# Regulated Digital Identity

## Vertrauenwürdige digitale Identitäten für rechtssichere Geschäfte

**Für rechtssichere Geschäfte ist ein rechtssicherer Identitätsnachweis erforderlich. Ohne physischen Kontakt müssen Drittanbieter die Identitäten verifizieren. Digitale Identitäten sind zuverlässiger und sicherer. Sie ermöglichen außerdem eine präzise Auswahl der relevanten Informationen, die ausgetauscht werden sollen.**

### Definition

Digitale Identitäten umfassen sämtliche digitalen Anmeldedaten, etwa für soziale Netzwerke, Banken oder Behörden. Sie garanteiren aber nicht, dass die sich ausweisende Person oder Organisation tatsächlich authentisch ist. Für bestimmte Arten digitaler Geschäfte ist eine sichere Authentifizierung jedoch verpflichtend. In solchen Fällen müssen vertrauenswürdige, typischerweise staatliche Stellen, die digitale Identität bestätigen, etwa durch regulierte digitale Identitäten.

Die Grundlage dafür bildet europaweit die eIDAS-Verordnung, die für „Electronic Identification, Authentication and Trust Services“ steht. Sie regelt den Einsatz von Vertrauensdiensten und die elektronische Identifizierung. Ein Referenzrahmen beschreibt zum einen die Schnittstellen der beteiligten Akteure sowie die Prozesse zur Attestierung und Nutzung digitaler Identitäten, und zum anderen die nationalen Kontrollgremien, die für die Sicherstellung der Vertrauenswürdigkeit verantwortlich sind.

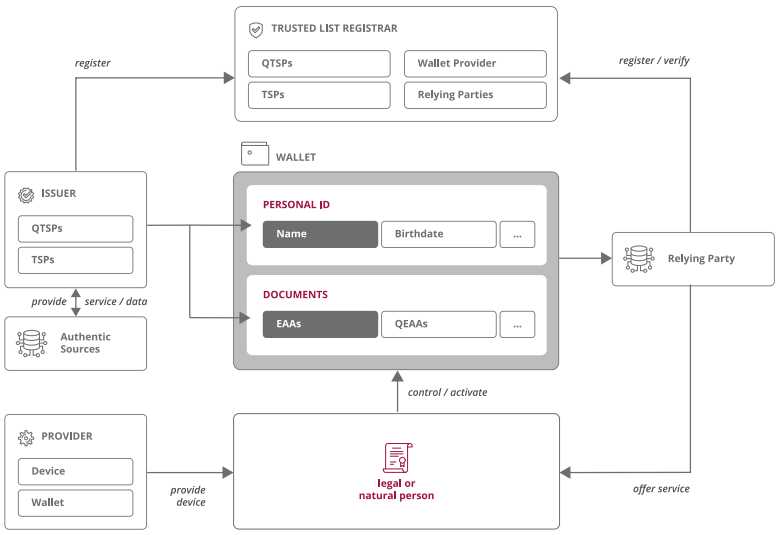
Eine Umsetzung davon ist das EU Digital Identity Wallet, kurz EUDI Wallet. Diese digitale Brieftasche, in Form einer Smartphone-App oder einer Smartcard, speichert sicher persönliche digitale Identitäten (PID) von Personen und Organisationen. Eine staatliche Behörde befüllt das Wallet nach einem physischen Identitätsnachweis zunächst mit der PID. Neben Identitäten können darin auch weitere Dokumente in Form attestierter Attribute abgelegt werden. Diese Attribute werden von Trusted Service Providern (TSP) oder ihrer qualifizierten Form (QTSP), die über eine besondere Vertrauensstellung verfügen, ausgestellt. Zu den Attributen gehören beispielsweise Fahrerlaubnisklassen.

Wallet-Inhaber können anschließend Dienstleistungen von Relying Partys in Anspruch nehmen. Um ein Geschäft abzuschließen, weist die Person oder Organisation ihre Identität mit der PID nach und kann die für das Geschäft erforderlichen attestierten Attribute übermitteln.

### Referenzszenario

Eine Person, die ein Bankkonto eröffnen möchte, muss ihre Identität dem Unternehmen gegenüber durch physische Anwesenheit und eine eigenhändige Unterschrift nachweisen. Das Unternehmen digitalisiert den Prozess nun und registriert sich als Relying Party. Kunden müssen weder persönlich erscheinen noch Identifikationsverfahren von Drittanbietern nutzen und können europaweit rechtssichere Geschäfte mit dem Unternehmen abwickeln.

