

Elektronische Vertrauensdienste verstehen und anwenden

Leitfaden

Oktober 2026

bitkom

Inhalt

1 Elektronische Vertrauensdienste als Grundlage sicherer digitaler Prozesse 3

2 Die eIDAS-Verordnung schafft den europäischen Rechtsrahmen für elektronische Vertrauensdienste 5

Von eIDAS 1.0 zu eIDAS 2.0 5

Identifizierung und Authentifizierung: Das Fundament jedes Vertrauensdienstes 6

Qualifiziert oder nicht-qualifiziert? 6

Blick über die EU hinaus: Interoperabilität mit der Schweiz 7

Umsetzung des Onlinezugangsgesetzes (OZG) 8

3 Elektronische Vertrauensdienste in der Praxis 9

Elektronische Signatur 9

Elektronisches Siegel 10

Elektronischer Zeitstempel 11

Elektronischer Einschreibdienst oder Zustelldienst 12

Website-Authentifizierungszertifikate 13

Elektronischer Bewahrungsdienst 13

Elektronischer Archivierungsdienst 15

Elektronische Attributsbescheinigung 17

Elektronisches Journal (Ledger) 19

4 So gelingt der Einstieg 20

Erste Schritte für Unternehmen und Organisationen 20

Was man bei der Auswahl eines Vertrauensdiensteanbieters berücksichtigen kann 20

Integration in bestehende Prozesse 21

5 Glossar 22

1 Elektronische Vertrauensdienste als Grundlage sicherer digitaler Prozesse

Elektronische Vertrauensdienste sind für Unternehmen und öffentliche Stellen in Deutschland und Europa unerlässlich, weil sie die **Grundlage für rechtssichere und effiziente digitale Prozesse** schaffen, die für die digitale Transformation notwendig sind.

Sie adressieren zentrale Herausforderungen digitaler Prozesse und Anwendungen, insbesondere die **Sicherstellung von Authentizität, Integrität und Vertraulichkeit**. In einer vollständig digitalen Umgebung sind diese Schutzziele von entscheidender Bedeutung. Die zunehmende Zugänglichkeit technischer Möglichkeiten gepaart mit einem Anstieg der Ambitionen, vermeintlich rechtsfreie Bereiche im digitalen Raum für kriminelle Aktivitäten zu nutzen, stellt ein erhebliches Missbrauchspotenzial dar. Dies erfordert von Gesellschaft, Staat und Unternehmen eine anhaltende und kontinuierliche Gegenwehr.

Vertrauensdiensteanbieter (engl. Trust Service Provider, kurz TSP) als europaweit regulierte und national in ihrer Konformität überprüfte Dienstleister bieten in diesem Umfeld einen sicheren und zuverlässigen Anlaufpunkt für entsprechende Komponenten in den Digitalisierungsvorhaben.

- **Rechtssicherheit und Authentizität**: Vertrauensdienste sind weit mehr als technische Werkzeuge; sie sind die rechtliche Infrastruktur für das digitale Zeitalter und gewährleisten rechtssichere und authentische digitale Prozesse. Eine qualifizierte elektronische Signatur (QES) ist beispielsweise der handschriftlichen Unterschrift rechtlich gleichgestellt und ermöglicht Unternehmen und Behörden, Dokumente und Prozesse rechtsverbindlich zu digitalisieren.
- **Effizienz und Kostenreduktion:** Die Digitalisierung von Geschäftsprozessen unter Einsatz von Vertrauensdiensten kann die Effizienz erhöhen und Kosten reduzieren. Dabei entfallen Medienbrüche etwa durch das Drucken, Unterschreiben, Scannen und das postalische Versenden von Dokumenten. Automatisierte digitale Abläufe tragen dazu bei, Zeit und Ressourcen zu sparen und Bearbeitungszeiten zu verkürzen.
- **Stärkung des Verbrauchervertrauens**: Im digitalen Raum ist das Vertrauen der Nutzerinnen und Nutzer in die Sicherheit und Integrität von Daten und Transaktionen entscheidend. Vertrauensdienste bieten hierfür eine solide Basis. Ein gültiger qualifizierter elektronischer Zeitstempel kann unwiderlegbar beweisen, dass ein bestimmtes Dokument zu einem exakten Zeitpunkt existierte und seitdem nicht verändert wurde, solange dieser Zeitstempel seine Gültigkeit nicht verloren hat oder seine Gültigkeit bewahrt wurde. Ein elektronisches Siegel bestätigt die Herkunft und Integrität von Daten einer juristischen Person (z. B. eines Unternehmens). Damit tragen Vertrauensdienste dazu bei, Betrug und Manipulation zu verhindern und das Vertrauen in digitale Angebote zu stärken.

- **Innovation und Wettbewerbsfähigkeit**: Vertrauensdienste sind nicht nur Werkzeuge zur Optimierung bestehender Prozesse, sondern Katalysatoren für neue digitale Geschäftsmodelle. Die Nutzung dieser Dienste ermöglicht es Unternehmen, schnellere, sicherere und kundenfreundlichere Dienste anzubieten. Damit stärken sie die Wettbewerbsfähigkeit und digitale Souveränität Deutschlands und Europas.

Vertrauensdienste spielen eine zentrale Rolle für die digitale Transformation in Deutschland, da sie die **Grundvoraussetzung für die Schaffung rechtssicherer, effizienter und vertrauenswürdiger digitaler Ökosysteme** sind. Sie sind der Kitt, der die technischen und rechtlichen Aspekte der Digitalisierung zusammenführt und es Deutschland ermöglicht, im internationalen Vergleich aufzuholen und eine führende Rolle einzunehmen.

2 Die eIDAS-Verordnung schafft den europäischen Rechtsrahmen für elektronische Vertrauensdienste

Von eIDAS 1.0 zu eIDAS 2.0

eIDAS 1.0 (2014)

Die Erbringung von Vertrauensdiensten ist seit 2014 in der **eIDAS-Verordnung (EU) Nr. 910/2014** (eIDAS 1.0) geregelt – eIDAS steht für electronic Identification, Authentication and Trust Services. Hierbei verfolgt die eIDAS-Verordnung das Ziel, einen einheitlichen europäischen Rechtsrahmen für elektronische Identifizierung und Vertrauensdienste zu schaffen, grenzüberschreitende digitale Transaktionen zu erleichtern und das Vertrauen in digitale Prozesse durch die EU-Vertrauensliste als öffentlichen Vertrauensanker zu stärken.

