verordnung speziell für Vertrauensdienste	01.07.2016
Pflicht zur Anerkennung notifizierter (qualifizierter) Vertrauensdienste (insbesondere der qualifizierten elektronischen Signatur, der qualifizierten elektronischen Zeitstempel, der qualifizierten elektronischen Siegel sowie der Validierungsdienste und Bewahrungsdienste)	01.07.2016
Pflicht zur Anerkennung notifizierter eID/Authentisierungsdienste (gilt nur für Behörden)	18.09.2018

Die Gremienstruktur zur Erarbeitung der Ausführungsbestimmungen sowie der fachlichen und technischen europäischen Normen, die diese untersetzen, gestaltet sich folgendermaßen:

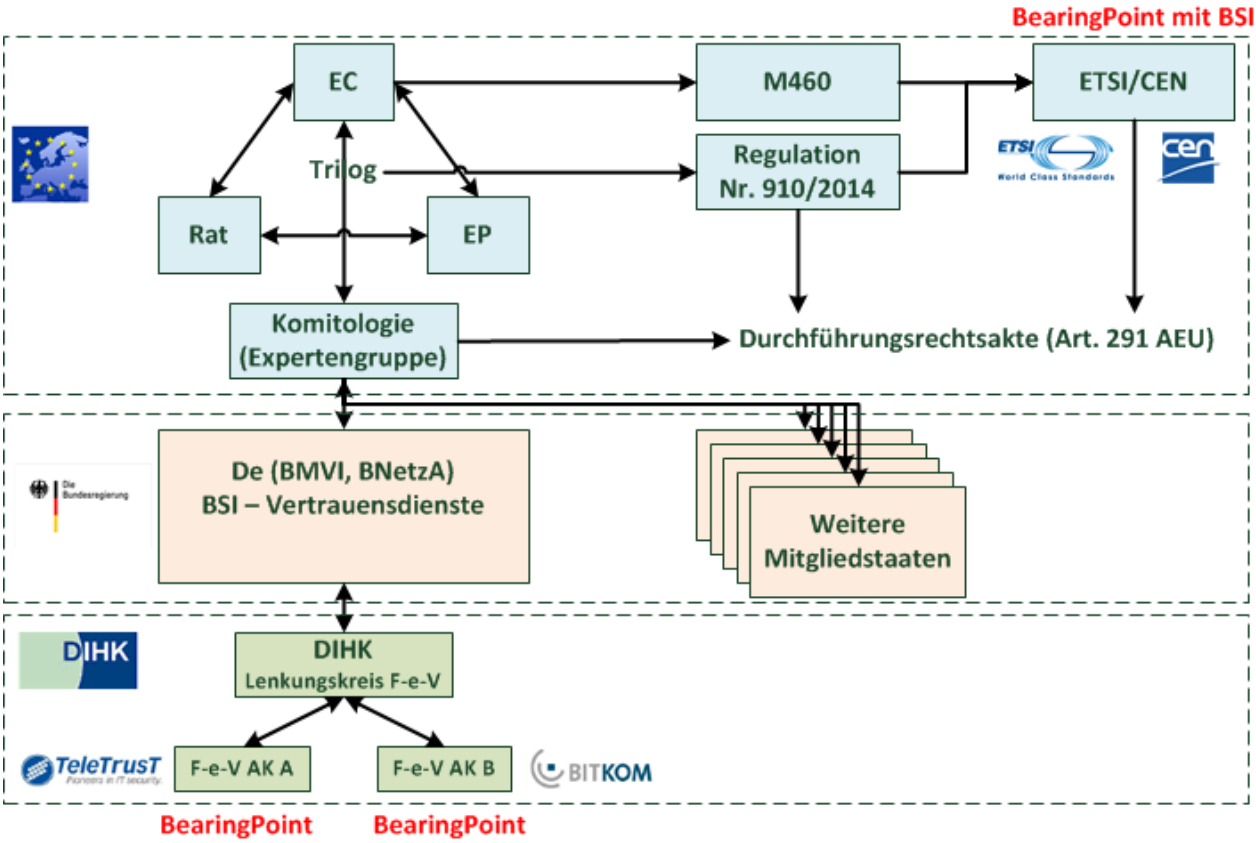


Abbildung 13: Gremienstruktur für Ausführungsbestimmungen und Normen

2.5 Status quo und mögliche Anpassungsbedarfe in Deutschland

Die eIDAS-Verordnung definiert Anforderungen an elektronische Signaturen, Zeitstempel, Siegel, Bewahrungsdienste, Zustelldienste und Authentisierungslösungen. Damit sind unmittelbar Kerninhalte des E-Government-Gesetzes des Bundes sowie potenziell der Länder betroffen, zum Beispiel die Verpflichtung zur Eröffnung eines Zugangs für

- elektronische Signatur
- den Neuen Personalausweis
- De-Mail

Ergänzt werden müsste diese Verpflichtung um die qualifizierten Vertrauensdienste für die qualifizierte elektronische Signatur sowie das qualifizierte elektronische Siegel bzw. – mit Geltung ab 2018 – für eID-Lösungen. Gleiches ist für Zustelldienste, also Alternativen zu De-Mail, empfehlenswert, um grenzüberschreitende Geschäftsprozesse zu erleichtern. Daneben wäre der Ersatz der Schriftform um das qualifizierte elektronische Siegel zu erweitern, das als faktische Organisationssignatur gemäß eIDAS-Verordnung angewendet werden kann. Ebenso wäre denkbar, hinsichtlich der Langzeitspeicherung auf die Bewahrungsdienste gemäß eIDAS-Verordnung zu verweisen, die ein europaweit standardisiertes Vorgehen zur

beweissicheren Langzeitspeicherung ermöglichen und Kosteneinsparungen implizieren. Weitere absehbare Änderungen ergeben sich für Signaturgesetz und Signaturverordnung hinsichtlich der Definition und Erzeugung qualifizierter elektronischer Signaturen, qualifizierter elektronischer Zeitstempel und qualifizierter elektronischer Siegel sowie Validierungslösungen. Die Auswirkungen auf die E-Government-Gesetze und das eJustice-Gesetz werden Anpassungen im Verwaltungsverfahrensgesetz, in der Zivilprozessordnung und im Bürgerlichen Gesetzbuch nach sich ziehen. Von weiteren Änderungen werden das Passgesetz und das Aufenthaltsgesetz betroffen sein. Die folgende Tabelle zeigt die beispielhaften Auswirkungen im Überblick.

Rechtsgrundlage	Relevanter Kerninhalt	Wesentliche Erweiterungen gemäß eIDAS-Verordnung	Relevante qualifizierte Vertrauensdienste gemäß eIDAS-Verordnung
EGovG Bund	Eröffnung eines Zugangs für qualifizierte elektronische Signaturen	- Erweiterung auf alle qualifizierten elektronischen Signaturen qualifizierter Vertrauensdiensteanbieter - Ergänzung um Eröffnung eines Zugangs für qualifizierte elektronische Siegel qualifizierter Vertrauensdiensteanbieter	Elektronische Signatur Elektronisches Siegel
	E-Akte/Langzeitspeicherung	Nutzung qualifizierter Bewahrungsdienste zur Beweiswerterhaltung signierter Dokumente	Bewahrungsdienste
	Eröffnung eines De-Mail-Kontos	De-Mail als qualifizierter Zustelldienst - Echtheitsvermutung - Grenzüberschreitende, vertrauenswürdige elektronische Kommunikation	Elektronische Einschreib- und Zustelldienste
SigG, SigV	Qualifizierte elektronische Signatur	- Erweiterung um elektronische Siegel - Erweiterung der Erzeugungsoptionen für die qualifizierte elektronische Signatur (USB-Token, Signaturkarte, Serverzertifikat), ggf. nationale Spezifizierung der Validierungsdienste	Elektronische Signatur Validierungsdienste
VwVfG	Schriftform	Ergänzung um Besiegelung anhand elektronischer Siegel	Elektronische Siegel
ZPO	Beweiswert	Berücksichtigung des elektronischen Siegels sowie weiterer Zustelldienste neben De-Mail	Elektronische Siegel Elektronische Einschreib- und Zustelldienste
BGB	Schriftform	Ergänzung um Besiegelung anhand elektronischer Siegel	Elektronische Siegel

2.6 Zusammenfassung der rechtlichen Aspekte

Die Kerninhalte der eIDAS-Verordnung aus rechtlicher Sicht sind nachstehend dargestellt:

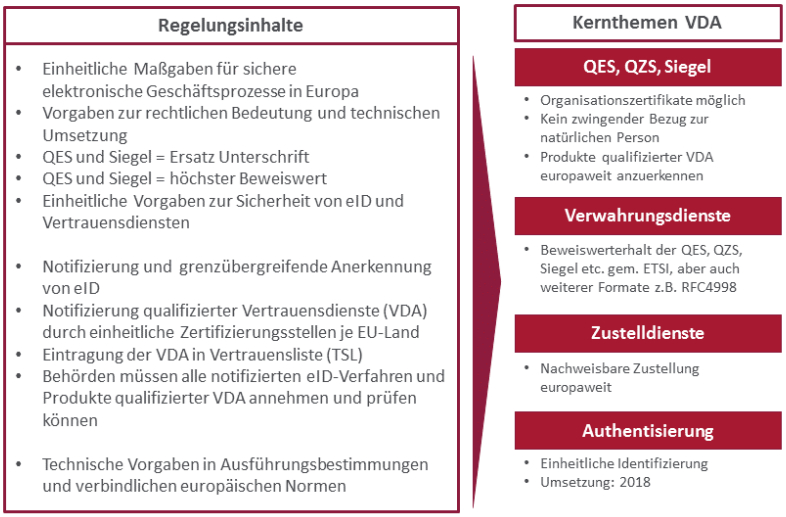


Abbildung 14: Kerninhalte der eIDAS-Verordnung

Mit der elektronischen Identifizierung sowie elektronischen Vertrauensdiensten werden einheitliche Maßgaben für vertrauenswürdige, nachweisbare elektronische Geschäftsprozesse und die Langzeitspeicherung geschaffen. Die eIDAS-Verordnung bildet somit künftig das regulatorische Dach zur Abbildung vertrauenswürdiger elektronischer Geschäftsprozesse in Europa. Nationale Regelungen werden an die eIDAS-Verordnung angepasst.

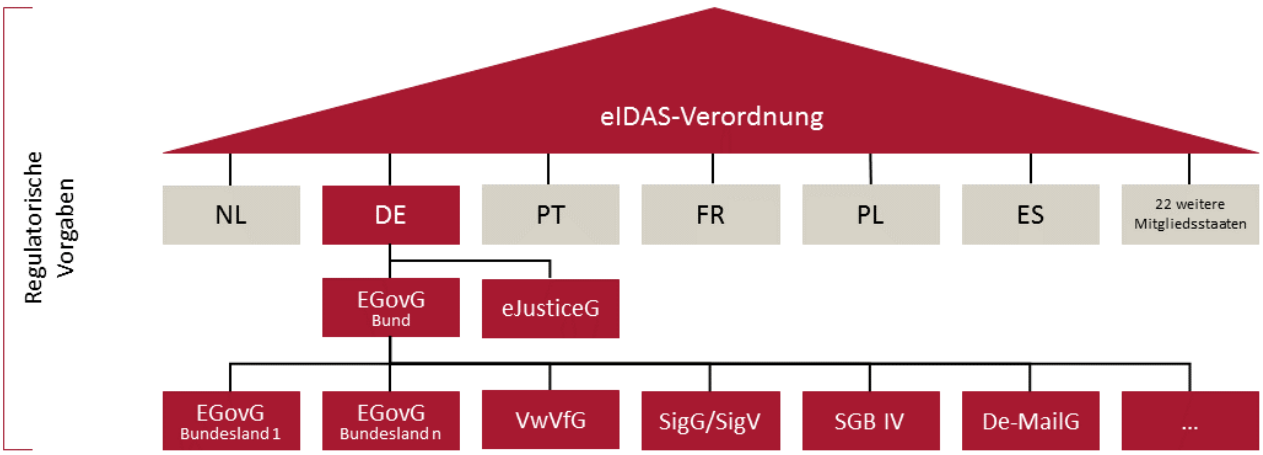


Abbildung 15: Rolle der eIDAS-Verordnung

Somit wird eine einheitliche Grundlage für die beweissichere elektronische Geschäftstätigkeit für Unternehmen, Behörden und Bürger geschaffen – zur Erreichung europaweiter Rechtssicherheit.

3 Fachlich-technischer Rahmen

Nach der Beschreibung der rechtlichen Vorgaben erläutert das dritte Kapitel die fachlich-technischen Aspekte der eIDAS-Verordnung und nennt die Standards und Initiativen, untergliedert in die verschiedenen Signaturarten - wie die personenbezogene qualifizierte elektronische Signatur, das qualifizierte elektronische (Organisations-) Siegel und den qualifizierten elektronischen Zeitstempel. Wir berichten über den aktuellen Stand und die möglichen Anpassungsbedarfe in Deutschland und beschreiben die Relevanz der eIDAS-Verordnung im weltweiten Kontext.

