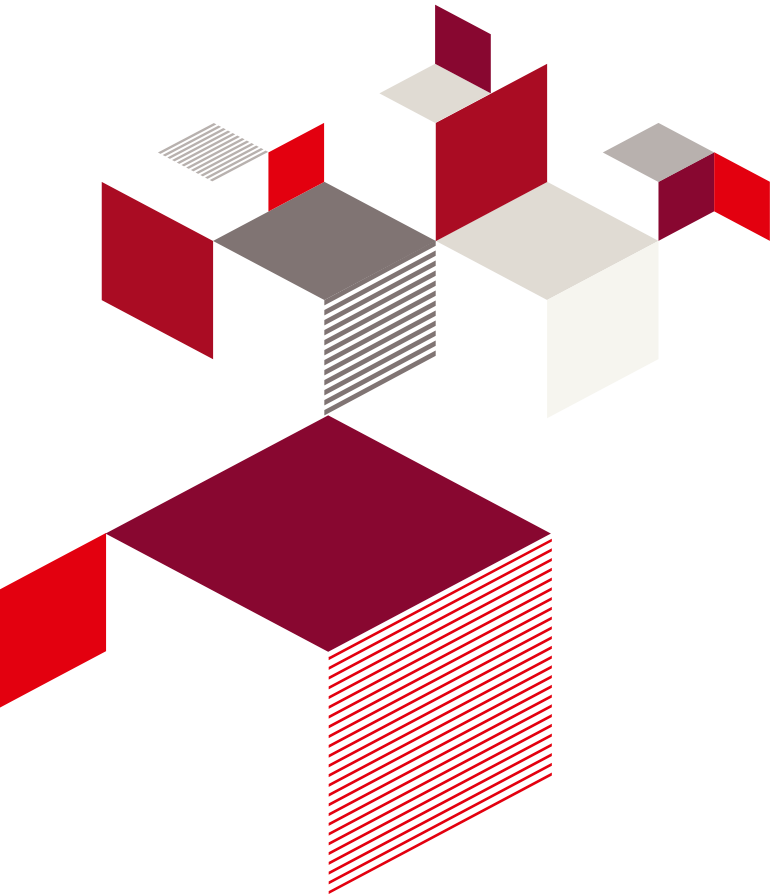
BearingPoint®

eIDAS – neue Chancen und Herausforderungen für vertrauenswürdige elektronische Geschäftsprozesse

Fakten und Handlungsempfehlungen für Entscheider



Inhalt

BearingPoint®

eIDAS – neue Chancen und Herausforderungen für vertrauenswürdige elektronische Geschäftsprozesse

Fakten und Handlungsempfehlungen für Entscheider

Vertrauenswürdige elektronische Geschäftsprozesse können derzeit aufgrund mangelnder Standardisierung und Anerkennung nur begrenzt eingesetzt und so keine Synergieeffekte erzielt werden

Status quo elektronischer Geschäftsprozesse

Trotz EU-Dienstleistungsrichtlinie, EU-Binnenmarkt, E-Government-Gesetz & Co. besteht bei elektronischen Transaktionen und E-Government ein europaweiter Flickenteppich nationaler Standards für sichere und vertrauenswürdige elektronische Geschäftsprozesse, Records Management und Aufbewahrung beziehungsweise Archivierung. Elektronische Signaturen, elektronische Identifizierungsmittel sowie Möglichkeiten zur sicheren elektronischen Kommunikation (wie zum Beispiel De-Mail) konnten sich bisher in Deutschland nicht flächendeckend durchsetzen. Die Möglichkeit sich mit dem elektronischen Personalausweis zu identifizieren sowie mittels einer elektronischen Signatur Dokumente zu unterzeichnen, wird weder von Bürgern noch von Behörden und Unternehmen umfassend genutzt. Gleichzeitig können internationale Lösungen aufgrund mangelnder Standardisierung und Anerkennung nur begrenzt eingesetzt und keine Synergieeffekte erzielt werden.