Hierzu sieht die eIDAS 1.0 Folgendes vor:

- Vergleichbare Anforderungen an die Vertrauensdiensteanbieter und ein vergleichbares Aufsichts- und Zertifizierungsregime.
- EU-weite Anerkennung aller Vertrauensdienste und damit Schaffung eines gemeinsamen europäischen Marktes.
- Gegenseitige Anerkennung der von den Mitgliedstaaten notifizierten elektronischen Identifizierungsmittel.
- Festlegung von Signatur- und Siegelformaten, die die Verwaltung akzeptieren muss, sofern sie mit elektronischen Siegeln und Signaturen arbeitet.
- Regelung der Rechtswirkungen qualifizierter Vertrauensdienste. Beispielsweise hat hierdurch die QES den gleichen Beweiswert wie eine händische Unterschrift.

eIDAS 2.0 (2024)

Trotz des mit eIDAS 1.0 geschaffenen gemeinsamen Rechtsrahmens blieben zentrale Herausforderungen bestehen: Nationale eID-Systeme folgten unterschiedlichen Standards, elektronische Identifizierung war vor allem auf den öffentlichen Sektor ausgerichtet und die grenzüberschreitende Nutzung blieb begrenzt. Die Novellierung durch die **eIDAS-Verordnung (EU) 2024/1183** (eIDAS 2.0) soll diese Lücken schließen, die Anwendung in den Mitgliedstaaten stärker vereinheitlichen und elektronische Identifizierung auch für private Anwendungsfälle ausbauen. Hierzu wurden

ausdrücklich technische Standards referenziert, um die Harmonisierung der Vertrauensdienste weiter zu forcieren. Zugleich erweitert sie das Spektrum der Vertrauensdienste um etwa die Herausgabe und Prüfung elektronischer Attributsbescheinigungen, den elektronischen Archivierungsdienst und die Erfassung elektronischer Daten in einem elektronischen Journal (Ledger).

Die wichtigste Neuerung der eIDAS-Revision ist jedoch die Schaffung der **European Digital Identity Wallet (EUDI-Wallet)**. Die Mitgliedstaaten werden hierbei verpflichtet, bis Ende 2026 Bürgerinnen und Bürgern die EUDI-Wallet mit ihren Kernfunktionalitäten Identifizierung, Authentifizierung und Nachweisübermittlung zur Verfügung zu stellen. In Deutschland ist der Start für den 2. Januar 2027 mit der d-you geplant. Die EUDI-Wallet hat hierbei zahlreiche Verknüpfungen zu Vertrauensdiensten und zunächst eine verpflichtende Funktionalität zur Erstellung und Auslösung von QES und qualifizierten elektronischen Siegeln. Ferner enthält das EUDI-Wallet-Ökosystem eine kostenlose Bürgersignatur, mit der für nicht gewerbliche Anwendungen kostenfreie QES bezogen werden können. Auch wird die Nachweisfunktion der Wallet mittels Vertrauensdiensten abgebildet, namentlich im Zusammenhang mit qualifizierten (QEAA), öffentlichen (PubEAA) und nicht-qualifizierten elektronischen Attributsbescheinigungen (EAA). Hierdurch entstehen neue Mechanismen zur Nutzung und Verbreitung der Nutzung von Vertrauensdiensten für den öffentlichen Bereich, die Privatwirtschaft sowie Privatpersonen.

Identifizierung und Authentifizierung: Das Fundament jedes Vertrauensdienstes

Jeder in diesem Leitfaden beschriebene Vertrauensdienst beruht letztlich auf der Frage, wie sicher die Identität einer Person oder Organisation festgestellt und bestätigt werden kann. Eine schwache Identifizierung kann den rechtlichen und praktischen Wert des darauf aufbauenden Vertrauensdienstes beeinträchtigen, unabhängig davon, wie stark die zugrunde liegende Kryptografie ist.

Die eIDAS-Verordnung unterscheidet bei elektronischen Identifizierungsmitteln zwischen den **Vertrauensniveaus niedrig, substanziell und hoch**. Sie beschreiben, wie hoch das Vertrauen darin ist, dass eine behauptete Identität tatsächlich der betreffenden Person zugeordnet werden kann. Mit steigendem Vertrauensniveau erhöhen sich die Anforderungen an die Identifizierung und Authentifizierung. Zur Erreichung des jeweiligen Vertrauensniveaus können unterschiedliche Identifizierungsverfahren eingesetzt werden, beispielsweise persönlich begleitetes und automatisiertes Videoident. Die BSI TR-03147 bietet einen Rahmen zur Bewertung des Vertrauensniveaus solcher Identifizierungsverfahren und berücksichtigt dabei auch relevante Angriffsszenarien.

Qualifiziert oder nicht-qualifiziert?

Die eIDAS unterscheidet hierbei bezüglich der einzelnen Vertrauensdienste zwischen qualifizierten und nicht qualifizierten Vertrauensdiensten.

- **Nicht-qualifizierte Vertrauensdienste** (z. B. eine fortgeschrittene Signatur) werden von nicht qualifizierten Vertrauensdiensteanbietern erbracht. Diese unterliegen nur grundlegenden Anforderungen im Bereich Informations- und IT-Sicherheit und der Ex-post-Aufsicht der nationalen Aufsichtsbehörden (in Deutschland der Bundesnetzagentur).
- **Qualifizierte Vertrauensdienste** dürfen nur von qualifizierten Vertrauensdiensteanbietern erbracht werden. Diese bedürfen einer vorherigen Konformitätsbewertung durch eine akkreditierte Konformitätsbewertungsstelle und der Überprüfung der Erfüllung der Anforderungen durch die zuständigen nationalen Aufsichtsbehörden und müssen sich initial und danach regelmäßig durch eine zugelassene, unabhängige Konformitätsbewertungsstelle auditieren lassen. Dabei gelten umfassende Anforderungen an Managementsysteme, insbesondere im Hinblick auf Risiken, Compliance sowie Informations- und IT-Sicherheit:

  - Für die meisten qualifizierten Vertrauensdienste müssen die Nutzerinnen und Nutzer zudem auf einem Vertrauensniveau zwischen substanziell und hoch identifiziert werden, insbesondere durch notifizierte eIDs, um eine sichere Zuordnung des qualifizierten Vertrauensdienstes zum richtigen Nutzer zu gewährleisten.
  - eIDAS sieht auch spezifische technisch-organisatorische Anforderungen an die jeweiligen qualifizierten Vertrauensdienste vor. Zudem gibt es technische Standards und Normen für jeden qualifizierten Vertrauensdienst, die zu einer Harmonisierung der Dienste beitragen.

  Nachdem die zuständige nationale Aufsichtsstelle einem Vertrauensdienst den qualifizierten Status erteilt hat, wird dieser in die nationale Vertrauensliste aufgenommen, die Bestandteil des europäischen Vertrauenslistensystems ist. Die EU-Vertrauensliste wird öffentlich, menschen- und maschinenlesbar geführt und erlaubt es auf diese Weise als zentraler Vertrauensanker allen vertrauenden Beteiligten die qualifizierten Vertrauensdienste auf ihre Gültigkeit zu überprüfen und somit ohne Kontaktierung und Mitwirkung der Vertrauensdiensteanbieter zu validieren.