Kurz und bündig:

Die eIDAS-Verordnung bietet den rechtlichen Rahmen für technische Standards und Normen zum Beispiel von ETSI, CEN, DIN und ISO.

Einige dieser Normen haben verbindlichen Charakter. Dazu zählen die Standards zu Signatur- und Siegelformaten, zur Ausgestaltung der Vertrauenslisten und zu den Sicherheitsniveaus für elektronische Identifizierungsmittel.

Einheitliche europäische Standards bewirken eine Harmonisierung der Vertrauensdienste t, was deren grenzüberschreitende Verwendung enorm vereinfacht und zu einer einheitlichen Rechtssicherheit beiträgt. Als Folge ist eine Zunahme der Nutzung elektronischer Vertrauensdienste und elektronischer Geschäftsprozesse generell zu erwarten.

3.1 Grundsatz und Überblick

Eine nachhaltige Geschäftstätigkeit von Behörden und Unternehmen gewährleistet die Authentizität, Integrität, Verfügbarkeit und Verkehrsfähigkeit geschäftsrelevanter Unterlagen unter Wahrung der geltenden rechtlich-organisatorischen Vorgaben (Compliance) bis zum Ablauf der geltenden Aufbewahrungsfristen.

Dies erfordert die Erzeugung beziehungsweise den Empfang und Austausch sowie die Bewahrung beweiskräftiger Unterlagen in der Form, dass die eigenen Geschäftsprozesse und Entscheidungen gegenüber Dritten eindeutig nachweisbar sind und Dokumentationsvorgaben eingehalten werden. Die eIDAS-Verordnung unterstützt dies für elektronische Geschäftsprozesse durch europaweit einheitliche rechtliche wie fachlich-technische Vorgaben.

Wie in Kapitel 2 beschrieben, stecken die Inhalte der eIDAS-Verordnung nur einen rechtlichen Rahmen ab - als Fundament für die nachkommenden fachlichen und technischen Vorgaben und Empfehlungen. Diese werden mithilfe von sogenannten Durchführungsrechtsakten veröffentlicht und verweisen in der Regel auf die durch ETSI und CEN erarbeiteten technischen Spezifikationen und Normen, die zum Teil bereits vorliegen oder gegenwärtig entwickelt bzw. erneuert werden.

Eine weitere Säule der Betrachtung der fachlichen und technischen Aspekte stellen zusätzliche nationale und internationale Standards (z. B. DIN bzw. ISO) dar. Insbesondere im internationalen Kontext agierende Institutionen und Unternehmen gehören zur Gruppe der starken Verfechter solcher Normen und wenden diese erhöht an. Im Weiteren werden zunächst die relevanten europäischen Normen und Standards sowie Projekte und Initiativen vorgestellt. Es folgt eine Übersicht über die deutschen Regularien und eine kurze Darstellung aus internationaler Sicht.

3.2 Europäische Standards und Initiativen auf Basis der eIDAS-Verordnung

3.2.1 Grundsatz & Überblick

Die Organisationen ETSI und CEN nehmen die Rolle eines europäischen Standardisierungsgremiums ein, das mit der Ausgabe des Standardisierungsmandats M460 EN für den Bereich Informations- und Kommunikationstechnologie angewandt auf elektronische Signaturen initiiert wurde. Der Bezug zwischen der eIDAS-Verordnung, ihren Ausführungsbestimmungen und den fachlich-technischen Normen gestaltet sich wie folgt:

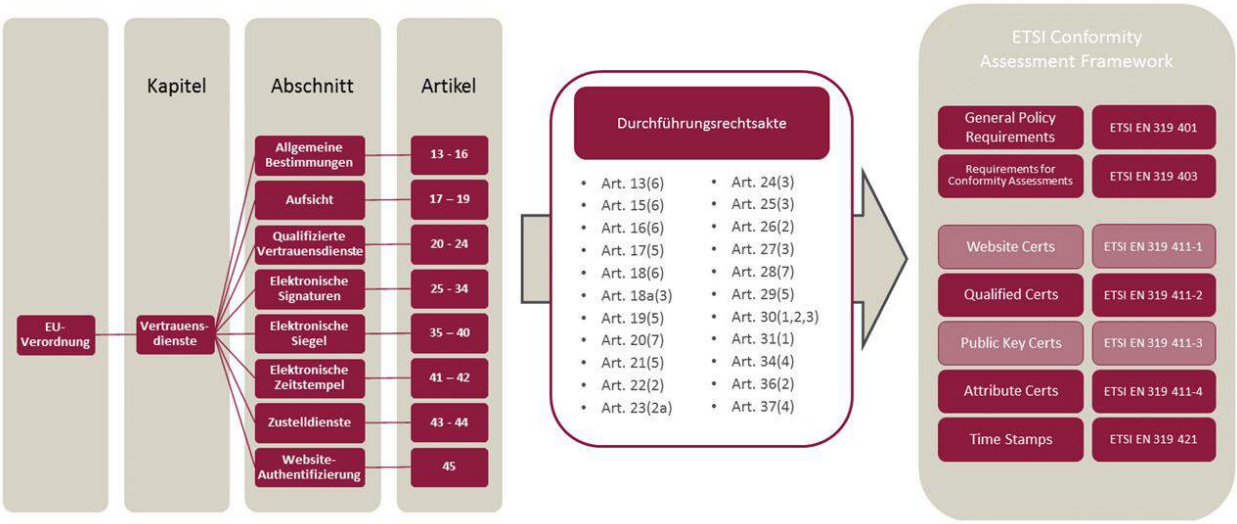


Abbildung 16: Beziehung zwischen Verordnung und fachlich-technischen Normen

Auf die Normen wird in den Ausführungsbestimmungen explizit verwiesen. Somit sind diese für die Umsetzung und Anwendung der eIDAS-Verordnung verbindliche Vorgaben.

Die mit der Erstellung der fachlich-technischen Normen verbundenen Aktivitäten wurden in Form eines Rahmenwerks in sechs getrennten Handlungsbereichen zusammengefasst:

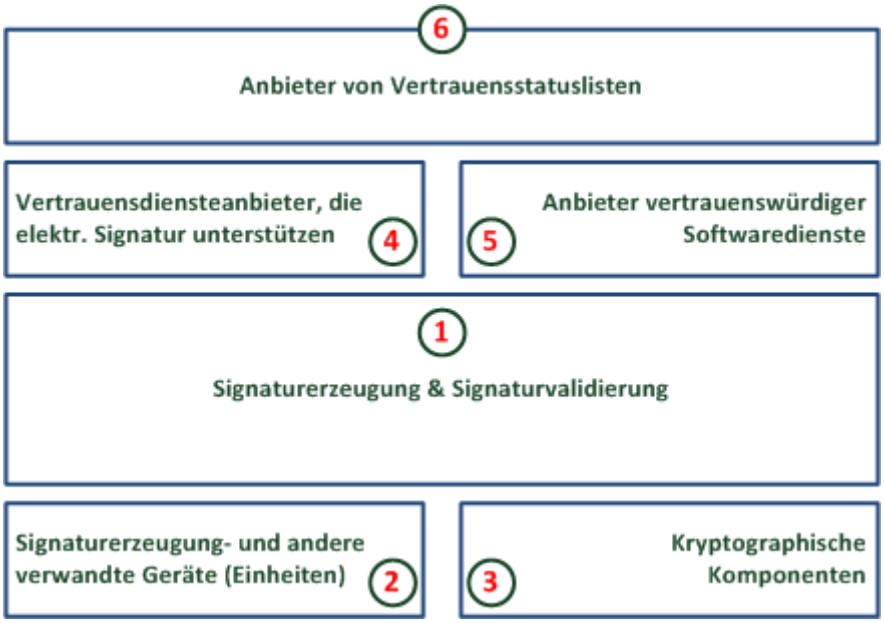


Abbildung 17: ETSI/CEN-Framework zur Bewältigung der Aufgaben aus dem M460-Mandat (Quelle: ETSI-M460)

Gemäß der Struktur der eIDAS-Verordnung sind die Themen in die folgenden sieben Bereiche unterteilt, für die jeweils durch ETSI/CEN definierte Normen vorbereitet und gegebenenfalls im Rahmen der Durchführungsrechtsakte publiziert werden: Identifizierungssysteme, Website-Zertifikate, elektronische Signaturen, elektronische Siegel, elektronische Zeitstempel, elektronische Zustelldienste und elektronische Bewahrungsdienste. Im Weiteren werden die einzelnen Bereiche kurz umrissen und eine Übersicht über den gegenwärtigen Stand der entsprechenden europäischen Standardisierungsarbeiten skizziert.

3.2.2 (Notifizierte) Identifizierungssysteme für Personen und Unternehmen

Anders als im Falle der elektronischen Signaturen mit Schwerpunkt auf Harmonisierung gelegt wurde, versucht die eIDAS-Verordnung im Bereich Identifizierungssysteme eine möglichst weitgehende Interoperabilität herzustellen. Für diese Zwecke wird im Rahmen des noch ausstehenden Durchführungsaktes ein Interoperabilitätsframework vorgegeben, das im Wesentlichen folgende Punkte ansprechen soll:

- Definition der Aspekte der grenzüberschreitenden Datenübertragung (nationale Kommunikation wird ausgeklammert) – hier basiert die Lösung insbesondere auf die Ergebnisse des Projektes STORK und dem darin erarbeiteten Ansatz (Proxy- bzw. Middleware-basiert)
- Festlegung eines minimalen Satzes an Daten, die unterstützt werden müssen, um eine natürliche beziehungsweise juristische Person eindeutig identifizieren zu können. Weil in vielen Fällen das eingesetzte Identifizierungsmittel gleichzeitig hoheitliche Aufgaben erfüllen soll (zum Beispiel der

Neue Personalausweis oder der elektronische Aufenthaltstitel), bietet sich ein Abgleich des Umfangs des Datensatzes mit den Vorgaben der ICAO (vgl. ICAO 9303) an

- Definition von einheitlichen Vertrauensniveaus – Ableitung eines dreistufigen Systems basierend auf ISO 29115 und Ergebnissen des Projekts STORK (vgl. [eIDAS], Kapitel II, Artikel 8)
- Bestimmung von Anforderungen an den sicheren Betrieb von eIDAS-Software – zum Beispiel durch Etablierung eines gemäß ISO 27001 aufgebauten Information Security Management Systems (ISMS) im Allgemeinen beziehungsweise gemäß BSI-Grundschutz im Speziellen

Die Ausrichtung auf die Interoperabilität hat zur Folge, dass die Identifizierungsmittel selbst keiner verstärkten Standardisierung unterworfen werden sollen. Lediglich deren Einsatz soll mit Hilfe des Interoperabilitätsframework EU-weit gesichert werden. In vielen EU-Mitgliedsstaaten sind nationale Identifizierungssysteme bereits betrieben oder ist der Betrieb in Planung. Gemäß der eIDAS-Verordnung besteht kein Zwang zur Notifizierung vorhandener Identifizierungssysteme, jedoch müssen notifizierte Systeme spätestens ab 18.09.2018 durch alle EU-Mitgliedsstaaten anerkannt werden.

Da es sich bei den Identifizierungsmitteln oft um SmartCard-basierte Systeme handelt, kann dabei auf die Vorgaben der CEN/TS 15480-Spezifikation zum Thema European Citizen Card sowie der ISO 19794 zum Thema Austausch von biometrischen Daten und der ISO 24727 zum Thema Ausgestaltung von Schnittstellen zurückgegriffen werden. Eine interessante Alternative in Richtung der Harmonisierung der Identifizierungssysteme bietet die gemeinsame deutsch-französische Spezifikation von BSI[7] und ANSSI[8] TR-03110[9] – „Advanced Security Mechanisms for Machine Readable Travel Documents and eIDAS Token“ dar (vgl. Abbildung 18).