Wesentliche Hemmnisse bei der Umsetzung sowohl länderübergreifender als auch innerstaatlicher, sicherer elektronischer Prozesse, waren aus deutscher Sicht bislang:

- Rein nationale Regelungen und infolgedessen begrenzte Einsatzgebiete für beispielsweise den Personalausweis, De-Mail in Deutschland und damit verbundene Rechtsunsicherheiten in der internationalen Kommunikation
- Unterschiedliche technische und fachliche Standards in den einzelnen EU-Staaten
- Ausschließlicher Bezug auf eine natürliche Person bei qualifizierten Zertifikaten
- Erzeugung der qualifizierten elektronischen Signatur (QES) nur mit Signaturkarte und damit verbunden hohem organisatorischen wie technischen Aufwand für die Einführung und Anwendung sowie fehlende Benutzerfreundlichkeit.

Im Ergebnis entstanden nur sehr begrenzte Anwendungsfälle sowohl für übergreifende vertrauenswürdige elektronische Transaktionen in Europa als auch für die nationale Anwendung entsprechender Technologien zur Prozesssicherheit. Der Bedarf nach sicheren wie vertrauenswürdigen Transaktionen zur Erfüllung von Compliance konnte so nur bedingt gedeckt werden. Den Technologien fehlt die grundsätzliche Durchdringung und Breitenwirkung.

BearingPoint®

Beispiel: Ein deutsches Unternehmen beteiligt sich an einer öffentlichen Ausschreibung in Schweden

Konkrete Vorteile

Weniger Papieraufkommen

Bisher:

Jetzt:

Kürzere Bearbeitungszeit

Bisher: 1 bis 2 Wochen

Jetzt: Einige Stunden bis wenige Tage

Geringere Kosten

Bisher: 50 bis 100€

Jetzt:10 bis 20€

Nach einer Darstellung „eIDAS – How it will benefit your business?“ der Europäischen Kommission: www.derwid.com/wp-content/uploads/2014/10/eIDASregulationInfographic1.jpg

BearingPoint®

Die eIDAS-Verordnung schafft einheitliche und verbindliche Regelungen für sichere elektronische Geschäftsprozesse

Sie adressiert die Themenkomplexe eID (elektronische Identifizierung) und Vertrauensdienste

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.

Sinn und Zweck ist es einheitliche und verbindliche Regelungen für sichere elektronische Geschäftsprozesse in EU und EFTA zu schaffen. Hierfür gelten folgende Maßgaben gemäß der eIDAS-Verordnung:

eIDAS

Harmonisierung

- eIDAS schafft eine europäische Grundlage für vertrauenswürdige, durchgängig elektronische Geschäftsprozesse
- eIDAS ermöglicht damit die Compliance und Vertrauenswürdigkeit elektronischer Unterlagen in EU und EFTA

Verbindlichkeit

- als Verordnung ist eIDAS unmittelbar geltendes Recht
- eIDAS geht anderslautenden nationalen Regelungen vor – diese werden auf eIDAS angepasst

Akzeptanz

- alle Behörden sind verpflichtet, qualifizierte Vertrauensdienste (Signaturen, Zeitstempel, Siegel) und eID europaweit anzuerkennen – egal in welchem Land welcher Anbieter genutzt wird
- die Zertifizierung erfolgt durch gemeinsame Zertifizierungsstellen auf Basis der eIDAS und europaweiter Standards

Kerninhalte der eIDAS

Die eIDAS-Verordnung adressiert die Themenkomplexe eID (elektronische Identifizierung) und Vertrauensdienste. Diese können von sogenannten Vertrauensdiensteanbietern, nach vorheriger Anerkennung beziehungsweise Zertifizierung, erbracht werden.