Blick über die EU hinaus: Interoperabilität mit der Schweiz

Auch über den EU-Rahmen hinaus zeigt sich, wie wichtig anschlussfähige Regelungen für grenzüberschreitende digitale Transaktionen sind. In der Schweiz bildet seit dem 1. Januar 2005 das Bundesgesetz über Zertifizierungsdienste im Bereich der elektronischen Signatur (ZertES) den rechtlichen Rahmen für die Anerkennung elektronischer Signaturen. Mit der Revision zum 1. Januar 2017 wurde das Regelwerk an technische Entwicklungen, internationale Standards und praktische Nutzungsanforderungen angepasst. Obwohl ZertES und eIDAS eigenständige Rechtsrahmen darstellen, zielen fortlaufende Harmonisierungsbemühungen darauf ab,

die technische Interoperabilität sowie die grenzüberschreitende Nutzung und Anerkennung elektronischer Signaturen und Vertrauensdienste zwischen der Schweiz und den EU-Mitgliedstaaten zu fördern.

Umsetzung des Onlinezugangsgesetzes (OZG)

Ein zentraler Treiber der digitalen Transformation in der öffentlichen Verwaltung in Deutschland ist das **Onlinezugangsgesetz (OZG)**. Es verpflichtet Bund, Länder und Kommunen, ihre Verwaltungsleistungen bis Ende 2022 auch digital anzubieten. Vertrauensdienste sind hierfür unerlässlich:

- Bürgerinnen und Bürger können Anträge und Formulare mit ihrer digitalen Identität rechtssicher ausfüllen und elektronisch signieren.
- Behörden können Bescheide und offizielle Dokumente mit einem elektronischen Siegel versehen, um ihre Authentizität zu garantieren.

Ohne Vertrauensdienste wäre die rechtsgültige Kommunikation zwischen Bürgerinnen und Bürger und Staat im digitalen Raum nicht möglich. Sie ermöglichen es, dass die OZG-Ziele überhaupt erst erreicht werden können.

3 Elektronische Vertrauensdienste in der Praxis

Viele deutsche Unternehmen, von mittelständischen Betrieben bis zu Großkonzernen, nutzen Vertrauensdienste, um ihre Geschäftsprozesse zu optimieren und neue digitale Geschäftsmodelle zu erschließen, wie beispielsweise in den folgenden Branchen:

- **Automobilindustrie und Industrie 4.0:** Vertrauensdienste sichern den Datenaustausch zwischen Maschinen und Zulieferern ab, indem sie die Authentizität und Integrität von Daten gewährleisten.
- **Finanz- und Versicherungsbranche:** Kreditanträge, Versicherungsverträge und Kontoeröffnungen können vollständig online und rechtsverbindlich abgewickelt werden.
- **Gesundheitswesen:** Die elektronische Patientenakte und die Telemedizin benötigen Vertrauensdienste, um die sensiblen Patientendaten sicher und authentifiziert zu verarbeiten.

Im Folgenden geben wir einen praxisnahen Überblick über die einzelnen Vertrauensdienste nach der eIDAS-Verordnung.

Elektronische Signatur

Was ist das und welchen Nutzen bietet sie?

Die **elektronische Signatur (ES)** ermöglicht medienbruchfreie digitale Geschäfts- und Verwaltungsprozesse. In ihrer qualifizierten Form ist die **Qualifizierte Elektronische Signatur (QES)** der handschriftlichen Unterschrift rechtlich gleichgestellt.

Wofür kann sie genutzt werden?

Elektronische Signaturen können grundsätzlich für alle Dokumente eingesetzt werden, die eine Unterschrift erfordern. Typische Anwendungsfälle sind:

- Verträge
- Wartungsprotokolle
- Anträge
- Dokumentationen
- Vereinbarungen

Wie funktioniert sie?

Elektronische Signaturen können lokal oder als Fernsignatur erstellt werden. Bei einer Fernsignatur werden alle notwendigen Komponenten durch den (qualifizierten) Vertrauensdiensteanbieter bereitgestellt werden.

Für die Nutzung selbst von (Q)ES wird eine Software benötigt, die die Verbindung zum (qualifizierten) Vertrauensdienst eröffnet. Solche Lösungen umfassen häufig vollständige, kundenspezifisch konfigurierbare Signaturprozesse.

Wesentliche Voraussetzungen für die Erzeugung einer QES sind:

- Identifizierung der unterzeichnenden Person durch den QTSP: per Personalausweis mit Online-Ausweisfunktion, persönlich, mit einer anderen QES, mit einem zertifizierten alternativen Verfahren z. B. Videoident oder automatisiertem Videoident, oder per EUDI-Wallet (ab 2027)
- Eine Zwei-Faktor-Authentisierung (also z. B. PIN + TAN) durch den QTSP

Elektronisches Siegel

Was ist das und welchen Nutzen bietet es?

Das **elektronische Siegel** ist für juristische Personen vorgesehen und übernimmt dort eine der elektronischen Signatur vergleichbare Funktion: Es bestätigt Herkunft und Integrität elektronischer Daten, ohne jedoch eine persönliche Willenserklärung einer natürlichen Person zu ersetzen, und stärkt damit das Vertrauen in automatisierte und datenbasierte Prozesse.

Im öffentlichen Bereich erfüllt gemäß dem OZG 2.0 das **qualifizierte elektronische Siegel** zudem in bestimmten Fällen die Schriftform.

Wofür kann es genutzt werden?

Typische Anwendungsfälle sind:

- Behördliche Bescheide und Dokumente
- Bestätigungen und Beglaubigungen
- Herkunftsnachweise
- Integritätssicherung beim ersetzenden Scannen gemäß der BSI-Richtlinie TR-RESISCAN

Wie funktioniert es?

Technisch ist das elektronische Siegel der elektronischen Signatur ähnlich. Das Siegel kann als Fernsiegel angeboten werden und für die Nutzung wird auch eine Software benötigt, die die Verbindung zum (qualifizierten) Vertrauensdienst herstellt. Je nach Anbieter und Lösung können elektronische Siegel und Signaturen gemeinsam oder getrennt angeboten werden.

Im Gegensatz zur elektronischen Signatur ist das elektronische Siegel nicht an einzelne Nutzerinnen und Nutzer gebunden. Je nach technischer und organisatorischer Ausgestaltung kann für eine Behörde oder ein Unternehmen ein gemeinsames Zertifikat eingesetzt und bei Bedarf um weitere Zertifikate zur Ausfallsicherheit ergänzt werden. Dadurch lässt sich das Siegel einfach in automatisierte Prozesse integrieren und ermöglicht eine schnelle und effiziente Digitalisierung.

Wesentliche Voraussetzungen für die Erzeugung eines qualifizierten Siegels sind:

- Identifizierung der juristischen Person sowie des Siegelinhabers
- Freischaltung des Siegels mittels Zwei-Faktor-Authentisierung durch den Siegelinhaber, wobei die anschließende Erzeugung einzelner Siegel ohne erneute Zwei-Faktor-Authentisierung über eine Maschine-zu-Maschine-Kommunikation (M2M) zwischen dem Anwendungsprogramm des Nutzers und der Siegelsoftware erfolgen kann.

Elektronischer Zeitstempel

Was ist das und welchen Nutzen bietet er?