[7] Bundesamt für Sicherheit in der Informationstechnik

[8] Agence nationale de la sécurité des systèmes d’information

[9] **https://www.bsi.bund.de/DE/Publikationen/TechnischeRichtlinien/tr03110/index_htm.html**

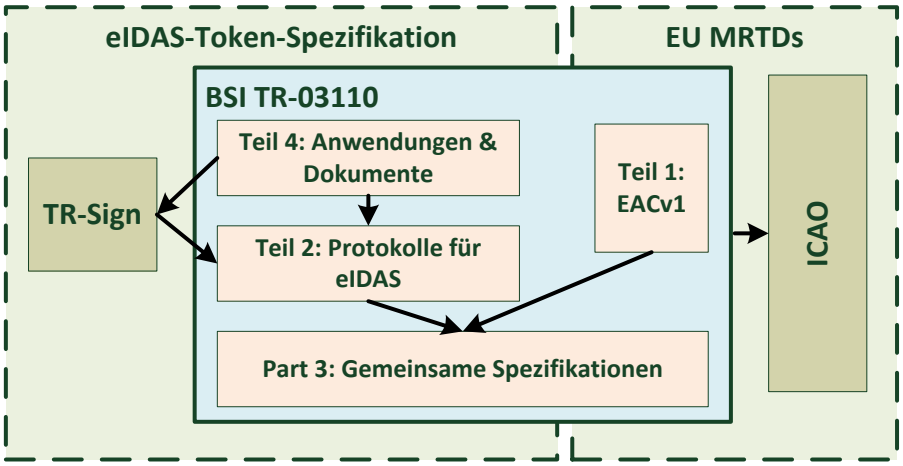


Abbildung 18: Überblick der eIDAS-Token-Spezifikation

Der deutsche Neue Personalausweis (sowie der elektronische Aufenthaltstitel) entsprechen bereits weitgehend den Vorgaben der eIDAS-Verordnung und könnten somit relativ zeitnah notifiziert werden.

3.2.3 (Qualifizierte) elektronische Signaturen

Elektronische Signaturen dienen sowohl dem Schutz der Integrität elektronischer Daten als auch, im Falle der qualifizierten elektronischen Signatur, der rechtskonformen elektronischen Unterschrift sowie der Erlangung wie Erhaltung des Beweiswerts[10].

Auf Basis der eIDAS-Verordnung wurden die zugelassenen Formate für elektronische Signaturen, die von Vertrauensdiensteanbietern erzeugt und validiert werden, normiert. Demnach sind für eIDAS-konforme elektronische Geschäftsprozesse künftig folgende Signaturformate zugelassen:

- **CAdES** – CMS-basierte elektronische Signaturen
- **XAdES** – XML-basierte elektronischer Signaturen
- **PAdES** – PDF-basierte elektronischer Signaturen
- **ASiC** – ZIP-basierter Signaturcontainer

Bei ASiC ist zu beachten, dass die zugrundeliegende ZIP-Spezifikation aktuell in ISO 21320-1 genormt wird, und neben dem reinen Signaturformat auch als standardisierter Datencontainer zur beweiswerterhaltenden Langzeitspeicherung sowie zum Datenaustausch verwendet werden kann.

[10] Bei der Beweiswerterhaltung im Verbund mit einem qualifizierten Zeitstempel vgl. DIN 31647

Die in Deutschland häufig verwendete PKCS#7-Signatur ist als Signaturformat somit nicht mehr zulässig. Um den Aufwand zu begrenzen, wären die aktuellen CMS-Signaturen einzusetzen. Alternativ kommen XML-/PDF-Signaturen oder ASiC-Signaturcontainer in Frage.

Neben den Signaturformaten werden die fachlich-technischen Sicherheitsanforderungen an TrustCenter (Certification Authorities) sowie die Signaturerstellungseinheiten (SEE) normiert. Hinsichtlich Signaturerstellungseinheiten erfolgt dies in Form von Protection Profiles nach Common Criteria.

Qualifizierte Vertrauensdiensteanbieter für elektronische Signaturen müssen nicht nur nach den Normen für Signaturformate und TrustCenter zertifiziert werden, sondern müssen mit ihren Signaturerstellungseinheiten auch konform zu den Protection Profiles sein. Andernfalls erfolgt keine Anerkennung als qualifizierter Vertrauensdienst. Damit sind sowohl IT-Sicherheit als auch Interoperabilität elektronischer Signaturen als Basis vertrauenswürdiger elektronischer Geschäftsprozesse in Europa gewährleistet.

Das Verfahren zu Zertifizierung der Signatur-/Siegelerstellungseinheiten (zum Beispiel Hardware Security Modules) gestaltet sich folgendermaßen:

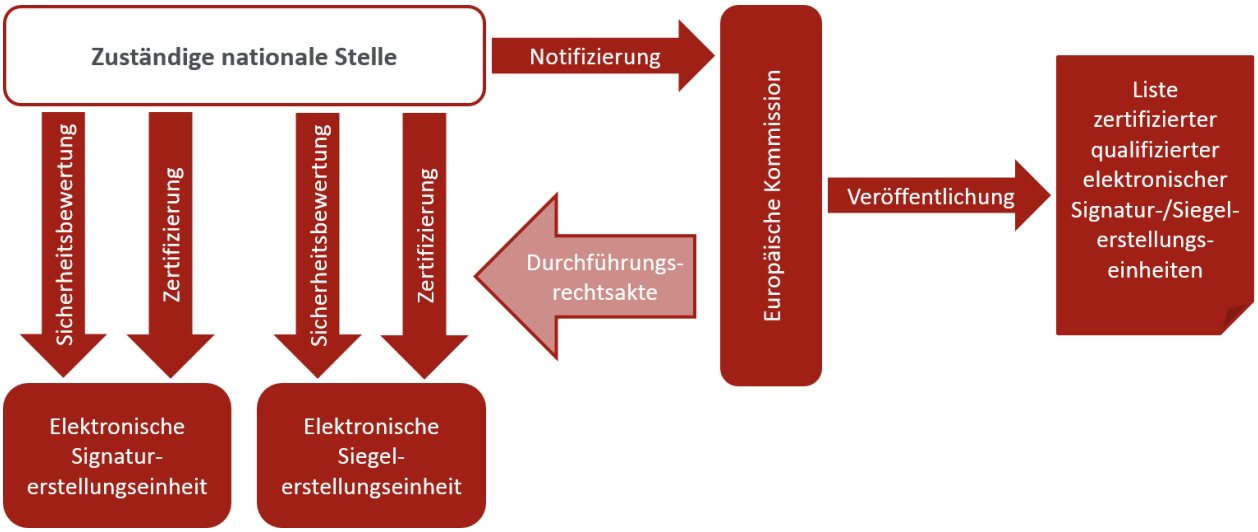


Abbildung 19: Zertifizierung Signatur-/Siegelerstellungseinheiten

Zuständige nationale Stellen sind in Deutschland voraussichtlich die BNetzA und/oder das BSI.

3.2.4 (Qualifizierte) elektronische Siegel

Elektronische Siegel sind elektronische Signaturen basierend auf einem Organisationszertifikat. Dadurch gelten die gleichen technischen Vorgaben. Mit qualifiziertem elektronischem Siegel können flächendeckend elektronische Unterschriften durch eine Institution geleistet werden, ohne dass Zertifikate für jeden Mitarbeiter auszustellen sind. Der Aufwand für rechtsverbindliche elektronische Prozesse und Dokumente wird somit erheblich verringert und als wesentlicher Kritikpunkt an der qualifizierten elektronischen Signatur in Deutschland pragmatisch gelöst.

3.2.5 (Qualifizierte) elektronische Zeitstempel

Neben qualifizierten elektronischen Signaturen und qualifizierten elektronischen Siegeln ist der qualifizierte elektronische Zeitstempel eine dritte Möglichkeit, um die Integrität der Daten zu schützen. Weiterhin wird mit Hilfe eines qualifizierten Zeitstempels die Existenz der Daten in dieser Form zu einem bestimmten Zeitpunkt bescheinigt. Eine große Rolle spielt der qualifizierte Zeitstempel (mit qualifizierter Signatur) insbesondere im Bereich der beweiswerterhaltenden Langzeitspeicherung (Bewahrungsdienste für die qualifizierte elektronische Signatur) und des ersetzenden Scannens. Zum Thema qualifizierte Zeitstempel sind vorrangig drei europäische Normen zu nennen:

Art	Rubrik	Bezeichnung
Norm	Anforderungen an Vertrauensdiensteanbieter, wenn diese einen (qualifizierten) Zeitstempeldienst anbieten	EN 319 421
	Formate und Prozeduren verbunden mit der Anfrage, Erstellung und Auslieferung von Zeitstempeln	EN 319 422
	Anforderungen an die Richtlinien für die Überwachung und Evaluierung von (qualifizierten) Vertrauensdiensteanbietern, die einen (qualifizierten) Zeitstempeldienst anbieten	EN 319 423

Weiterhin spielt der qualifizierte Zeitstempel eine Rolle in der Ausgestaltung bestimmter Profiles der einzelnen qualifizierten elektronischen Signaturen:

- CAdES-B-T und CAdES-B-LTA – ETSI EN 319 122-1 „CAdES digital signatures; Part 1: Building blocks and CAdES baseline signatures“,
- XAdES-B-T und XAdES-B-LTA – ETSI EN 319 132-1 „XAdES digital signatures; Part 1: Building blocks and XAdES baseline signatures“,

- PAdES-B-T und PAdES-B-LTA – ETSI EN 319 142-1 „PAdES digital signatures; Part 1: Building blocks and PAdES baseline signatures“.

In allen drei genannten Fällen wird mithilfe qualifizierter elektronischer Zeitstempel die vorhandene elektronische Signatur abgesichert. Im Falle von B-T-Profilen wird die Existenz einer Signatur zu einem bestimmten Zeitpunkt bestätigt. Bei B-LTA-Profilen wird ein Mechanismus definiert, wie die Beweiskraft der zugrundeliegenden elektronischen Signatur über eine längere Zeitperiode erhalten bleibt.

In Deutschland sind aktuell für die Anwendung qualifizierter elektronischer Zeitstempel neben der Verwendung als Eingangsnachweis in der elektronischen Kommunikation die beweiswerterhaltende Langzeitspeicherung gemäß Technischer Richtlinie des BSI TR-03125 (TR-ESOR) sowie das ersetzende Scannen gemäß Technischer Richtlinie des BSI TR-03138 (TR-RESISCAN) relevant.

3.2.6 (Qualifizierte) elektronische Einschreib- und Zustelldienste

Elektronische Einschreib- und Zustelldienste werden gemeinsam mit qualifizierten Bewahrungsdiensten in der eIDAS-Verordnung und gemäß ETSI als Produkte sogenannter Vertrauenswürdiger Softwaredienstanbieter (Trusted Application Service Provider) betrachtet. Die wesentlichen Anforderungen an Funktion und Sicherheit werden in einem eigenen Framework von ETSI (ETSI SR 019 050) von Juni 2015 definiert. Dabei wird zwischen registrierten Mailservices (Registered Mail Services) und Zustelldiensten (Delivery Services) unterschieden. Ein solcher Dienst soll grundsätzlich folgende Eigenschaften beinhalten:

- Sichere Authentisierung oder Identifikation von Sender und Empfänger
- Verschlüsselte Kommunikation einschließlich der Option einer Ende-zu-Ende-Verschlüsselung
- Eindeutiger Nachweis von Absendung, Zustellung und Empfang einer Nachricht
- Sicherung der Integrität der Nachricht
- Gewährleistung der Authentizität des Absenders
- Erzeugung und Prüfung elektronischer Signaturen
- Erzeugung und Prüfung von Zeitstempeln
- Beweiswerterhaltung
- Austausch und Prüfung von Beweisdaten
- Antivirus- und Antispamprüfung
- Wahrung der Vertraulichkeit und Verfügbarkeit
- Nutzung vertrauenswürdiger Kommunikationsverbindungen
- Adressmanagement
- Übertragung strukturierter und unstrukturierter Inhalte
- Definierte Verfahrensweisen bei Betriebsaufgabe

- Definierte Governance für den Betrieb
- Angebot verschiedener Service Level (optional)
- Übersetzungsservice (optional)
- Semantische Prüfungen (optional)

Das Framework wird aktuell in verschiedenen europäischen Normen und Spezifikationen zur Prüfung der Normenkonformität sowie Gewährleistung der Interoperabilität der Dienste im Detail definiert.

Art	Rubrik	Bezeichnung
Norm	Funktionale Vorgaben und Sicherheitsanforderungen an Einschreib- und Zustelldienste	EN 319 521 (Zustelldienste) EN 319 531 (Einschreibdienste)
	Technische Vorgaben an Einschreib- und Zustelldienste	EN 319 522 (Zustelldienste) EN 319 532 (Einschreibdienste)
Spezifikation	Grundsätzliche Anforderungen an Vertrauenswürdige Softwarediensteanbieter	TS 119 504
	Konformitäts- und Interoperabilitätsspezifikationen	TS 119 524 (Zustelldienste) TS 119 534 (Einschreibdienste)

Aktuell erfüllt in Deutschland De-Mail nominell bereits zahlreiche Anforderungen. Insofern bleibt derzeit abzuwarten, welche Detailtiefe die zu entwickelnden europäischen Normen aufweisen werden. Danach ist zu prüfen, inwieweit sich ein Anpassungsbedarf bei De-Mail ergibt.

3.2.7 (Qualifizierte) elektronische Bewahrungsdienste für (qualifizierte) elektronische Signaturen

Äquivalent zu § 17 Signaturverordnung fordert auch die eIDAS-Verordnung Maßnahmen zur Signaturerneuerung, sobald die Sicherheitseignung der zugrundeliegenden Algorithmen abgelaufen ist. Hintergrund ist das Risiko der Nachrechnung von Hash- und Signaturalgorithmen und somit der Fälschung eines elektronischen Dokuments. Das Dokument könnte ohne Maßnahmen zur Beweiswerterhaltung faktisch geändert und erneut mit der vorhandenen Signatur versehen werden, deren Algorithmen einfach nachgerechnet und für das geänderte Dokument erneut erzeugt wurden – eine (fast) perfekte Manipulation.