BearingPoint®

eIDAS ermöglicht die europaweit eindeutige Identifizierung von Systemen, juristischen und natürlichen Personen

Entfall der Verpflichtung zum Einsatz von Kartenleser und Signaturkarte

Elektronische Unterschrift für Organisationen ohne Personenbezug durch das elektronische Siegel möglich

Einheitliche eID – Elektronische Identifizierung in Europa

eIDAS ermöglicht durch einheitliche Vorgaben die europaweit eindeutige Identifizierung von Systemen, juristischen und natürlichen Personen. Damit werden vertrauenswürdige Transaktionen in Portalen und Netzwerken erleichtert und so der Aufbau von Onlinediensten für Unternehmen wie Behörden spürbar unterstützt. Gleichzeitig ermöglicht dies die Nachvollziehbarkeit und Transparenz der Geschäftsprozesse und in der Folge wirtschaftliche Vorteile, durch technische Vereinfachung,

Einfache und sichere Lösungen durch Serversignaturen und Siegel

Mit der eIDAS-Verordnung entfällt die Verpflichtung zum Einsatz von Kartenleser und Signaturkarte – elektronische Signaturen können so mit begrenztem Aufwand umfassend in elektronische Prozesse integriert werden. Kosteneinsparungen und Effizienzvorteile sind so absehbar. Die Nutzung einer mobilen Signatur eröffnet zudem neue Anwendungsfelder und Geschäftsmodelle wie zum Beispiel in der elektronischen Versicherung, im Gesundheitswesen oder bei Antragsprozessen in öffentlichen Institutionen.

Bisher

Signaturkarte und Lesegerät für Signaturerzeugung nötig

eIDAS

Speicherung der Signaturerstellungsdaten und Erzeugung der Signatur bei VDA möglich

Mehrwerte

- Prozessvereinfachung
- Erleichterte Integration in elektronische Transaktionen und IT
- Kosteneinsparung und neue Geschäftsmodelle
- Mobile Signatur für Smartphone, Tablet etc.

Zusätzlich ermöglicht das elektronische Siegel erstmals in Deutschland die elektronische Unterschrift für Organisationen . Damit ist in Behörden und Unternehmen nicht mehr die qualifizierte elektronische Signatur eines einzelnen Mitarbeiters notwendig. Nebenbei bietet das elektronische Siegel eine einfache Art zur Identifizierung von Organisationen.

Technisches Pendant zur elektronischen Signatur

Erstmals Siegelvergabe für juristische Personen möglich

Nachweis von Integrität und Herkunft der Daten

Qualifiziertes elektronisches Siegel

Einsatzmöglichkeiten

- Zentraler Postausgang
- Ersetzendes Scannen
- Stellvertretersignatur
- Unterschrift für Behörden
- Identifikation der Organisation

Alle qualifizierten elektronischen Signaturen (QES), Zeitstempel und Siegel, jedes qualifizierten Vertrauensdiensteanbieters in Europa müssen durch alle öffentlichen Institutionen europaweit anerkannt und geprüft werden können. So kann im konkreten Anwendungsfall zum Beispiel auch eine französische oder spanische QES in Deutschland genutzt werden und ist durch alle öffentlichen Stellen anzuerkennen.

BearingPoint®

Die eIDAS-Verordnung definiert die beweissichere Aufbewahrung von (elektronischen) Dokumenten

eIDAS vereinfacht elektronische Transaktionen durch die sichere und medienbruchfreie Übertragung elektronischer Unterlagen