Der **elektronische Zeitstempel** weist eindeutig und manipulationssicher nach, dass bestimmte elektronische Dokumente oder Datenmengen (wie Dokumente, Nachrichten, Datenbankeinträge oder Transaktionen) zu einem spezifischen, verifizierten Zeitpunkt in einer bestimmten Form existiert haben. Im Gegensatz zur einfachen Systemzeit eines Computers, die leicht verstellbar ist, bietet der qualifizierte Zeitstempel eine unabhängige, kryptografisch gesicherte und gesetzlich anerkannte Zeitbestätigung.

Ebenso wie im Umfeld der Signaturen und Siegel gibt es beim Zeitstempel die Unterscheidung zwischen einfachen und qualifizierten Zeitstempeln. Der **qualifizierte elektronische Zeitstempel** bietet die höchste Sicherheitsstufe und kommt insbesondere für rechtlich kritische Prozesse in Betracht. Der entscheidende Unterschied liegt in der rechtlichen Beweiskraft in allen EU-Mitgliedstaaten und der Quelle der Zeitinformation, geregelt durch die eIDAS-Verordnung. Die Zeitangabe muss auf einer nationalen amtlichen Zeitquelle basieren, die hochgenau und rückführbar ist.

Wofür kann er genutzt werden?

Der qualifizierte elektronische Zeitstempel eignet sich insbesondere für Anwendungsfälle, bei denen Fristen, Prioritäten oder eine belastbare Dokumentation nachgewiesen werden sollen:

- **Justiz und Patentrecht**: Nachweis des Zeitpunkts einer Erfindung oder der Erstellung eines Quellcodes.
- **Öffentliche Verwaltung**: Sekundengenaue Dokumentation der Einreichung von Anträgen oder Ausschreibungsunterlagen.
- **Versicherungen**: Nachweis des genauen Zeitpunkts eines Vertragsabschlusses und der damit verbundenen Ansprüche.

Wie funktioniert er?

Zunächst wird aus dem digitalen Dokument ein kryptografischer Hash-Wert erzeugt. Dieser Hash ist eine Art digitaler Fingerabdruck des Dokuments. Der Hash-Wert wird zusammen mit dem exakten Zeitpunkt an einen Vertrauensdienstanbieter übermittelt,

der auf (EU) 2025/1929[1] basiert und letztlich auf die Policy & Security Requirements in ETSI EN 319 421 verweist, die wiederum auf ETSI EN 319 422 und RFC 3161 verweisen. Dieser bestätigt die Kombination aus Daten und Zeit mit seinem eigenen elektronischen Siegel und sendet den gestempelten Hash-Wert an die Nutzerin oder den Nutzer zurück. Jeder Empfänger kann später anhand des Siegels des TSP überprüfen, ob das Dokument zu dem angegebenen Zeitpunkt existierte und seitdem nicht verändert wurde, sofern die Sicherheit der Signatur oder des Siegels des Zeitstempels bewahrt wurde. Jede nachträgliche Änderung würde einen anderen Hash-Wert erzeugen und wäre dadurch erkennbar.

Der Zeitstempel bindet damit die eindeutig identifizierbaren Daten in der Regel durch eine entsprechende Ergänzung kryptografisch an den Faktor Zeit.

Elektronischer Einschreibdienst oder Zustelldienst

Was ist das und welchen Nutzen bietet er?

Der **Dienst für die Zustellung elektronischer Einschreiben (Electronic Registered Delivery Service, ERDS)** ermöglicht den sicheren, nachweisbaren und rechtsverbindlichen Austausch elektronischer Nachrichten. Er erfüllt im digitalen Raum dieselbe Funktion wie ein klassisches postalisches Einschreiben – bietet aber höhere Sicherheit, schnellere Zustellung und EU-weite Gültigkeit.

Die eIDAS-2.0-Verordnung hat die Anforderungen an ERDS modernisiert und harmonisiert. Die in Deutschland vorgesehene Beweislastumkehr über die Zustellfiktion bei physischen Einschreiben ist bei den ERDS im Rahmen der EU-weit gültigen Verordnung nicht vorgesehen. Der Empfang und die Kenntnisnahme der Nachricht müssen demnach durch den Vertrauensdienst zugesichert werden.

Die eIDAS-Verordnung unterscheidet auch hier zwischen nicht qualifizierten und **qualifizierten elektronischen Einschreibdiensten (QERDS)**. Letztere erfüllen strengere Sicherheits- und Identitätsanforderungen und sind rechtlich vollständig einem Einschreiben mit Rückschein gleichgestellt.

Wofür kann er genutzt werden?

ERDS schaffen so ein europaweit interoperables, vertrauenswürdiges Fundament für den Austausch sensibler oder rechtlich relevanter Dokumente, wie z. B.:

- **Zahlungsaufforderungen, Vertragsunterlagen oder fristgebundene Mitteilungen (B2C/C2C Kommunikation):**
  Digitaler Versand mit Nachweis des Zugangs und des genauen Zeitpunkts.
- **Vertragsangelegenheiten zwischen Unternehmen (B2B Kommunikation):**
  Sichere Übermittlung von Angeboten, Vertragsentwürfen oder rechtsverbindlichen Erklärungen.

[1] ↗Commission Implementing Regulation (EU) 2025/1929.

- **Behördliche Bescheide und Verwaltungsverfahren (A2C/A2B Kommunikation):** Digitale Zustellung von Bescheiden wie Steuerbescheiden, Genehmigungen oder Fristsetzungen sowie Nachweis von Empfang oder Widerspruch.

Wie funktioniert er?

Ein QERDS stellt sicher, dass Absender und Empfänger zuverlässig identifiziert sind, dass die Daten während der Übertragung vor unbemerkten Veränderungen geschützt sind (Integrität) und, dass überprüfbare Nachweise über Versand und Empfang einschließlich der jeweiligen Zeitpunkte vorliegen. Diese Nachweise werden im Rahmen des qualifizierten Zustellprozesses erzeugt und durch qualifizierte elektronische Signaturen oder Siegel sowie qualifizierte elektronische Zeitstempel abgesichert. Sie sind als Beweismittel in gerichtlichen Verfahren zulässig. Die Vertraulichkeit der Kommunikation wird durch geeignete technische und organisatorische Maßnahmen geschützt.

Website-Authentifizierungszertifikate

Was ist das und welchen Nutzen bieten sie?

Website-Authentifizierungszertifikate sichern den Datenverkehr im Internet. Das **qualifizierte Website-Authentifizierungszertifikat (QWAC)** entspricht dem Extended Validation (EV)-Zertifikat und umfasst neben der Validierung der Domain auch die qualifizierte Identifizierung des Websiteinhabers. Somit kann eine Person überprüfen, wer hinter einer Webseite steckt. Dies kann Phishing und ähnliche Betrugsversuche verhindern.

Wofür können sie genutzt werden?

QWACs können zur Sicherung von Websites sowie von QR-Codes und Schnittstellen (APIs) genutzt werden. Beispielsweise sichern QWACs im Anwendungsbereich der PSD2 die Kommunikation über Bankkontoschnittstellen zwischen Zahlungsdienstleistern und Banken.

Wie funktionieren sie?

Website-Authentifizierungszertifikate sind sogenannte Transport-Layer-Security (TLS)-Zertifikate und werden von Inhabern von Websites genutzt. Sie verschlüsseln den Datenverkehr zwischen Website und Besuchenden und verhindern, dass Dritte mitlesen können.