Qualifizierte elektronische Bewahrungsdienste bieten Vertrauensdiensteanbietern die Möglichkeit ihre Services – die erfolgreiche Qualifizierung vorausgesetzt – EU-weit anzubieten. Betreiben Behörden bereits eine Langzeitspeicherlösung für den eigenen Bedarf, muss diese nicht zwingend eIDAS-konform geführt werden, da sie sich auf einen geschlossenen Benutzerkreis bezieht. Dennoch ist auch für Behörden eine Qualifizierung durchaus sinnvoll, um einen höchstmöglichen Beweiswert der Daten zu erhalten und eventuell selbst als Diensteanbieter zu agieren.

Die Signaturerneuerung erfolgt gemäß ETSI durch die Anbringung eines spezifischen qualifizierten Archivzeitstempels[11], der eine qualifizierte elektronische Signatur beinhaltet. Im Gegensatz zum Hashbaumverfahren, wie es unter anderem in Deutschland Anwendung findet, wird der Archivzeitstempel derzeit überwiegend im 1:1-Verhältnis an einer Einzelsignatur angebracht. Mit dem Signaturcontainer ASiC wurde jedoch bereits eine Möglichkeit zur Nutzung von Hashbäumen zur Signaturerneuerung geschaffen. In diesem Fall wird das Beweisdokument, der reduzierte Hashbaum, im Signaturcontainer abgelegt.

Um auch für alle anderen Signaturformate gemäß ETSI eine wirtschaftliche Beweiswerterhaltung unter Verwendung von Merkle-Hashbäumen zu ermöglichen, wurde in der TR-ESOR v.1.1 ein eIDAS-konformes Austauschformat für Beweisdokumente geschaffen. Dabei wird der von ETSI geforderte Zeitstempel ATSv3 an die Signatur des Archivzeitstempels angebracht, der den Merkle-Hashbaum absichert. Durch das Repräsentationsprinzip, wonach dieser Archivzeitstempel alle Hashwerte und somit die darunterliegenden Daten repräsentiert, sind folglich alle gehashten Daten eIDAS-konform signiert. Die folgende Grafik verdeutlicht das Vorgehen:

[11] Sog. ATSv3, nicht mit dem Archivzeitstempel für Merkle-Hashbäume zu verwechseln.

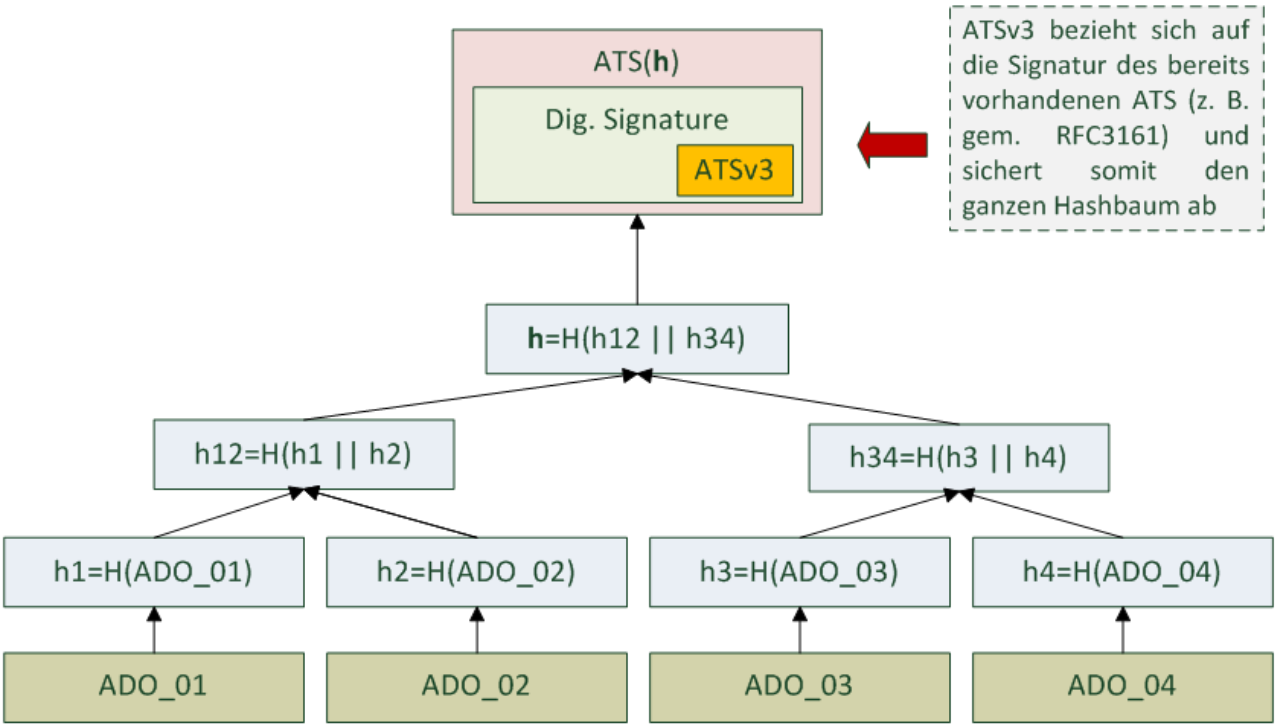


Abbildung 20: Interoperabilität zwischen TR-ESOR und eIDAS

In Deutschland lässt sich mittels der Technischen Richtlinie des BSI TR-ESOR sehr einfach eine beweiswerterhaltende Langzeitspeicherung gemäß europäischer Vorgaben umsetzen. Mit TR-ESOR und der eIDAS-Verordnung lassen sich die Vorteile einer europaweit einheitlichen Erzeugung und Prüfung sowie des standardisierten Austauschs signierter Unterlagen mit einer effizienten und wirtschaftlichen Beweiswerterhaltung – durch Hashbäume – verbinden. Dies wird bei einigen Behörden und Unternehmen aktuell bereits praktiziert.

3.2.8 (Qualifizierte) Website-Zertifikate

Die Verbreitung vertrauenswürdiger Website-Zertifikate und die damit verbundene voranschreitende Umstellung der Webkommunikation auf sichere Protokolle (z. B. https, insbesondere mit Hilfe von TLS und SSL) spielt angesichts der stetig wachsenden Anzahl von Cyberangriffen eine zunehmend stärkere Rolle.

Die eIDAS-Verordnung definiert im Anhang IV eine Reihe von Anforderungen an qualifizierte Zertifikate für die Website-Authentifizierung (kurz: Website-Zertifikate), die wesentliche verpflichtende Inhalte eines Website-Zertifikats vorschreiben (vgl. [eIDAS], Kapitel III, Abschnitt 8, Artikel 45 Absatz 1). Weiterhin behält sich der Gesetzgeber vor, mit Hilfe eines Durchführungsrechtsakts genauere technische Angaben bezüglich der Ausgestaltung der Website-Zertifikate vorzunehmen (vgl. [eIDAS], Kapitel III, Abschnitt 8, Artikel

45, Absatz 2). Das Grundgerüst für diese Vorgabe kann insbesondere die europäische Norm EN 319 411-1 liefern, die wesentliche Anforderungen an einen Zertifikatsanbieter (CA) ausformuliert, der die qualifizierten Website-Zertifikate ausgibt. Anhang IV der eIDAS-Verordnung gibt den logischen Aufbau eines Website-Zertifikats grob vor. Eine detaillierte technische Spezifikation für den Aufbau eines qualifizierten Website-Zertifikats – ausgegeben für eine Organisation – kann der europäischen Norm EN 319 412-4 entnommen werden. Diese Eingaben werden durch die Definition der allgemeinen Datenstrukturen für ein Zertifikat – EN 318 412-2 sowie die Vorschriften zur Erbringung des Nachweises über die Qualifikation des Zertifikates (qualified certificate statement – QCStatement) – EN 319 412-5 - ergänzt. Außer qualifizierten Website-Zertifikaten für Organisationen sieht die eIDAS-Verordnung auch die Möglichkeit vor, qualifizierte Website-Zertifikate für natürliche Personen auszustellen. In diesem Fall würde anstatt der Norm EN 319 412-3 die verwandte Norm EN 319 412-2 herangezogen, die ein Profil für qualifizierte Zertifikate für natürliche Personen definiert.

Abbildung 21: Überblick über die relevanten Normen zum Thema Website-Zertifikate

Die genaue Ausgestaltung der Vorgaben wird voraussichtlich im Rahmen eines korrespondierenden Durchführungsrechtsakts publiziert.

3.3 Status quo und mögliche Anpassungsbedarfe in Deutschland

Kurz und bündig:

Die europaweite Interoperabilität nationaler Signaturen führte nicht zum Erfolg. Die eIDAS-Verordnung harmonisiert die Signaturen zu einheitlichen Standards, EU-weiter Akzeptanz und Rechtsverbindlichkeit.

BSI TR-ESOR 1.2, DIN 31644 und DIN 31647 werden für eIDAS-Bewahrungsdienste empfohlen.

Die eIDAS-Verordnung vereinfacht das ersetzende Scannen nach BSI TR-RESISCAN durch reduzierten Aufwand bei der Signaturerstellung.

3.3.1 (Qualifizierte) elektronische Signaturen, Siegel, Zeitstempel und Validierungsdienste

Ziel der EU-Richtlinie 1999/93/EG war die Schaffung einer Basis für die Etablierung der qualifizierten elektronischen Signatur als Werkzeug zur Förderung des europäischen Binnenmarkts. Durch die fokussierte Interoperabilität und die unterschiedlichen Umsetzungen in den einzelnen Mitgliedsstaaten blieb die Verbreitung der qualifizierten elektronischen Signatur jedoch deutlich hinter den Erwartungen zurück. Der Ansatz der eIDAS-Verordnung will nun nicht mehr die Interoperabilität, sondern vielmehr die Harmonisierung der qualifizierten elektronischen Signatur vorantreiben. Als wichtigste Neuerungen gelten dabei folgende Punkte:

- Festlegung der Rechtsverbindlichkeit einer qualifizierten elektronischen Signatur in allen Mitgliedsstaaten und deren EU-weite gegenseitige Anerkennung
- Einführung von qualifizierten Organisationszertifikaten – sogenannten qualifizierten elektronischen Siegeln
- Reduzierung der Anforderungen an die qualifizierte elektronische Signatur – keine Anforderungen an Signaturanwendungskomponenten wie Lesegerät und Anzeige

Die neuen reduzierten Anforderungen an die qualifizierte elektronische Signatur tragen zwangsläufig dazu bei, dass bereits etablierte nationale technische Standards und Normen gegebenenfalls überarbeitet wer-

den müssen, um dem neuen Status quo zu entsprechen. Der Einsatz der qualifizierten elektronischen Signatur wurde in Deutschland insbesondere in zwei Bereichen durch das Signaturgesetz sowie die zugehörigen technischen Richtlinien des BSI geregelt:

- die elektronische Signatur mit einer eGK bzw. einem elektronischen Heilberufsausweis (HBA) im Gesundheitswesen,
- die qualifizierte elektronische Signatur mithilfe des Neuen Personalausweises und des elektronischen Aufenthaltstitels

Unter anderem müssen folgende technischen Standards und Normen aus dem Umfeld der (qualifizierten) elektronischen Signatur gegen die Anforderungen der neuen eIDAS-Verordnung geprüft und angepasst werden, da diese nur auf das SigG bzw. die SigV referenzieren:

- Common PKI[12] – ist ein Profil über international anerkannte Standards für elektronische Signaturen
- BSI TR-03114: „Stapelsignatur mit dem Heilberufsausweis“[13] – Realisierung einer qualifizierten elektronischen Stapelsignatur durch die Verwendung eines Heilberufsausweises in der Telematik-Umgebung eines Leistungserbringers
- BSI TR-03115: „Komfortsignatur mit dem Heilberufsausweis“[14] – Durchführung mehrfacher Signiervorgänge ermöglicht durch einmalige Authentifizierung des Karteninhabers in der Telematik-Umgebung eines Leistungserbringers
- BSI TR-03117: „eCards mit kontaktloser Schnittstelle als sichere Signaturerstellungseinheit“[15] – Signaturerstellungseinheit für die Erstellung qualifizierter elektronischer Signaturen auf Basis des Neuen Personalausweises und des elektronischen Aufenthaltstitels
- BSI TR-03119: “Requirements for Smart Card Readers Supporting eID and eSign Based on Extended Access Control”[16] – Anforderungen an Kartenleser für die Erstellung qualifizierter elektronischer Signaturen auf Basis des Neuen Personalausweises und des elektronischen Aufenthaltstitels
- SAGA[17] - eine Zusammenstellung von Referenzen auf Spezifikationen und Methoden für Software-Systeme der öffentlichen Verwaltung