Langfristig sicher durch beweiswerterhaltende Aufbewahrung

Die eIDAS-Verordnung definiert weiterhin Maßnahmen zur beweissicheren Aufbewahrung von (elektronischen) Dokumenten. Hintergrund ist das Risiko von veralteten und folglich unsicheren Hash- und Signaturalgorithmen. 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 Bewahrungsdienste sind die Antwort der eIDAS auf diese Herausforderung. Nicht nur in Deutschland lässt sich zum Beispiel mittels der Technischen Richtlinie des BSI TR-ESOR sehr einfach eine beweiswerterhaltende Langzeitspeicherung gemäß europäischer Vorgaben und internationaler Normen umsetzen. Mit TR-ESOR und der eIDAS-Verordnung lassen sich die Vorteile einer europaweit einheitlichen Erzeugung und Prüfung sowie des standardisierten Austauschs signierter Dokumente mit einer effizienten und wirtschaftlichen Beweiswerterhaltung verbinden. Dies wird bei Behörden und europäischen Unternehmen aktuell bereits praktiziert.

Ein solcher beweissicherer Langzeitspeicher beziehungsweise Bewahrungsdienst ermöglicht die Aufbewahrung aller elektronischen Unterlagen unabhängig von einer speziellen Hard- oder Software. Ziel ist der Nachweis elektronischer Prozesse gegenüber Gerichten, Prüfbehörden sowie sonstigen Dritten.

Sichere Kommunikation mit Einschreib- und Zustelldiensten

Die sichere wie medienbruchfreie Übertragung elektronischer Unterlagen ist ein Kernelement von E-Government und elektronischen Transaktionen. Die zweifelsfreie Kenntnis von Sender und Empfänger bei gleichzeitigem Schutz der gesendeten Dokumente ist ein kritischer Erfolgsfaktor für Behörden und Unternehmen. Mit den Einschreib- und Zustelldiensten bietet die eIDAS-Verordnung hier eine Lösung für alle elektronischen Unterlagen.

Ein solcher Dienst soll im Wesentlichen folgende Eigenschaften beinhalten:

- Sichere Authentisierung oder Identifikation von Sender und Empfänger durch vertrauenswürdige Kommunikationsverbindungen
- Verschlüsselte Kommunikation mit der Option einer Ende-zu-Ende-Verschlüsselung
- Eindeutiger Nachweis von Absendung, Zustellung und Empfang einer Nachricht
- Sicherung der Integrität und der Authentizität der Nachrichten
- Erzeugung und Prüfung elektronischer Signaturen und Zeitstempeln
- Beweiswerterhaltung
- Wahrung der Vertraulichkeit und Verfügbarkeit.

Damit wird eine bedarfsgerechte, branchenübergreifende elektronische Kommunikation möglich – unter Wahrung von Compliance und Sicherheit.

BearingPoint®

Die eIDAS-Verordnung leistet einen großen Vorschub für branchenübergeifend sichere, medienbruchfreie elektronische Prozesse und eine EU-weit gültige gerichtsverwertbare Dokumentation in Unternehmen und Behörden

Vertrauenswürdige Transaktionen durch Website-Authentisierung

Neben einer nachweisbaren und sicheren Kommunikation löst die eIDAS auch Fragen zur Vertrauenswürdigkeit und Echtheit von Websites – dem vermutlich wichtigsten Kriterium erfolgreicher Webshops und Onlineauftritte. Diesem Ziel dienen (qualifizierte) Vertrauensdienste zur Website-Authentisierung. Die technischen Standards werden bis 2018 definiert und gelten danach verbindlich für EU und freiwillig für EFTA. Fälschungen und Missbrauch von Websites können so wirksam verhindert werden.

Fahrplan zur Umsetzung

Die **Anerkennung notizierter (qualifizierter) Vertrauensdiensteanbieter (VDA**) muss **ab 01.07.2016** in den Mitgliedsstaaten durch öffentliche Stellen möglich sein. Dies bedeutet, dass VDA ab 01.07.2016 ihre Dienste gemäß eIDAS anbieten könnten. Gleiches gilt für die **Anerkennung notifizierter eID/Authentisierungsdienste ab 18.09. 2018**.