Im Browser werden Website-Authentifizierungszertifikate häufig mit einem kleinen Schloss angezeigt. Im Rahmen von eIDAS 2.0 werden die Browser verpflichtet, QWACs verbraucherfreundlich anzuzeigen, was diesen Effekt noch weiter verbessert.

Elektronischer Bewahrungsdienst

Was ist das und welchen Nutzen bietet er?

Der **elektronische Bewahrungsdienst** ermöglicht die Beweiswerterhaltung von elektronischen Signaturen, Siegeln, Zeitstempeln und Zertifikaten bzw. von Daten

unter Verwendung digitaler Signaturtechniken durch die Aufrechterhaltung der Gültigkeit sowie entsprechender Nachweise über die Existenz der zugehörigen signierten und nicht signierten Daten (Proof of Existence) in dem Zustand, in dem sie sich zum Zeitpunkt der Übergabe an den Bewahrungsdienst befanden. Das gilt auch dann, wenn der Signaturschlüssel später kompromittiert wird, das Zertifikat abläuft oder kryptografische Angriffe auf den Signatur- oder Hash-Algorithmus der übermittelten Signatur möglich werden.

In Deutschland ist das funktionale Ziel des Dienstes durch die BSI TR-03125 TR-ESOR bekannt, die seit 2010 Anforderungen an entsprechende Produkte definiert und als gesetzlicher Stand der Technik zur Bewahrung gilt.

Neben klassischen signierten, gesiegelten oder zeitgestempelten Dokumenten kommen für den Bewahrungsdienst auch elektronische Attributsbescheinigungen oder Nachrichten aus Zustelldiensten als Input infrage, um die Bewahrung digitaler Nachweise zu ermöglichen.

Wofür kann er genutzt werden?

Anwendungsfälle für den elektronischen Bewahrungsdienst sind die Erfüllung jeglicher Dokumentations- und Nachweispflichten, insbesondere im Rahmen gesetzlicher Aufbewahrungsfristen, z. B. von mehr als fünf Jahren oder auch bis zu 110 Jahren nach § 5 des Personenstandsgesetzes, sowie die Absicherung gegen umfangreiche Haftungs- und sonstigen Geschäftsrisiken, die sich aus den Nachweispflichten ergeben.

In der Praxis kann der elektronische Bewahrungsdienst auch in Verbindung mit dem Archivierungsdienst oder einer Archivierungskomponente betrieben werden, sofern sich beide Dienste funktional und technisch ergänzen.

Wie funktioniert er?

Digitale Signaturen – d. h. elektronische Signaturen bzw. elektronische Siegel – sind zu erneuern, wenn die zugrunde liegenden Hash- und/oder Signaturalgorithmen ihre Sicherheitseignung zu verlieren sodass eine unbemerkte Manipulation der signierten bzw. gesiegelten Daten möglich wäre. Dazu benutzt der Bewahrungsdienst digitale Signaturtechniken für die:

- Übersignatur,
- Aufbringung eines neuen Zeitstempels oder
- Erzeugung und Fortschreibung von »Evidence Records« (siehe RFC 4998[2] bzw. RFC 6283[3]).

Dies erfolgt durch Verwendung von Hash-Bäumen, sodass eine Vielzahl von (signierten oder gesiegelten) Daten bzw. Datengruppen oder Signaturen und Siegeln mit genau einem Archivzeitstempel langfristig gesichert werden kann, um jeweils die Integrität und Existenz langfristig sicherzustellen. Bei einem drohenden Verlust der Sicherheitseignung

[2] ↗https://www.rfc-editor.org/rfc/rfc4998.txt
[3] ↗https://datatracker.ietf.org/doc/html/rfc6283

- des Signaturalgorithmus wird der zuletzt erzeugte Archivzeitstempels mit einem zusätzlichen neuen obersten Archivzeitstempel gesichert bzw.,
- des Hashalgorithmus wird ein neuer Hashbaum mit einem aktuell sicherheitsgeeigneten Hash-Algorithmus aufgebaut.

Eine weitere Kernkomponente des Bewahrungsdienstes ist die langfristige Interoperabilität durch standardisierte Protokolle (Preservation-API gemäß ETSI TS 119 512), standardisierte Archivinformationspakete ((L)XAIP, ASiC-AIP) und Beweisdatenformate, für die auch Open-Source-Testprogramme zur Verfügung stehen. Diese sind mit TR-ESOR harmonisiert und ermöglichen den herstellerunabhängigen Austausch und die langfristige Prüfbarkeit kryptografisch geschützter Daten und Dokumente im eIDAS-Raum.

Die TR-ESOR war Grundlage der für den Bewahrungsdienst geltenden europäischen Standards. Ihre Nutzung ermöglicht signifikante Erleichterungen bei der Zertifizierung qualifizierter Bewahrungsdienste. Während die eIDAS-Verordnung auf den Service fokussiert, definiert die TR-ESOR das eingesetzte Produkt.

Elektronischer Archivierungsdienst

Was ist das und welchen Nutzen bietet er?

Der **elektronische Archivierungsdienst** schließt die bislang bestehende Lücke innerhalb der eIDAS-Verordnung für eine vollständige vertrauenswürdige Aufbewahrung elektronischer Unterlagen, indem er den bereits bestehenden Bewahrungsdienst (Beweiswerterhaltung elektronischer Signaturen, Siegel und Zeitstempel) um Funktionen zur Erhaltung der Daten selbst ergänzt. Er ist ein Dienst für die Entgegennahme, die Speicherung, den Abruf und die Löschung elektronischer Daten und elektronischer Dokumente, der ihre Dauerhaftigkeit und Lesbarkeit gewährleistet sowie ihre Unversehrtheit, Vertraulichkeit und den Nachweis ihrer Herkunft während des gesamten Bewahrungszeitraums erhält[4]. Er stellt sicher, dass diese elektronischen Daten und diese elektronischen Dokumente so aufbewahrt werden, dass sie vor Verlust und Veränderung geschützt sind, mit Ausnahme von Änderungen in Bezug auf das Medium oder das elektronische Format[5].

Neben klassischen Daten und Dokumenten kommen als aufzubewahrende Unterlagen für den Archivierungs- wie auch den Bewahrungsdienst auch elektronische Attributsbescheinigungen oder Nachrichten aus Zustelldiensten infrage, da diese ebenfalls digitale Nachweise ermöglichen.

Wofür kann er genutzt werden?

Anwendungsfälle für den elektronischen Archivierungsdienst sind die Erfüllung jeglicher Dokumentations- und Nachweispflichten, insbesondere bei Aufbewahrungsfristen von mehr als fünf Jahren, sowie die Absicherung gegen

[4] Regulation (EU) 2024/1183 of the European Parliament and of the Council of 11 April 2024 amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework, Artikel 3 Nr. 48.
[5] Regulation (EU) 2024/1183 of the European Parliament and of the Council of 11 April 2024 amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework, Artikel 45j.

umfangreiche Haftungs- und sonstigen Geschäftsrisiken, die sich aus den Nachweispflichten ergeben.