[12] http://www.common-pki.org/uploads/media/Common-PKI_v2.0.pdf

[13] https://www.bsi.bund.de/DE/Publikationen/TechnischeRichtlinien/tr03114/index_htm.html

[14] https://www.bsi.bund.de/DE/Publikationen/TechnischeRichtlinien/tr03115/index_htm.html

[15] https://www.bsi.bund.de/DE/Publikationen/TechnischeRichtlinien/tr03117/index_htm.html

[16] https://www.bsi.bund.de/DE/Publikationen/TechnischeRichtlinien/tr03119/index_htm.html

[17] http://www.cio.bund.de/Web/DE/Architekturen-und-Standards/SAGA/saga_node.html

- ausgewählte Bausteine aus dem Organisationskonzept 'elektronische Verwaltungsarbeit, zum Beispiel „E-Poststelle“, die mit der qualifizierten elektronischen Signatur in Berührung kommen.[18]

3.3.2 (Qualifizierte) Elektronische Bewahrungsdienste

Hinsichtlich der beweiswerterhaltenden Langzeitspeicherung sind fachlich keine Anpassungen erforderlich, da mit den vorhandenen Standards und Normen die Vorgaben der eIDAS-Verordnung effizient umgesetzt werden können. Grundsätzlich sind für die Langzeitspeicherung die Erhaltung der Daten selbst und deren Beweiswerte zu beachten. Die wesentlichen Standards sind[19]:

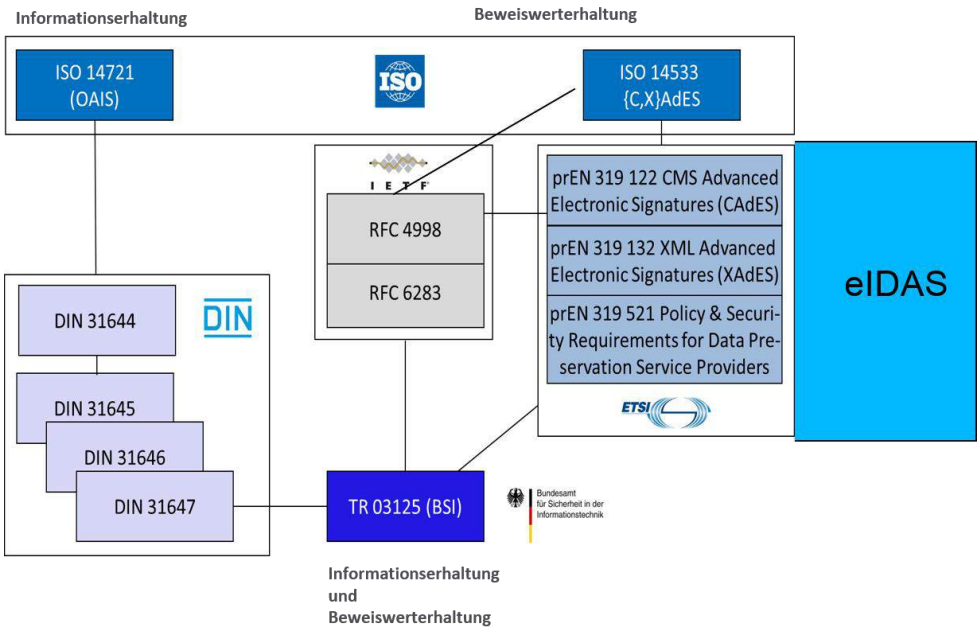


Abbildung 22: Relevante Standards der beweiswerterhaltenden Langzeitspeicherung

Die wesentlichen Normen und Standards sind im Folgenden näher beschrieben:

Norm/Standard	Inhalt und Bedeutung
ISO-14721: Open Archival Information System	• Weltweite Norm zur Langzeitspeicherung und Archivierung elektronischer Unterlagen • Branchenübergreifende Anwendung

[18] http://www.verwaltung-innovativ.de/DE/E_Government/orgkonzept_everwaltung/orgkonzept_everwaltung_artikel.html

[19] Die europäischen Normen zur Signatur sind zu Übersichtlichkeit nur ausgewählt dargestellt.

Norm/Standard	Inhalt und Bedeutung
	• Definiert die notwendigen Prozesse/Funktionen und Informationspakete zur sicheren Aufbewahrung digitaler Daten • Grundlage zahlreicher Umsetzungen in verschiedenen Industrien • Beinhaltet Daten- und Beweiswerterhaltung
DIN 31644: Kriterien für vertrauenswürdige digitale Langzeitarchive	• Definiert Anforderungen an vertrauenswürdige digitale Archivierung auf Basis von OAIS • Ergänzt faktisch die Maßgabe der eIDAS-Verordnung um Fachanforderungen an Prozesse und Datenpakete
DIN 31647:2015: Beweiswerterhaltung kryptographisch signierter Dokumente	• Definiert die notwendigen Funktionen zur Beweiswerterhaltung in einem OAIS-konformen digitalen Archiv auf Basis nationaler und internationaler Normen und Standards • Fachlicher Rahmen zur Beweiswerterhaltung gemäß eIDAS-Verordnung • Ermöglicht effiziente Beweiswerterhaltung durch Hashbäume • Bedeutung wird mit der eIDAS-Verordnung eher zunehmen
BSI-TR-ESOR, Version 1.2	• Standard zur Daten- und Beweiswerterhaltung auf Basis internationaler Normen • Referenziert auf verschiedene Gesetze (unter anderem auf das E-Government-Gesetz) • Definiert Referenzarchitektur, Prozesse, Funktionen, Austauschformate und Konformitätsregeln für Marktlösungen • Ermöglicht effiziente Beweiswerterhaltung durch Hashbäume

Norm/Standard	Inhalt und Bedeutung
	• Ermöglicht mit Version 1.2 die Umsetzung der Beweiswerterhaltung gemäß eIDAS-Verordnung • Bedeutung wird mit der eIDAS-Verordnung eher zunehmen
ISO-14533 und ETSI-Normen	• Technische Vorgaben für elektronische Signaturen, Siegel und Zeitstempel • Technische Basis für die eIDAS-Verordnung • Bedeutung wird europaweit zunehmen

3.3.3 (Qualifizierte) Elektronische Einschreib- und Zustelldienste

Das deutsche Pendant zu den elektronischen Einschreib- und Zustelldiensten ist die De-Mail. Diese ist gesetzlich definiert und gilt als vertrauenswürdige und nachweisbare elektronische Kommunikation. Gemäß E-Government-Gesetz Bund ist hierfür durch Bundesbehörden sowie bundesrechtausführende Behörden ein Zugang anzubieten.

De-Mail erfüllt die Mehrheit der aktuell geplanten Anforderungen an elektronische Einschreib- und Zustelldienste bereits heute. Offen bleibt die Frage, welche konkreten Anforderungen in den ETSI-Normen in Bezug auf sichere Authentisierung und Identifikation, verschlüsselte Kommunikation oder auf vertrauenswürdige Kommunikationsverbindungen gestellt werden. So ist denkbar, dass die Sicherheitsanforderungen unter denen der De-Mail angesiedelt werden. Gleiches gilt für die übrigen Anforderungen an Einschreib- und Zustelldienste. Dies würde den Markt der vertrauenswürdigen elektronischen Kommunikation deutlich öffnen und dem Anwender die Auswahl entsprechender Lösungen spürbar erleichtern. Ebenso sind im Zuge der ETSI-Normung zur vertrauenswürdigen elektronischen Kommunikation und möglicher Ausführungsbestimmungen Anpassungen rechtlicher Regelungen denkbar, die derzeit exklusiv auf De-Mail fokussieren. Wesentliche derzeit absehbare Unterschiede zwischen De-Mail und elektronischen Einschreib- und Zustelldiensten gemäß eIDAS-Verordnung zeigt die nachstehende Grafik:

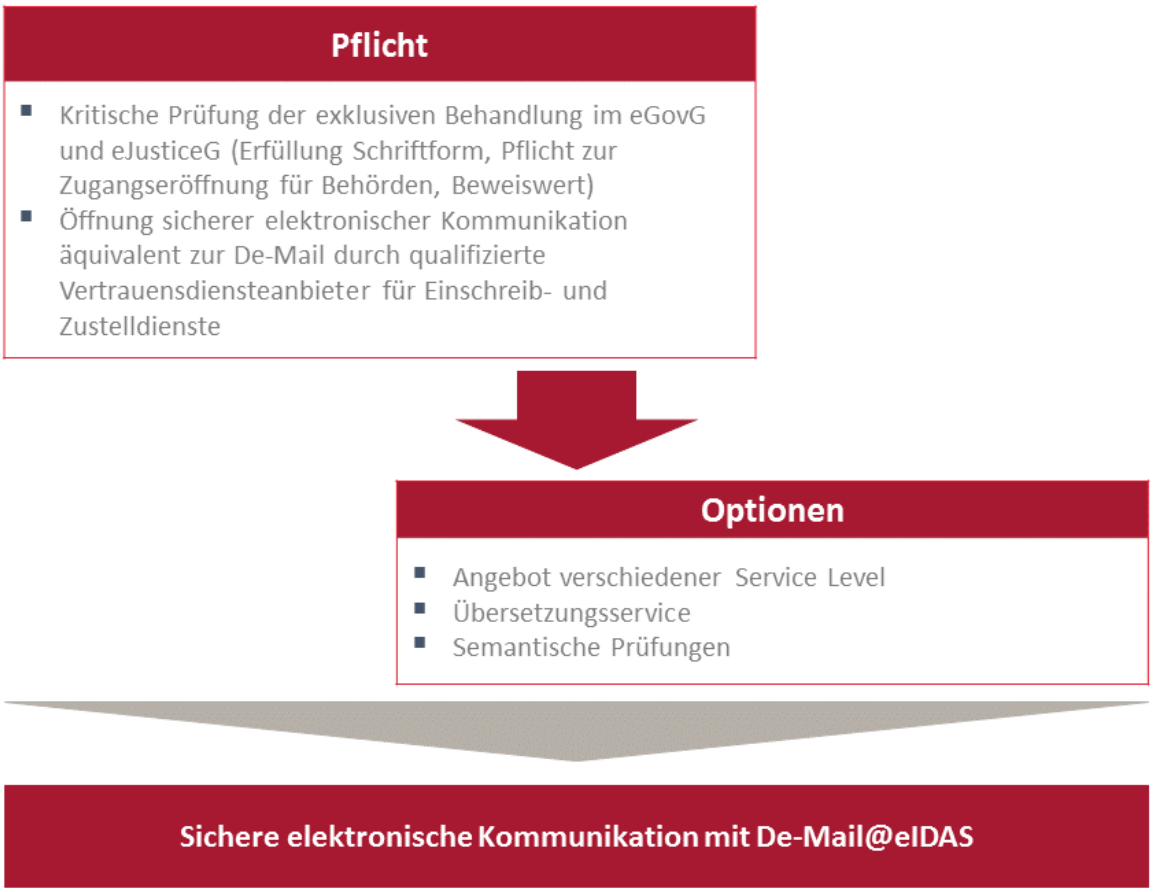


Abbildung 23: Mögliche Anpassungsbedarfe bei De-Mail

3.3.4 (Qualifizierte) Authentifizierungsdienste und Website-Authentifizierung

Im Bereich der Authentifizierungsdienste setzt die eIDAS-Verordnung auf die Herstellung weitgehender Interoperabilität zwischen den einzelnen notifizierten Authentifizierungsdiensten der 28 Mitgliedsstaaten. Dies soll den notwendigen Schub für die Akzeptanz und Weiterentwicklung solcher Dienste erzeugen. Die Grundlage der angestrebten Interoperabilität soll die von der EU-Kommission selbst entwickelte Interoperabilitätsplattform bilden, die, angereichert durch passende Übersetzungsmodule der einzelnen Identifizierungsdienste, das Herz des geplanten Systems bildet. Weiterhin wurden im Rahmen der eIDAS-Verordnung verbindliche und einheitliche Vertrauensniveaus definiert.