Chancen und Herausforderungen

Mit eIDAS ist erstmals eine EU-weit durchgängige Vertrauenswürdigkeit in elektronischen Prozessen möglich – von der Authentifizierung und Erstellung von Datensätzen bis zur Bearbeitung und beweiswerterhaltenden Aufbewahrung. Die eIDAS-Verordnung leistet damit einen großen Vorschub für branchenübergreifend sichere, medienbruchfreie elektronische Prozesse und eine EU-weit gültige gerichtsverwertbare Dokumentation in Unternehmen und Behörden. eIDAS verspricht spürbare Erleichterung im Scan- und Signaturprozess, zum Beispiel durch elektronische Siegel ohne Personenbezug und Zulassung von Alternativen zur Signaturkarte. Sie sorgt für eine schnelle Verbreitung von Werkzeugen und Methoden zur sicheren und vertrauenswürdigen elektronischen Transaktion, Identifizierung und Nachweisführung.

Die Verordnung wird durch technische Normen untersetzt. Diese legen Sicherheitsanforderungen, technische Formate und Anforderungen an Produkte etc. europaweit einheitlich fest. In den Ausführungsbestimmungen der eIDAS wird direkt auf die Normen verwiesen – so dass diese verbindlich sind! Details hierzu finden sich in unserem Kompendium **„Die Bedeutung der eIDAS-Verordnung für Unternehmen und Behörden“**.

Chancen

- Rechts- und Beweissicherheit durch europaweite Vorgaben
- Europaweit einheitliche Standards sorgen für Interoperabilität, flexible wie wirtschaftliche Lösungen
- Prozessbeschleunigung durch Serversignaturen (Automatisierung)
- Begrenzung des organisatorischen und technischen Aufwands durch Einsatz des Siegels
- Wirtschaftlichkeit und hohe Integrationsfähigkeit durch europaweite Anerkennung
- Hohe Sicherheit und Transparenz durch Vertrauenslisten und gemeinsame Standards
- Leichtere Umsetzung sicherer elektronischer Prozesse und Vermeidung von Medienbrüchen

Herausforderungen

- EU-weite Auswahl an Vertrauensdiensteanbietern und eID-Anbietern
- Erhöhtes Aufkommen von QES/Siegeln
- Anerkennung aller qualifizierten elektronischen Signaturen, Siegel und Zeitstempel durch öffentliche Institutionen
- Anpassung der IT-Infrastruktur
- Laufende Anpassung der technischen Infrastruktur für eID-Zugang, Siegel, Signaturen, Zeitstempel
- Klärung von Verantwortlichkeiten
- Umsetzung der eindeutigen Identifizierung von juristischen Personen (Siegel)
- Korrespondenz zwischen unterschiedlichen Zustelldiensten

BearingPoint®

Handlungsempfehlungen

Aufgrund unserer umfangreichen Projekterfahrung in der Privatwirtschaft und der öffentlichen Verwaltung – von der Fachkonzeption bis zur technischen Umsetzung – möchten wir einige Anregungen für die Umsetzung der eIDAS in Behörden und Unternehmen an die Hand geben:

Wollen Sie sichere wie nachweisbare elektronische Prozesse umsetzen?	Die EU-weite Standardisierung und Interoperabilität durch eIDAS erzeugt hier wesentliche Vorteile. eIDAS vereinfacht zudem die Anwendung entsprechender IT-Verfahren im Vergleich zu bisherigen deutschen regulatorischen Vorgaben.
Wollen Sie Kosteneinsparungen erzielen und Prozesse verschlanken, indem Sie die eID-Funktionen in Ihren Portalen nutzen?	Dann wäre die Verwendung der qualifizierten Identifizierungsdienste von Vorteil.
Wollen Sie Wettbewerbsvorteile erzielen oder neue Angebote aufbauen durch Identifizierungsdienste?	Hier bieten sich zahlreiche Optionen, von der elektronischen Willenserklärung im Allgemeinen bis hin zur digitalen, bisher papierenen Police im Besonderen.
Haben Sie zeitkritische Prozesse, bei denen Papierbindung und Schriftform aufgrund langer Transportwege hinderlich sind?	Dann könnte die Verwendung von eID, Serversignaturen sowie von qualifizierten Einschreib- und Zustelldiensten Ihre Organisation beschleunigen.
Benötigen Sie eine hohe Vertrauenswürdigkeit bei der Identifizierung Ihrer Website und ist für Ihre Kunden die Echtheit Ihrer Website wichtig?	Dann wären die neuen Website-Zertifikate die richtige Wahl.
Signieren Sie elektronische Dokumente derzeit aufwändig mit einer personenbezogenen qualifizierten elektronischen Signatur, zum Beispiel zur Unterzeichnung oder beim ersetzenden Scannen?	Dann könnte der Einsatz des qualifizierten elektronischen Siegels oder einer Serversignatur Ihre Prozesse durch Wegfall des Personen- beziehungsweise Kartenbezugs erheblich vereinfachen.
Wünschen Sie eine hohe Rechtssicherheit in der elektronischen Kommunikation?	Dann kann die Nutzung von qualifizierten Einschreib-/Zustelldiensten sinnvoll sein. Diese wären entgegen nationaler Lösungen EU-weit verfügbar.
Arbeiten Sie mit (nicht nur) elektronisch signierten Dokumenten und möchten deren Beweiswert dauerhaft und gerichtsverwertbar erhalten?	Dann empfehlen sich die neuen qualifizierten Bewahrungsdienste für die beweiswerterhaltende Langzeitaufbewahrung (nicht nur) elektronisch signierter Dokumente.
Verfügen Sie über große physische Papierarchive, die Sie zum Beispiel durch ersetzendes Scannen* abbauen möchten, um Miet- und Recherchekosten zu reduzieren?	Dann sind die neuen qualifizierten elektronischen Siegel ohne Personenbezug und die qualifizierten Bewahrungsdienste eine kostengünstige Option.
Suchen Sie nach neuen Geschäftsmodellen auf Basis der eIDAS-Verordnung?	Dann können Sie als Service Provider diese Dienste anbieten und Ihren Kunden die Vorteile der eIDAS unmittelbar verfügbar machen.

* Unter ersetzendem Scannen wird das Scannen mit anschließender Vernichtung des Originals bei weitgehender Beibehaltung des Beweiswerts verstanden

BearingPoint®

Kontakt

Stephan Weber
Partner
stephan.weber@bearingpoint.com

Weitere Informationen:
Kompendium „Die Bedeutung der eIDAS-Verordnung für Unternehmen und Behörden“

Über BearingPoint

BearingPoint Berater haben immer im Blick, dass sich die wirtschaftlichen Rahmenbedingungen permanent verändern und die daraus entstehenden komplexen Systeme flexible, fokussierte und individuelle Lösungswege erfordern. Unsere Kunden, ob aus Industrie und Handel, der Finanz- und Versicherungswirtschaft oder aus der öffentlichen Verwaltung, profitieren von messbaren Ergebnissen, wenn sie mit uns zusammenarbeiten. Wir kombinieren branchenspezifische Management- und Fachkompetenz mit neuen technischen Möglichkeiten und eigenen Produkt-Entwicklungen, um unsere Lösungen an die individuellen Fragestellungen unserer Kunden anzupassen. Dieser partnerschaftliche, ergebnisorientierte Ansatz bildet das Herz unserer Unternehmenskultur und hat zu nachhaltigen Beziehungen mit vielen der weltweit führenden Unternehmen und Organisationen geführt. Unser globales Beratungs-Netzwerk mit 9.700 Mitarbeitern unterstützt Kunden in über 70 Ländern und engagiert sich gemeinsam mit ihnen für einen messbaren und langfristigen Geschäftserfolg.

Für weitere Informationen: www.bearingpoint.com

BearingPoint®

www.bearingpoint.com