In der Praxis kann der elektronische Bewahrungsdienst auch in Verbindung mit dem Archivierungsdienst oder einer Archivierungskomponente betrieben werden, sofern geltende Dokumentations- und Nachweispflichten beide Dienste betreffen können. Bestehende Archivierungslösungen können zudem Komponenten gemäß TR-ESOR umfassen.

Wie funktioniert er?

Der (qualifizierte) Archivierungsdienst umfasst gemäß der eIDAS-Verordnung folgende Funktionen:

- Er verwendet Verfahren und Technologien, die die Beständigkeit und Lesbarkeit elektronischer Daten und Dokumente über die technologische Gültigkeitsdauer hinaus und mindestens während der gesetzlichen oder vertraglichen Aufbewahrungsfrist gewährleisten und gleichzeitig deren Integrität und die Richtigkeit ihrer Herkunft bewahren.
- Er stellt sicher, dass diese elektronischen Daten und Dokumente so aufbewahrt werden, dass sie vor Verlust und Veränderung geschützt sind, mit Ausnahme von Änderungen des Speichermediums oder des elektronischen Formats.
- Er erstellt automatisierte Reports, jeweils versehen mit seiner digitalen qualifizierten elektronischen Signatur, die bestätigen, dass die aus einem (qualifizierten) elektronischen Archiv abgerufenen elektronischen Daten und Dokumente vom Beginn der Aufbewahrungsfrist bis zum Zeitpunkt des Abrufs unverändert sind oder nur eine Formatumwandlung stattgefunden hat. Eine externe Überprüfung, ob die archivierten Daten unverändert geblieben sind, ist nicht vorgesehen.

Für den Nachweis der Herkunft erzeugt der Archivdienst beschreibende Herkunftsinformationen (»Provenance information« als Metadaten, oder der Erzeuger der aufzubewahrenden Daten erzeugt Herkunftsinformationen als beschreibende Metadaten oder mithilfe von digitalen Signaturtechnologien erzeugten (qualifizierten) digitalen Signaturen, die er bzw. sie an den Archivdienst mitübergibt.

Sofern Dokumente und Daten mit (qualifizierten) elektronischen Signaturen, Siegeln oder Zeitstempeln bzw. QEAA oder PubEAA archiviert werden, integriert der Archivierungsdienst entweder eine entsprechende Komponente zu deren Erhalt, z. B. ein Produkt gemäß BSI TR-03125 TR-ESOR, oder einen (qualifizierten) Bewahrungsdienst gemäß der eIDAS-Verordnung. Auch letzterer umfasst in Deutschland i.d.R. eine Komponente gemäß TR-ESOR[6].

Darüber hinaus gilt: Da es sich beim elektronischen Archivdienst um die Aufbewahrung elektronischer Unterlagen handelt, kann deren Integrität (insbesondere über mehrere Jahre hinweg) vernünftigerweise (die Verkehrsfähigkeit muss wegen der zitierten

[6] ↗Commission Implementing Regulation (EU) 2025/2532, https://eur-lex.europa.eu/eli/reg_impl/2025/2532/oj/eng

Nachweispflichten gegeben sein) nur mithilfeder kryptografischer Mittel zugesichert werden. In dem Fall eröffnet sich eine weitere Aufgabe für einen Bewahrungsdienst, um die Gültigkeit dieser Mittel zu erhalten.

Elektronische Attributsbescheinigung

Was ist das und welchen Nutzen bietet sie?

Eine **elektronische Attributsbescheinigung (engl. Electronic Attestation of Attributes, kurz EAA)** ist eine in elektronischer Form vorliegende Bescheinigung, die die Authentifizierung von Attributen ermöglicht. Ein Attribut ist ein Merkmal, eine Qualität, ein Recht oder eine Erlaubnis einer natürlichen oder juristischen Person oder eines Objekts.

Elektronische Attributsbescheinigungen lassen sich in drei Kategorien einteilen:

- **Qualifizierte elektronische Attributsbescheinigungen (QEAA)**: Eine QEAA ist eine von einem QTSP ausgestellte EAA, die die Anforderungen nach Art. 45d und nach Anhang V der eIDAS-Verordnung erfüllt.
  - Mögliche Beispiele: Zertifizierung, Nachweis über Bonität, Konzerttickets; denkbar sind alle Bescheinigungen, die vor allem eine hohe Vertrauenswürdigkeit im Rechtsverkehr benötigen.
- Von oder im Namen einer für eine authentische Quelle zuständigen öffentlichen Stelle ausgestellte elektronische Attributsbescheinigungen (Pub-EAA): Eine Pub-EAA ist eine EAA, die gemäß Art. 45f der eIDAS-Verordnung und Anhang VII von einer öffentliche Stelle[7], die für eine authentische Quelle[8] zuständig ist (Alternative 1), oder von einer öffentlichen Stelle, die von dem Mitgliedstaat dafür benannt wurde, solche Attributsbescheinigungen im Namen der öffentlichen Stellen, die für authentische Quellen zuständig sind, auszustellen (Alternative 2), ausgestellt wurde.
  - Mögliche Beispiele: EU-Gesellschaftsbescheinigung9, digitale EU-Vollmacht10, digitaler Führerschein11, Geburtsurkunde, Meldebescheinigung über den Wohnsitz.
- **Elektronische Attributsbescheinigungen (EAA ohne qualifizierten Status)**: Eine EAA erfüllt nicht die Anforderungen, die an eine QEAA und eine Pub-EAA gestellt werden. Sie werden von einem nicht qualifizierten Anbieter elektronischer Attributsbescheinigungen (NQTSP) ausgestellt, der kein qualifizierter Vertrauensdiensteanbieter im Sinne der eIDAS-Verordnung ist.

[7] Zum Begriff der öffentlichen Stelle siehe die Begriffsbestimmung des Art. 3 Nr. 7 eIDAS-Verordnung.
[8] Zum Begriff der authentischen Quelle siehe die Begriffsbestimmung des Art. 3 Nr. 47 eIDAS-Verordnung.
[9] Siehe Art. 2 Nr. 21 der Richtlinie (EU) 2025/25 (auch bekannt als Digitalisierungsrichtlinie II).
[10] Ebd.
[11] Europäisches Parlament, Pressemitteilung vom 21.10.2025, Mehr Verkehrssicherheit durch modernisierte EU-Fahrvorschriften (↗hier abrufbar; zuletzt aufgerufen am 14.11.2025).

- Beispiele: Nachweis einer Mitgliedschaft, Bescheinigung über die Teilnahme an einem internen Schulungsprogramm.

An die verschiedenen Formen werden unterschiedliche Voraussetzungen und Rechtswirkungen geknüpft. QEAA und Pub-EAA sind allerdings weitestgehend gleichgestellt – auch wenn dies zum Teil in unterschiedlichen Rechtsvorschriften in der eIDAS-Verordnung geregelt ist, siehe insbesondere:

- Anerkennung in anderen Mitgliedstaaten für QEAA und Pub-EAA[12]
- Gleichstellung mit rechtmäßig ausgestellten Bescheinigungen in Papierform
- Pflicht des Ausstellers zur Bereitstellung einer Schnittstelle[13].