Bezogen auf die Website-Authentifizierung definiert die eIDAS-Verordnung durch den Gesetzestext und die begleitenden Normen, publiziert im Durchführungsakt, die Anforderungen an (qualifizierte) Website-Zertifikate. Betroffen wären hier die gängigen Ansätze für die sichere Webkommunikation, zum Beispiel https mit Hilfe von TLS/SSL. Die Anpassungen gemäß der Vorgaben des Interoperabilitätsframeworks sowie die

neuen Vertrauensniveaus und Regeln zur Ausgestaltung der Website-Zertifikate, spiegeln sich in der Prüfung und Anpassung folgender gegenwärtig existierender Richtlinien und Normen wider:

- BSI TR-03107: „Elektronische Identitäten und Vertrauensdienste im E-Government“[20]
  - Teil 1: “Vertrauensniveaus und Mechanismen” – Abstimmung der verwendeten Definition für die Vertrauensniveaus bezogen auf die Identifizierung einer Person bzw. eines Dienstes,
  - Teil 2: “Schriftformersatz mit elektronischem Identitätsnachweis“ – Vertrauensniveaus und Aspekte der Identifizierung (sowohl von Personen als auch von Webseiten) im Kontext möglicher Anwendung für Schriftformersatz,
- BSI TR-03109: „Technische Vorgaben für intelligente Messsysteme und deren sicherer Betrieb“[21]
- BSI TR-03110: “Advanced Security Mechanisms for Machine Readable Travel Documents and eIDAS token”[22]
- BSI TR-03124: “eID-Client”[23]
- BSI TR-03116: “Kryptographische Vorgaben für Projekte der Bundesregierung”[24]
  - Teil 4: “Kommunikationsverfahren in Anwendungen”
- BSI TR-03127: „Architektur Elektronischer Personalausweis“[25]
- BSI TR-03130: „eID-Server“[26]
- BSI TR-03139: “Common Certificate Policy for the Extended Access Control Infrastructure for Passports and Travel Documents issued by EU Member States”[27]

3.4 Relevanz der eIDAS-Verordnung und begleitender Normen im weltweiten Kontext

Die eIDAS-Verordnung regelt verbindlich sowohl vertrauenswürdige elektronische Geschäftsprozesse als auch deren Nachweisbarkeit durch Signaturen, Siegel und Zeitstempel in Europa und somit Anforderungen an Authentizität, Integrität, Verfügbarkeit und Verkehrsfähigkeit digitaler Unterlagen. Vergleichbare fachli-

[20] https://www.bsi.bund.de/DE/Publikationen/TechnischeRichtlinien/tr03107/index_htm.html
[21] https://www.bsi.bund.de/DE/Publikationen/TechnischeRichtlinien/tr03109/index_htm.html
[22] https://www.bsi.bund.de/DE/Publikationen/TechnischeRichtlinien/tr03110/index_htm.html
[23] https://www.bsi.bund.de/DE/Publikationen/TechnischeRichtlinien/tr03124/index_htm.html
[24] https://www.bsi.bund.de/DE/Publikationen/TechnischeRichtlinien/tr03116/index_htm.html
[25] https://www.bsi.bund.de/DE/Publikationen/TechnischeRichtlinien/tr03127/tr-03127.html
[26] https://www.bsi.bund.de/DE/Publikationen/TechnischeRichtlinien/tr03130/tr-03130.html
[27] https://www.bsi.bund.de/DE/Publikationen/TechnischeRichtlinien/tr03139/index_htm.html

che Anforderungen werden in verschiedenen internationalen Normen und Standards sowie Branchenstandards gestellt, ohne detaillierte Beschreibung, wie diese zu erfüllen sind. Diese Lücke schließt in Europa die eIDAS-Verordnung. Auf deren Basis können internationale Vorgaben europaweit auf einheitlicher Basis erfüllt werden, was die Nutzung für weltweit aktive Unternehmen und internationale Institutionen vereinfacht.
Die folgende Grafik zeigt beispielhaft wesentliche Standards und Normen, die mit der eIDAS-Verordnung leichter erfüllt werden können:

Norm/Standard	Anwendungsgebiet
Organisationskonzept 'elektronische Verwaltungsarbeit'	Public Sector
Prüfhandbuch des Bundesversicherungsamts für Sozialversicherungsamt, die sogenannte 'BVA-Richtlinie'	Health Care, Krankenkassen, Landesversicherungsanstalten
FDA	Kliniken, Health Care LifeScience/Pharma
ISO 30301	Records Management und Compliance elektronischer Unterlagen weltweit
ISO 15489	Records Management, Archivierung und Compliance elektronischer Unterlagen weltweit
ISO 14721	Langzeitarchivierung weltweit

Angesichts der Tatsache, dass die ETSI-Standards außerhalb Europas noch im arabischen Raum und in Asien eingesetzt werden, sind mit der eIDAS-Verordnung Synergieeffekte über Europa hinaus zu erwarten.

3.5 Zusammenfassung der fachlich-technischen Aspekte

Die eIDAS-Verordnung referenziert auf vorhandene und etablierte Standards und Normen – unter anderem auf DIN, ISO, ETSI und CEN – und bildet den regulatorischen Rahmen für die technischen Spezifikationen. Unter diesem Dach werden die fachlich-technischen europäischen Normen zur Umsetzung erarbeitet. Aus

fachlich-technischer Sicht sind die Anpassungsbedarfe in Deutschland als überschaubar einzuschätzen. Vielmehr geht es um eine Harmonisierung, zumal die relevanten europäischen Normen in der Regel bereits Anwendung finden und im eIDAS-Kontext nur fortgeschrieben werden. Insofern gewinnen die bestehenden Normen mit der eIDAS-Verordnung an Verbindlichkeit.

Die fachlich-technische Basis in einem verbindlichen rechtlichen Rahmen ist geschaffen. Es gilt sie umzusetzen, um europaweit einheitliche, interoperable und vertrauenswürdige elektronische Geschäftsprozesse zu realisieren und bestehende Vorgehen zu optimieren.

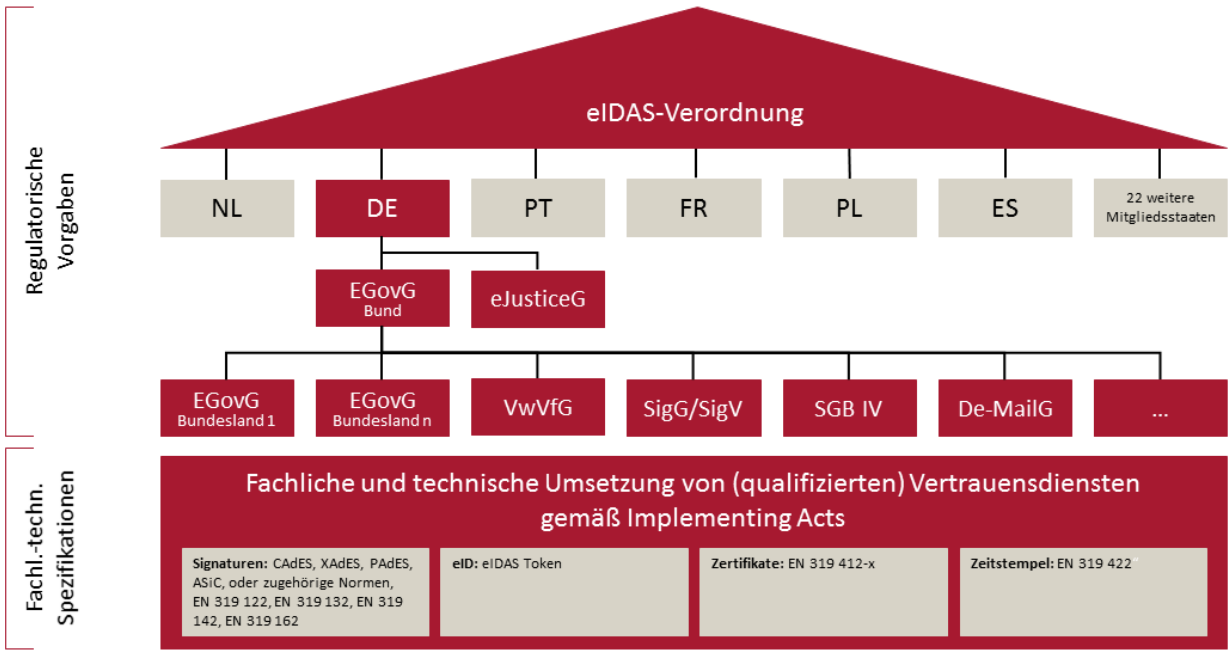


Abbildung 24: Rolle der eIDAS-Verordnung und fachlich-technische Umsetzung

4 Chancen & Herausforderungen

Das vierte Kapitel benennt Chancen und Herausforderungen, die sich aus den rechtlichen und fachlich-technischen Maßgaben der eIDAS-Verordnung ergeben – untergliedert in eID, die verschiedenen Signaturarten und Vertrauensdienste.
Aufbauend auf den hier genannten Chancen und Herausforderungen werden in Kapitel 6 konkrete Handlungsempfehlungen erläutert.

Kurz und bündig:

Die eIDAS-Verordnung regelt den Rechtsrahmen und definiert die Technik über Standardisierung und Interoperabilität; nicht jedoch Prozesse und organisatorische Aspekte.

Die Standardisierungsbestrebungen bieten große Chancen. Erstmals ist eine EU-weite durchgängige Vertrauenswürdigkeit in elektronischen Prozessen möglich: von der Authentifizierung und Erstellung von Datensätzen bis zur Bearbeitung und beweiswerterhaltenden Langzeitspeicherung.

Die eIDAS-Verordnung leistet einen großen Vorschub für eine EU-weit gültige gerichtsverwertbare Dokumentation in Unternehmen und Behörden.

Wir prüfen die Möglichkeiten, die sich aus der Umsetzung der eIDAS-Verordnung ergeben und nennen die wichtigsten Herausforderungen, die es zu berücksichtigen gilt. Aus Gründen der Übersichtlichkeit beschränken wir uns auf den Anwender aus der Privatwirtschaft und der öffentlichen Verwaltung. Für Anbieter qualifizierter Vertrauensdienste gelten die für Anwender getroffenen Aussagen vielfach ebenso - ergänzt um große wirtschaftliche Potenziale, die sich aufgrund neu zu schaffender Produkte, Dienstleistungen und Geschäftsmodelle erschließen.

4.1 Elektronische Identifizierung

Grundsätzlich wird im Bereich der elektronischen Identifizierung auf eine Strategie der Interoperabilität gesetzt, d.h. unterschiedliche nationale Ansätze sollen grenzüberschreitend kompatibel sein. Bisher wurde diese Vorgehensweise auch für elektronische Signaturen praktiziert, was allerdings dazu führte, dass sich die Technik der elektronischen Signatur nicht flächendeckend durchsetzen konnte. Vermutlich wird sich diese Entwicklung im Bereich der elektronischen Identifizierung wiederholen. Die unterschiedlichen Ansätze der einzelnen Mitgliedstaaten werden dazu führen, dass eine kontinuierliche Weiterentwicklung der

sogenannten Interoperabilitätsplattform notwendig wird. Diese Entwicklung verursacht Herausforderungen, bietet jedoch auch Chancen.

Herausforderungen	Chancen
• Integration von eID-Lösungskomponenten und -hardware in bestehende Infrastrukturen sowie deren Betrieb und Pflege • Anbindung an Fachanwendungen und Vertrauensdiensteanbieter • Klärung spezifischer organisatorischer, prozessualer und regulatorischer Aspekte, zum Beispiel beim Schriftformersatz und bei Zuständigkeiten im Streitfall	• Reduktion der Verwaltungskosten durch Vermeidung von Papier und Medienbrüchen • Risikominimierung durch EU-weit anerkannte vertrauenswürdige Identifizierung • Schnellere Prozessdurchlauf- und kürzere Antwortzeiten, zum Beispiel bei der Identifizierung über Webseiten • Wettbewerbsvorteile durch neue Produkte, Dienstleistungen und Geschäftsmodelle, die sich dem Anwender durch eID erschließen

4.2 (Qualifizierte) elektronische Signaturen, Siegel und Zeitstempel

Die Harmonisierung der Anwendung elektronischer Signaturen, elektronischer Siegel sowie elektronischer Zeitstempel, insbesondere im qualifizierten Bereich, sowie die Absenkung der Anforderungen an die Signaturerstellungsumgebung lassen darauf schließen, dass diese mittelfristig vermehrt im Geschäftsverkehr genutzt werden.

Herausforderungen	Chancen
• Integration von Signaturanwendungskomponenten und Signaturhardware in bestehende Infrastrukturen sowie deren Betrieb und Pflege • Anbindung an Fachanwendungen und Vertrauensdiensteanbieter	• Höhere Akzeptanz von elektronischen Signaturen durch vereinfachte Signaturprozesse (Verzicht auf Personenbezug und Zulassung von Serversignaturen) • Vereinfachtes *ersetzendes Scannen* nach BSI TR-RESISCAN durch Nutzung von elektronischen Siegeln und Serversignaturen

• Implementierung von Lösungen zur beweiswerterhaltenden Langzeitspeicherung • Klärung spezifischer organisatorischer, prozessualer und regulatorischer Aspekte	• Kostengünstige Prüfbarkeit aller europäischer Signaturen • Reduktion der Verwaltungskosten durch Vermeidung von Papier und Medienbrüchen • Schaffung durchgängiger Vertraulichkeit in elektronischen Prozessen und Dokumenten • Risikominimierung durch vermehrten rechtsverbindlichen Ersatz der Schriftform

4.3 (Qualifizierte) elektronische Zustelldienste

Die eIDAS-Verordnung betont die EU-weite Rechtssicherheit der qualifizierten elektronischen Zustelldienste und formuliert die Anforderungen an qualifizierte Anbieter solcher Dienste (vgl. Artikel 43, 44 eIDAS). Im Rahmen eines Durchführungsakts können weitere Details, insbesondere Verfahren und technische Formate, im Kontext der Verordnung spezifiziert werden. Die in Deutschland implementierte De-Mail wird als qualifizierter Zustelldienst bezeichnet und zeitnah als solcher notifiziert.

Herausforderungen	**Chancen**
• Integration von Message Brokern in bestehende Mail- und De-Mail-Infrastrukturen sowie deren Betrieb und Pflege • Anbindung an Fachanwendungen und Vertrauensdiensteanbieter • Implementierung von Lösungen zur beweiswerterhaltenden Langzeitspeicherung • Klärung spezifischer organisatorischer, prozessualer und regulatorischer Aspekte	• Reduktion der Verwaltungskosten durch Vermeidung von Papier und Medienbrüchen • Schaffung durchgängiger Vertraulichkeit in elektronischen Prozessen und Dokumenten • Wettbewerbsvorteile durch neue Produkte, Dienstleistungen und Geschäftsmodelle, die sich dem Anwender durch den Wegfall der analogen Post erschließen

4.4 (Qualifizierte) elektronische Bewahrungsdienste für (qualifizierte) elektronische Signaturen

Mit Inkrafttreten der eIDAS-Verordnung wurde gemäß Artikel 34 und 40 die Notwendigkeit der beweiswerterhaltenden Aufbewahrung der qualifizierten elektronischen Signaturen bzw. qualifizierten elektronischen Siegel bescheinigt. Die geplante Präzisierung der Vorgaben durch die Veröffentlichung des zugehörigen Durchführungsakts kann vorgenommen werden. Es besteht jedoch keine Verpflichtung dazu.

Herausforderungen	Chancen
• Implementierung von Lösungen zur beweiswerterhaltenden Langzeitspeicherung in bestehende Infrastrukturen sowie deren Betrieb und Pflege • Anbindung an Fachanwendungen und Vertrauensdiensteanbieter • Klärung spezifischer organisatorischer, prozessualer und regulatorischer Aspekte	• Risikominimierung durch höchste Beweiskraft elektronischer Dokumente • Hohe Kosteneinsparung durch Zentralisierung des standardisierten Langzeitarchivs und Wegfall der Hardwarebindung • Reduzierung von Archiv- und Lagerkosten • Schnellere Prozessdurchlauf- und kürzere Antwortzeiten • Dauerhafte Signaturerneuerung und Beweiswerterhaltung • EU-weite richterliche Akzeptanz

5 Fazit

Kurz und bündig:

Die erwartete EU-weite Interoperabilität von eID-Diensten, die Harmonisierung und Standardisierung von Signaturen und Verfahren sowie die Schaffung von qualifizierten Vertrauensdiensten bieten Chancen für eine schnelle Verbreitung und hohe Anwenderakzeptanz. Herausforderungen sind Aufbau und Pflege der erforderlichen IT-Infrastruktur und die Klärung offener rechtlicher Fragen.

Grundsätzlich überwiegt der Nutzen der Standardisierungs- und Interoperabilitätsbestrebungen die Herausforderungen: elektronische Identitäten, Dokumente und Kommunikationswege werden EU-weit nachprüfbar und vertrauenswürdig, Papierarchive werden reduziert und sparen Such- und Lagerkosten und elektronische Dokumente werden vor Gericht den papiergebundenen gleichgestellt. Diese Entwicklungen werden zu einer Zunahme von elektronischen Geschäftsprozessen in Deutschland und Europa führen.

Mit einem nominalen Bruttoinlandsprodukt von etwa 20 Billionen Dollar erwirtschaften die 28 EU-Mitgliedsstaaten sowie Island, Liechtenstein, Norwegen und die Schweiz rund ein Viertel des globalen BIP. Die eIDAS-Verordnung bildet den rechtlichen und organisatorischen Rahmen für den sicheren und vertrauenswürdigen elektronischen Geschäftsverkehr im somit größten Binnenmarkt der Welt.

Sie definiert technische Standards, die helfen, Kosten und Aufwände zu reduzieren, um die schnelle Verbreitung von elektronischen Prozessen und Diensten zu fördern. Sie regelt Interoperabilität, wo Standards zunächst nicht erreichbar sind, beispielsweise in der national sehr unterschiedlichen Umsetzung der elektronischen Identifizierung. Und sie bietet Verbrauchern, Unternehmen und der öffentlichen Verwaltung das nötige Vertrauen durch transparente Service Level, Notifizierungen und EU-weit einheitliche Kontrollverfahren. Kurzum: Noch nie war es so einfach und wirtschaftlich, elektronische Transaktionen rechtskonform und vertrauenswürdig abzusichern, Dokumente zu signieren oder Papierdokumente beweiswerterhaltend und ersetzend in eine e-Akte zu integrieren. Die eIDAS-Verordnung ist die Basis für ein starkes digitales Europa!

Die nächsten Jahre werden zeigen, wie schnell die 28 EU-Mitglieds- und 4 EFTA-Staaten auf die steigende Nachfrage nach neuen elektronischen Vertrauensdiensten aufgrund der raschen Digitalisierung reagieren können. So müssen Interoperabilitätsplattformen für die elektronische Identifizierung entwickelt, betrieben

und gepflegt sowie Infrastrukturen zur Signatur-, Zeitstempel- und Siegelerstellung sowie -prüfung erweitert und notifiziert werden. Neue elektronische Zustell- und Einschreibdienste müssen ebenso wie die neuen Bewahrungsdienste für die dauerhafte Beweiswerterhaltung und Integritätssicherung elektronischer Dokumente aufgebaut, betrieben und zu anderen nationalen Lösungen interoperabel gehalten werden.

So gesehen stehen den Vorteilen der Harmonisierung zunächst beträchtliche technisch-fachliche Herausforderungen gegenüber. Für die Bundesrepublik Deutschland dürfte der Aufwand zur Erreichung der IT-Compliance im Verhältnis zu anderen Mitgliedsstaaten überschaubar ausfallen, denn das Land ist bei vielen Standardisierungen und der Entwicklung von Technologien und Verfahren federführend.

Der Ausblick ist vielversprechend: eine halbe Milliarde Menschen werden auf Basis eines einheitlichen Rahmens elektronische Geschäftsprozesse und Dokumente vertrauenswürdig, beweiskräftig und rechtssicher nutzen können – ein entscheidender Wettbewerbs- und Standortfaktor in einem geeinten Europa.

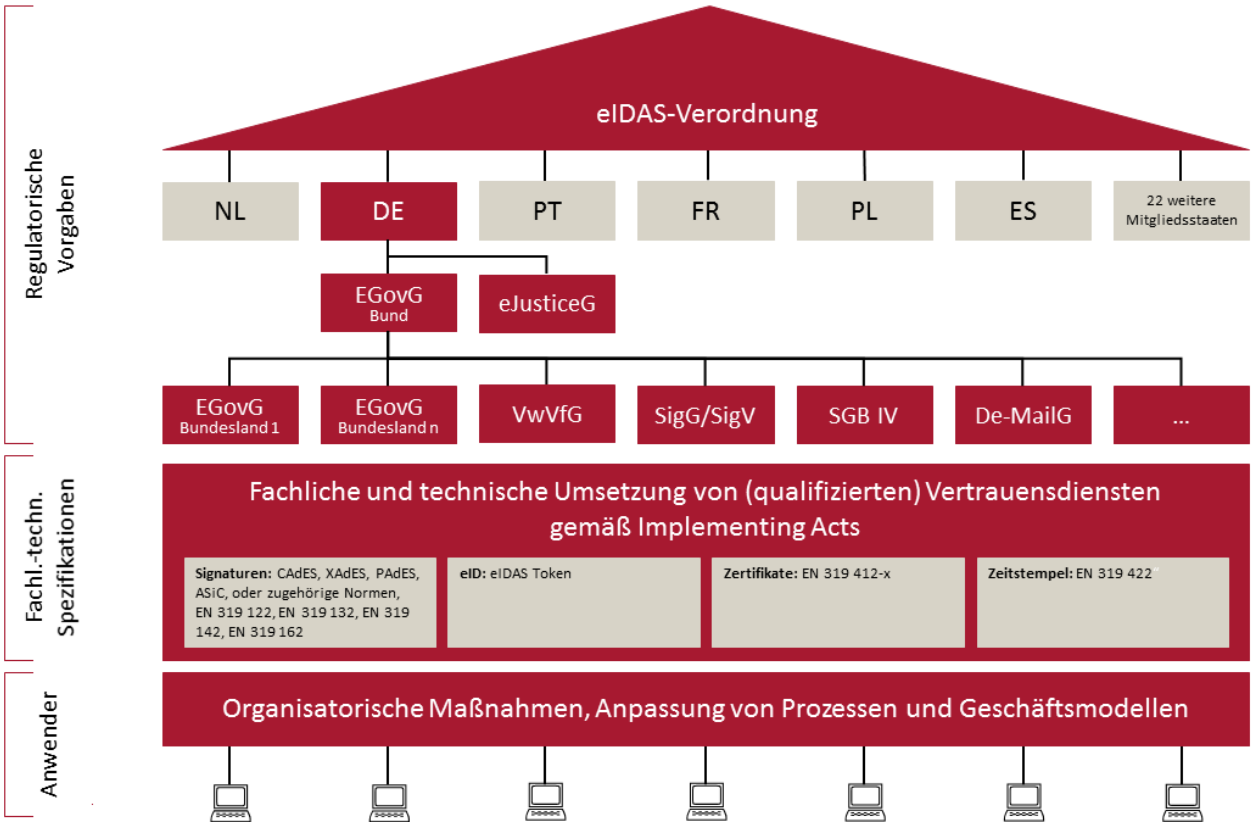


Abbildung 25: Rolle der eIDAS-Verordnung, fachlich-technische Umsetzung und Maßnahmen beim Anwender

6 Handlungsempfehlungen

Die Berater von BearingPoint sind seit vielen Jahren in der Prozess- und Organisationsberatung tätig. Aufgrund unserer umfangreichen Projekterfahrung in der Privatwirtschaft und der öffentlichen Verwaltung – von der Fachkonzeption bis zur technischen Umsetzung – möchten wir Ihnen einige Anregungen an die Hand geben.

Die folgenden Fragen sind hilfreich bei der Evaluierung:

1. Werden in meinem Unternehmen oder in meiner Behörde sichere elektronische Geschäftsprozesse umgesetzt?
   → Dann liefert die eIDAS-Verordnung große Vorteile durch eine EU-weite Standardisierung und Interoperabilität. Sie bietet außerdem eine vereinfachte Anwendung im Vergleich zu bisherigen deutschen regulatorischen Vorgaben.

2. Wollen Sie Kosteneinsparungen erzielen und Prozesse verschlanken, in dem Sie die eID-Funktionen in Ihren Portalen nutzen?
   → Dann wäre die Verwendung der qualifizierten Identifizierungsdienste von Vorteil.

3. Wollen Sie Wettbewerbsvorteile erzielen oder neue Angebote aufbauen durch Identifizierungsdienste und Vertrauensdienste?
   → Hier bieten sich zahlreiche Optionen, von der elektronischen Willenserklärung im Allgemeinen bis hin zur digitalen Police im Besonderen.

4. Gibt es zeitkritische Prozesse, bei denen die Papierbindung und Schriftformerfordernis aufgrund langer Transportwege hinderlich sind?
   → Dann könnte die Verwendung von eID und der qualifizierten Einschreib- und Zustelldiensten die Prozesse in Ihrer Organisation/Ihrem Unternehmen beschleunigen.

5. Ist eine hohe Vertrauenswürdigkeit bei der Identifizierung meiner Website erforderlich? Ist für Ihre Kunden die Nachvollziehbarkeit der Echtheit Ihrer Website wichtig?
   → Dann wären die neuen Website-Zertifikate die richtige Wahl.

6. Signieren Sie elektronische Dokumente derzeit aufwändig mit einer personenbezogenen qualifizierten elektronischen Signatur, z.B. zur Unterzeichnung oder beim ersetzenden Scannen?
   → Dann könnte Ihnen der Einsatz des qualifizierten elektronischen Siegels oder einer Serviersignatur Ihre Prozesse durch Wegfall des Personen- bzw. Kartenbezugs erheblich vereinfachen.

7. Wünschen SIe hohe Rechtssicherheit in der elektronischen Kommunikation und soll die elektronische Kommunikation die analoge ersetzen?
   → Dann kann die Nutzung qualifizierter Einschreib- und Zustelldienste vorteilhaft sein. Diese wären entgegen nationaler Lösungen EU-weit verfügbar.