Wofür kann sie genutzt werden?

QEAA können überall dort eingesetzt werden, wo bestätigte und vertrauenswürdige Nachweise benötigt werden. Dies sind insbesondere:

- eGovernment-Antragsprozesse
- Bewerbungsprozesse und Mitarbeiter-Onboarding
- Einschreibeprozesse bei Schulen und Universitäten
- Antragsprozesse bei Banken und Versicherungen
- Produktpässe und Management von Lieferketten

Wie funktioniert sie?

Die Nachweise können als maschinenlesbare, strukturierte und EUDI-Wallet-kompatible Credentials ausgegeben werden. Die Credentials sind hierbei nicht nur gegen nachträgliche Veränderung geschützt, sondern machen auch die ausgebende Stelle nachvollziehbar.

QEAAs beinhalten nicht nur die qualifizierte Identifizierung der Nutzerin oder des Nutzers oder des Herausgebers, sondern auch die Validierung der inhaltlichen Richtigkeit der jeweiligen Attribute durch den qualifizierten Vertrauensdiensteanbieter. Hierbei werden Mitgliedsstaaten verpflichtet, für eine breite Anzahl an Nachweisen, bspw. Für Zeugnisse, Erlaubnisse, Steuernummern und Vertretungsbefugnisse, einen Mechanismus zur Verfügung zu stellen. Über diesen können qualifizierte Vertrauensdiensteanbieter die Richtigkeit des Attributs direkt und automatisiert gegenüber der staatlichen authentischen Quelle überprüfen. Einen maßgeblichen Beitrag zum Erfolg des eIDAS- beziehungsweise EUDI-Ökosystems werden vor allem die QEAA leisten.

[12] Nach Art. 45 d, e, f eIDAS-Verordnung.
[13] Nach Art. 45 e eIDAS-Verordnung nur für QEAA und PubEAA.

Elektronisches Journal (Ledger)

Was ist das und welchen Nutzen bietet er?

Das **elektronische Journal** definiert de facto Distributed Ledger Technology (DLT) oder Blockchain als (qualifizierten) Vertrauensdienst. Es löst damit wesentliche Herausforderungen für den Einsatz von DLT in regulierten Branchen durch geprüfte Sicherheit und klare Haftung, wie sie für alle (qualifizierten) Vertrauensdienste gelten. Wichtig zu beachten: Der Dienst umfasst zentrale und Distributed Ledger.

Im Kern wurde der elektronische Ledger in die eIDAS-Verordnung aufgenommen, um die Europäische Blockchain-Service-Infrastruktur (EBSI) auch für regulierte Anwendungen nutzbar zu machen. Dabei handelt es sich um einen von den Mitgliedstaaten betriebenen Ledger.

Wofür kann er genutzt werden?

Anwendungsfälle für den elektronischen Ledger sind z. B.:

- Data-Sharing Agreements gemäß Art. 35 Data Act
- Smart Contracts
- Digitaler Produktpass und Lieferkettennachweise
- Produktherkunftsnachweise
- Tokenization u. a. gemäß MiCAR
- Nachweis und Handel jeglichen Eigentums
- Carbon Credit und Circular Economy
- Notarization
- Digitale Zahlungen und digitaler Euro

Praktisch kann ein elektronischer Ledger als Infrastruktur auch für andere Vertrauensdienste genutzt werden, z. B. als Vertrauensregister für EAA (wie aktuell bspw. für digitale Zeugnisse oder Unternehmensnachweise bei EBSI oder dem Large-Scale-Pilot DC4EU verwendet) oder als Audit Log für Zustelldienste.

Wie funktioniert er?

Wesentliche Funktionen sind:

- Er wird von einem oder mehreren qualifizierten Vertrauensdiensteanbietern erstellt und verwaltet.
- Er gewährleistet die eindeutige, chronologische Reihenfolge der Datensätze im Ledger.
- Er erfasst Daten so, dass jede nachträgliche Änderung sofort erkennbar ist und somit deren Integrität über die Zeit gewährleistet wird, solange die verwendeten kryptografischen Algorithmen ihre Sicherheitseignung noch nicht verloren haben.

4 So gelingt der Einstieg

Der Einstieg in Vertrauensdienste muss nicht kompliziert sein – entscheidend sind ein strukturiertes Vorgehen und eine am konkreten Bedarf ausgerichtete Auswahl. Nehmen Sie zunächst eine ehrliche Evaluierung Ihrer gegenwärtigen Verfahrensweisen vor: Welche Dokumente werden zum jetzigen Zeitpunkt noch ausgedruckt, postalisch versandt oder in Präsenz unterzeichnet? In der Regel sind diese Medienbrüche die besten Kandidaten für eine erste Digitalisierung, bei der Vertrauensdienste eingesetzt werden.

Erste Schritte für Unternehmen und Organisationen

Die Implementierung eines Pilotprojekts, beispielsweise die Einführung elektronischer Signaturen für Arbeitsverträge oder die digitale Archivierung von Rechnungen, hat sich als zielführend erwiesen. Legen Sie bei der Definition präzise dar, welche Funktionalitäten für Sie erforderlich sind: Handelt es sich um einfache elektronische Signaturen für interne Abläufe oder um qualifizierte Signaturen für rechtlich relevante Dokumente? Der Zeitbedarf für ein Pilotprojekt hängt vom konkreten Anwendungsfall sowie von den technischen und organisatorischen Rahmenbedingungen der jeweiligen Organisation ab und kann mehrere Monate betragen. Alle betroffenen Abteilungen sollten von Anfang an einbezogen werden: IT, Recht und Fachabteilungen.

Was man bei der Auswahl eines Vertrauensdiensteanbieters berücksichtigen kann

Bei der Auswahl eines Vertrauensdiensteanbieters bietet es sich an, zunächst zu prüfen, ob der jeweilige Anwendungsfall den Einsatz eines qualifizierten Vertrauensdienstes erfordert oder ob ein nicht qualifizierter Dienst ausreichend ist.

Nicht qualifizierte Dienste können für bestimmte Einsatzszenarien eine geeignete Lösung darstellen. Qualifizierte Vertrauensdienste kommen insbesondere dann in Betracht, wenn gesetzliche Anforderungen, eine erhöhte Beweiskraft oder weitergehende Sicherheitsanforderungen zu erfüllen sind.

Ist ein qualifizierter Vertrauensdienst erforderlich, kann geprüft werden, ob der Anbieter gemäß der eIDAS-Verordnung als qualifizierter Vertrauensdiensteanbieter gelistet ist. Eine Übersicht qualifizierter Anbieter stellt die Bundesnetzagentur über die von der Europäischen Kommission bereitgestellte EU Trusted List zur Verfügung. Dort sind aktive qualifizierte Vertrauensdiensteanbieter entsprechend gekennzeichnet. Darüber hinaus kann berücksichtigt werden, ob der Anbieter die für den jeweiligen Anwendungsfall benötigten Vertrauensdienste, beispielsweise elektronische Signaturen, elektronische Siegel, Zeitstempel oder elektronische Zustelldienste, anbietet.