8. Arbeiten Sie (nicht nur) elektronisch signierten Dokumenten und möchte ich deren Beweiswert dauerhaft und gerichtsverwertbar erhalten?
   → Dann empfehlen sich die neuen qualifizierten Bewahrungsdienste für die beweiswerterhaltende Langzeitaufbewahrung (nicht nur) elektronisch signierter Dokumente.

9. Verfügt Ihre Organisation oder Ihr Unternehmen über große physische Papierarchive, die beispielsweise über das ersetzende Scannen nach BSI TR-RESISCAN abgebaut werden sollen, um Miet- und Recherchekosten zu reduzieren?
   → Dann sind die neuen qualifizierten elektronischen Siegel ohne Personenbezug und die qualifizierten Bewahrungsdienste eine kostengünstige Option.

10. Suchen Sie nach neuen Geschäftsmodellen auf Basis der neuen eIDAS-Verordnung?
    → Dann kann Ihr Unternehmen als Service Provider die Identifizierungs- und Vertrauensdienste Dienste anbieten und Ihre Kunden an den Vorteilen beteiligen.

7 Wie kann BearingPoint Sie unterstützen?

7.1 Beratung mit Management- und Technologiekompetenz

BearingPoint ist eine unabhängige, partnergeführte Unternehmensberatung, die Management- und Technologiekompetenz vereint. Unsere Kunden sind namhafte, weltweit agierende Unternehmen, Finanzinstitutionen und Organisationen der öffentlichen Hand. Wir bieten Beratungsleistungen im Bereich Business Consulting: Für unsere Kunden erzielen wir einen messbaren Geschäftserfolg, indem wir Prozesse, IT und Organisationsmodelle optimieren. Mit unserem tiefgreifenden Branchen-Know-how und unserer fachlichen Kompetenz verstehen und berücksichtigen wir die individuellen Bedürfnisse unserer Kunden – und helfen ihnen so, ihre Ziele zu erreichen.
Unser Team setzt sich aus leidenschaftlichen, engagierten Beratern mit einer pragmatischen und zugleich innovativen Denkweise zusammen. Rund 140 Partner tragen die persönliche Verantwortung für unser Beratungsgeschäft. Wir betreuen ca. 1.100 Kunden und beschäftigen 3.350 Mitarbeiter an 32 Standorten in 20 Ländern. 2014 wurde ein Umsatz von 558 Millionen Euro erwirtschaftet. In Deutschland ist BearingPoint an acht Standorten vertreten. Im Geschäftsjahr 2013 erwirtschafteten rund 1.200 Mitarbeiter einen Umsatz von 238 Millionen Euro. In Deutschland belegt BearingPoint laut Lünendonk-Liste derzeit Platz 15 unter den Top 25 Managementberatungsunternehmen.

7.2 Standorte und Struktur

BearingPoint ist mit 32 Büros in 20 Ländern (Belgien, Dänemark, Deutschland, Finnland, Frankreich, Großbritannien, Irland, Italien, Marokko, Niederlande, Norwegen, Österreich, Rumänien, Russland, Shanghai, Schweden, Schweiz, Ukraine, USA, Vereinigte Arabische Emirate) vertreten.

*Abbildung 1: BearingPoint-Standorte – **Option 1***

7.3 Unser Service-Portfolio

Wir begleiten unsere Kunden von den ersten strategischen Überlegungen über eine dezidierte Fachkonzeption bis hin zur Produktbeschaffung und Einführung sicherer elektronischer Geschäftsprozesse auf Basis der eIDAS-Verordnung. Die nachstehende Grafik zeigt unser Serviceangebot im Überblick:

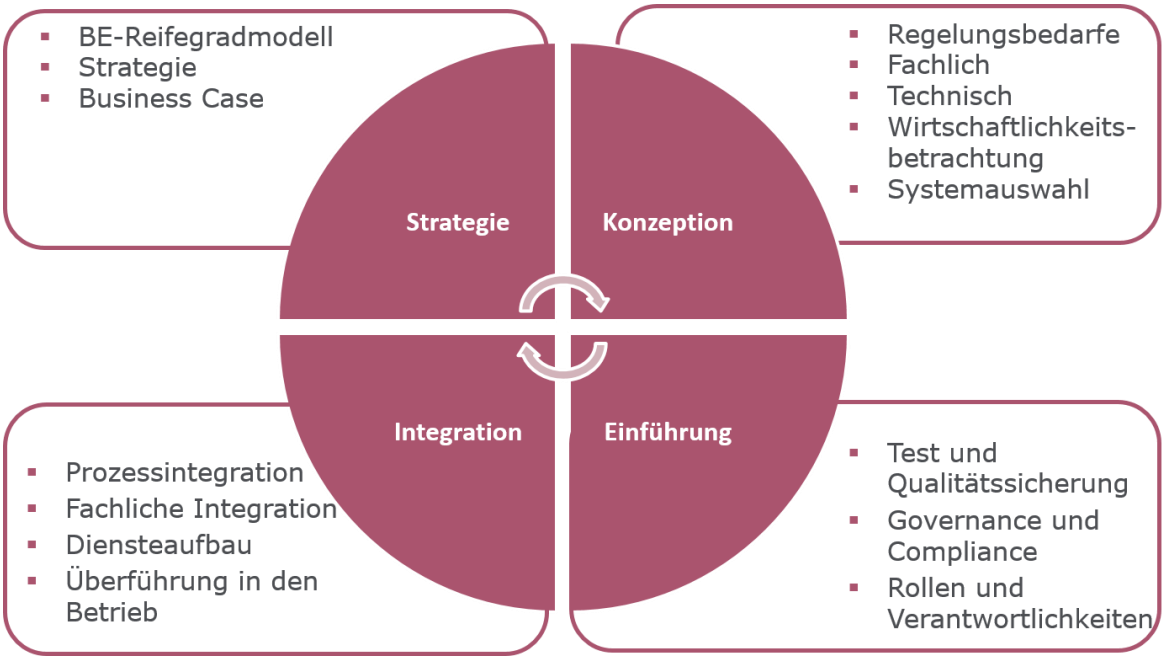


Abbildung 26: BearingPoint Serviceangebot eIDAS

Strategie

Zunächst gilt es Chancen und Herausforderungen der eIDAS zur Umsetzung oder Reorganisation sicherer elektronischer Geschäftsprozesse zu beurteilen. Hierzu gehören die Erhebung der relevanten Prozesse, Regularien, Verantwortlichkeiten und Unterlagen sowie deren Abgleich mit den Maßgaben der eIDAS selbst. Gleiches gilt für bestehende IT-Dienste und Dienstleistungen öffentlicher wie privater IT-Dienstleister Anhand des BearingPoint-Reifegradmodells erfolgt die standardisierte Einordnung der Erhebungsergebnisse in die für sichere elektronische Prozesse relevanten Dimensionen. Diese wurden unmittelbar an den Vorgaben der eIDAS sowie der hierauf basierenden Standards und Normen zur Compliance elektronischer Unterlagen entwickelt und ermöglichen so eine gezielte Identifikation bestehender Schwachstellen und Handlungsbedarfe. Das Ergebnis bildet ein dezidierter Maßnahmenkatalog sowie ein strategisches Zielbild zur Meisterung der Herausforderungen und Nutzung der Chancen von eIDAS. Diese Unterlagen bilden die Basis späterer Konzeptionen und Umsetzungsschritte.

Konzeption

Im Rahmen der Konzeption erarbeiten wir kundenspezifische Lösungen zur Umsetzung medienbruchfreier wie sicherer Geschäftsprozesse für Anwender und den Aufbau kundengerechter eIDAS-konformer Lösungen für IT-Dienstleister. Hierbei konzentrieren wir uns auf die:

- rechtlichen und fachlichen Anforderungen
- sichere elektronische Kommunikation
- die Umsetzung von Dokumentationspflichten (Compliance, Governance)
- Digitalisierung sicherheits-/geschäftsrelevanter Prozesse
- Umsetzung der gesetzlicher Vorgaben
- Anpassungen an bestehender IT-Diensten
- Identifikation von Anwendungsfällen und deren Umsetzung
- Methoden zur langfristigen Beweiswert- und Datenerhaltung
- Entwicklung von Geschäftsmodellen
- Beschreibung technischer Komponenten und deren Funktionalitäten
- Fragen zum Betrieb der künftigen Lösung
- notwendigen organisatorischen Regelungen und Verantwortlichkeiten
- Wirtschaftlichkeitsbetrachtungen

Die in der Konzeption definierten Anforderungen überführen wir bei Bedarf in Ausschreibungsunterlagen und begleiten die Systemimplementierung bis hin zur -abnahme. Wir kennen die relevanten IT-Verfahren

sowie deren Stärken und Schwächen, sind dabei jedoch vollständig herstellerunabhängig und nur den Interessen unserer Kunden verpflichtet.

Einführung

Die Einführung einer eIDAS-konformen Lösung schließt in der Regel unmittelbar an die Konzeption und Beschaffung an und ist ein weiteres Element unseres Serviceangebots. Wir unterstützen unsere Kunden bei allen Fragen rund um die Einführung wie z. B. Konzeption und Durchführung von Softwaretests, Erarbeitung technischer Konzepte oder Überführung des Verfahrens in den Betrieb. Wir übernehmen die Erarbeitung notwendiger organisatorischer Regelungen sowie Coaching- und Schulungsmaßnahmen.

Integration

Um die eIDAS-konforme Lösung wie ePoststelle, elektronisches Siegel, qualifizierte elektronische Signatur fachgerecht in vorhandene oder neu zu schaffende elektronische Geschäftsprozesse einzubinden, unterstützen wir bei der Integration in bestehende IT-Infrastrukturen. Grundlage unseres Vorgehens bildet ein fundiertes Weiterentwicklungskonzept, das sich direkt am Bedarf des Kunden orientiert.

Unsere Arbeit basiert auf geltenden rechtlichen Rahmenbedingungen sowie einschlägigen Standards und Normen, mit denen wir bestens vertraut sind. Daneben wirken wir an der Erstellung und Fortschreibung einschlägiger Standards und Normen aktiv mit:

- im DIN NABD an der Normung der beweissicheren Langzeitspeicherung sowie der Schriftgutverwaltung und des Records Managements
- im BITKOM AK – Anwendung elektronischer Vertrauensdienste

8 Anhang

8.1 Abbildungsverzeichnis

8.2 Abkürzungsverzeichnis

ASiC	Associated Signature Container = ETSI-standardisiertes Signaturcontainer-Format auf ZIP-Basis
BGB	Bürgerliches Gesetzbuch
BNetzA	Bundesnetzagentur
BSI	Bundesamt für Sicherheit in der Informationstechnik
CA	Zertifikatsanbieter
CAdES	CMS Advanced Electronic Signature = ETSI-standardisiertes Signaturformat auf CMS-Basis
eAT	Elektronischer Aufenthaltstitel
eGK	Elektronische Gesundheitskarte
EGovG	E-Government-Gesetz
eID	Elektronische Identifizierung = Prozess der Verwendung von Personenidentifizierungsdaten in elektronischer Form, die eine natürliche oder juristische Person eindeutig repräsentieren; in Deutschland z.B. umgesetzt mittels nPA und eAT
eIDAS	Electronic Identification and Signatures
HSM	Hardware Security Module = eigenständige Einheit zur Generierung sowie zur sicheren Verwaltung und Aufbewahrung von kryptographischen Schlüsseln
nPA	Neuer Personalausweis
PAdES	PDF Advanced Electronic Signature = ETSI-standardisiertes Signaturformat für PDF-Dateien
PKI	Public-Key-Infrastruktur

QES	Qualifizierte elektronische Signatur
QZS	Qualifizierter elektronischer Zeitstempel
SigG	Signaturgesetz
SigV	Signaturverordnung
VDA	Vertrauensdiensteanbieter
VwVfG	Verwaltungsverfahrensgesetz
XAdES	XML Advanced Electronic Signature = ETSI-standardisiertes Signaturformat auf XML-Basis
ZPO	Zivilprozessordnung

Copyright BearingPoint GmbH, Frankfurt/Main, 2015

1. AuflageAlle Rechte vorbehalten.

Der Inhalt dieses Dokuments unterliegt dem Urheberrecht. Veränderungen, Kürzungen, Erweiterungen und Ergänzungen bedürfen der vorherigen schriftlichen Einwilligung durch BearingPoint GmbH, Frankfurt/Main.

Jede Vervielfältigung ist nur zum persönlichen Gebrauch gestattet und nur unter der Bedingung, dass dieser Urheberrechtsvermerk beim Vervielfältigen auf dem Dokument selbst erhalten bleibt. Jede Veröffentlichung oder jede Übersetzung bedarf der vorherigen schriftlichen Einwilligung durch BearingPoint GmbH, Frankfurt/Main.

Gewerbliche Nutzung oder Nutzung zu Schulungszwecken durch Dritte bedarf ebenfalls der vorherigen schriftlichen Einwilligung durch BearingPoint GmbH, Frankfurt/Main.

Fotocredit: Fotolia