Neben den regulatorischen Anforderungen können je nach Anwendungsfall auch praktische Gesichtspunkte berücksichtigt werden. Hierzu zählen beispielsweise die Kompatibilität mit bestehenden Systemen, verfügbare Integrationsmöglichkeiten, die Benutzerfreundlichkeit der angebotenen Lösungen sowie transparente und nachvollziehbare Kostenmodelle. Welche Kriterien relevant sind, hängt vom konkreten Bedarf der jeweiligen Organisation ab.

Integration in bestehende Prozesse

In der Praxis liegt die größte Herausforderung häufig weniger in der Technologie selbst als vielmehr in ihrer Einbindung in bestehende Geschäftsprozesse. Der Nutzen von Vertrauensdiensten hängt maßgeblich davon ab, wie gut sie in bestehende Arbeitsabläufe integriert werden. Je nach Ausgangssituation können sowohl eine schrittweise Erweiterung bestehender Systeme als auch eine umfassendere Systemumstellung in Betracht kommen. Welche Vorgehensweise geeignet ist, hängt von den technischen, organisatorischen und wirtschaftlichen Rahmenbedingungen der jeweiligen Organisation ab. Eine nachvollziehbare Dokumentation der angepassten Prozesse sowie die Schulung der Mitarbeitenden können dazu beitragen, die eingesetzten Lösungen sachgerecht anzuwenden.

Eine enge Zusammenarbeit der beteiligten Fachbereiche trägt wesentlich zu einer erfolgreichen Integration bei. Während die fachlichen Anforderungen regelmäßig durch die Businessverantwortlichen definiert werden, übernimmt die IT die technische Umsetzung. Die Bereiche Recht und Compliance begleiten die Einhaltung regulatorischer Anforderungen. Ein abgestimmtes Vorgehen kann dazu beitragen, Implementierungsrisiken zu reduzieren und die Digitalisierung von Geschäftsprozessen zu unterstützen.

5 Glossar

Abkürzung	Deutsche bzw. englische Bezeichnung
EAA	Elektronische Attributsbescheinigung (engl. Electronic Attestation of Attributes)
EBSI	Europäische Blockchain-Diensteinfrastruktur (engl. European Blockchain Services Infrastructure)
eIDAS 1.0	Verordnung (EU) Nr. 910/2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt
eIDAS 2.0	Verordnung (EU) 2024/1183 zur Änderung der Verordnung (EU) Nr. 910/2014 hinsichtlich der Schaffung des europäischen Rahmens für eine digitale Identität
ERDS	Dienst für die Zustellung elektronischer Einschreiben (engl. Electronic Registered Delivery Service)
EV	Extended Validation
M2M	Maschine-zu-Maschine-Kommunikation (engl. Machine-to-Machine Communication)
NQTSP	Nicht qualifizierter Vertrauensdiensteanbieter (engl. Non-Qualified Trust Service Provider)
Pub-EAA	Elektronische Attributsbescheinigung, die von oder im Namen einer für eine authentische Quelle zuständigen öffentlichen Stelle ausgestellt wird (engl. Electronic Attestation of Attributes Issued by or on Behalf of a Public Sector Body Responsible for an Authentic Source)
QEAA	Qualifizierte elektronische Attributsbescheinigung (engl. Qualified Electronic Attestation of Attributes)
QERDS	Qualifizierter Dienst für die Zustellung elektronischer Einschreiben (engl. Qualified Electronic Registered Delivery Service)
QES	Qualifizierte elektronische Signatur (engl. Qualified Electronic Signature)
QTSP	Qualifizierter Vertrauensdiensteanbieter (engl. Qualified Trust Service Provider)
QWAC	Qualifiziertes Zertifikat für die Website-Authentifizierung (engl. Qualified Website Authentication Certificate)

Abkürzung	Deutsche bzw. englische Bezeichnung
TLS	Transport Layer Security
TSP	Vertrauensdiensteanbieter (engl. Trust Service Provider)

Bitkom vertritt mehr als 2.200 Mitgliedsunternehmen aus der digitalen Wirtschaft. Sie generieren in Deutschland gut 200 Milliarden Euro Umsatz mit digitalen Technologien und Lösungen und beschäftigen mehr als 2 Millionen Menschen. Zu den Mitgliedern zählen mehr als 1.000 Mittelständler, über 700 Startups und nahezu alle Global Player. Sie bieten Software, IT-Services, Telekommunikations- oder Internetdienste an, stellen Geräte und Bauteile her, sind im Bereich der digitalen Medien tätig, kreieren Content, bieten Plattformen an oder sind in anderer Weise Teil der digitalen Wirtschaft. 82 Prozent der im Bitkom engagierten Unternehmen haben ihren Hauptsitz in Deutschland, weitere 8 Prozent kommen aus dem restlichen Europa und 7 Prozent aus den USA. 3 Prozent stammen aus anderen Regionen der Welt. Bitkom fördert und treibt die digitale Transformation der deutschen Wirtschaft und setzt sich für eine breite gesellschaftliche Teilhabe an den digitalen Entwicklungen ein. Ziel ist es, Deutschland zu einem leistungsfähigen und souveränen Digitalstandort zu machen.

Herausgeber
Bitkom e.V.
Albrechtstr. 10 | 10117 Berlin

Ansprechpartner/in
Lorène Slous | Referentin Vertrauensdienste & Digitale Identitäten
T 030 27576-157 | l.slous@bitkom.org

Verantwortliches Bitkom-Gremium
AK Anwendung elektronischer Vertrauensdienste

Autorinnen und Autoren
Marc Andreas Eckert | ING-DiBa AG, Iris Hagemann | d.velop mobile services GmbH, Detlef Hühnlein | ecsec GmbH, Ulrike Korte | Bundesamt für die Sicherheit in der Informationstechnik, Norman Krischke | DATEV eG, Focko Lowin | A-Trust Vertrauensdienste GmbH, Kurt Rindle | Swisscom Trust Services AG, Leslie Romeo | Famedly GmbH, Steffen Schwalm | msg systems AG, Henry Wade | Persona Identities (Ireland) Limited, Andreas Wand | D-Trust GmbH

Copyright
Bitkom 2026

Diese Publikation stellt eine allgemeine unverbindliche Information dar. Die Inhalte spiegeln die Auffassung im Bitkom zum Zeitpunkt der Veröffentlichung wider. Obwohl die Informationen mit größtmöglicher Sorgfalt erstellt wurden, besteht kein Anspruch auf sachliche Richtigkeit, Vollständigkeit und/oder Aktualität, insbesondere kann diese Publikation nicht den besonderen Umständen des Einzelfalles Rechnung tragen. Eine Verwendung liegt daher in der eigenen Verantwortung des Lesers. Jegliche Haftung wird ausgeschlossen. Alle Rechte, auch der auszugsweisen Vervielfältigung, liegen beim Bitkom oder den jeweiligen Rechteinhabern.