Ein Unternehmen verlangt von Bewerbern Nachweise der Hochschulabschlüsse. Als Relying Party registriert bietet es ihnen die Möglichkeit, sowohl ihre Identitäts- als auch Abschlussnachweise digital zu erbringen.



### Digitalisierung

- digitale Speicherung von Daten
- Online-Verträge
- elektronische Prozesse
- Smartphones / Smartcards

### Regulatorien

- Geldwäsche-Gesetz
- Onlinezugangsgesetz
- eIDAS
- DSGVO / GDPR
- EU Data Act

RDI

### Globalisierung

- überregionale Zusammenarbeit
- weltweite Lieferketten
- weltumspannender Handel

### Technologie

- PKI - Kryptografische Verfahren
- DLT - verteilte Konten

## Potenzial

Das Potenzial ist insbesondere in einer digitalisierten Welt enorm. Voraussetzung dafür ist, dass jede Person und Organisation über eine digitale Brieftasche verfügt. In dieser müssen die PID (Persönliche Identifikationsdaten) sowie notwendige Dokumente sicher und manipulationsgeschützt verfügbar sein. Die digitale Brieftasche muss europaweit einheitlich gestaltet sein. Es müssen klare Prozesse existieren, die den Ablauf von Attestierungen regeln. Dadurch können Personen und Organisationen europaweit gesetzeskonform digitale Geschäfte abschließen. Physische Kopien von Dokumenten werden überflüssig, und das Verlustrisiko verringert sich. Dank der Dezentralisierung in Form von Wallets behalten die Eigentümer zudem stets die Kontrolle darüber, wem sie welche ihrer Daten offenlegen.

## Reifegrad

Das Konzept ist etabliert und wird bereits bei Online-Geschäften genutzt. Allerdings verwalten die Dienstanbieter die Identitäten ihrer Kunden selbst, was zu mehreren digitalen Identitäten führt. Einige dieser Identitäten sind zudem nicht vertrauenswürdig. Eine europaweite Verordnung wurde bereits ratifiziert.

## Marktübersicht

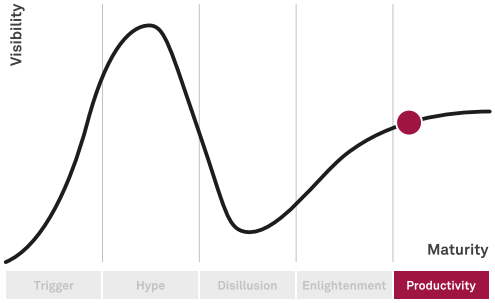
Der deutsche elektronische Personalausweis (ePA) stellt seit 2017 eine regulierte digitale Identität dar. Entsprechende Wallets, etwa die AusweisApp2, wurden bereits erprobt. Registrierte Dienstanbieter nutzen den ePA derzeit zur Authentifizierung, jedoch bleibt die Resonanz eher gering. Im skandinavischen Raum hingegen ist die Akzeptanz deutlich höher, und die Verfahren werden dort wesentlich häufiger genutzt. eIDAS ist eine rechtliche Verordnung für alle europäischen Länder, während die EUDI-Wallet eine europaweite Implementierung dieser Verordnung darstellt. Zahlreiche Dienstanbieter adaptieren sowohl die Verordnung als auch deren Implementierung.

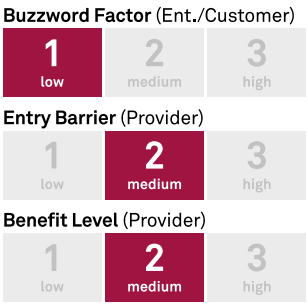
## Alternativen

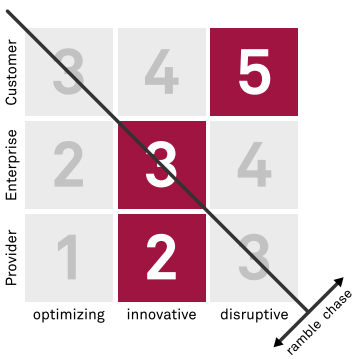
Die gängigste Alternative bleibt der Identitätsnachweis durch physische Anwesenheit. Verschiedene etablierte digitale Identitäten stammen meist aus dem Umfeld sozialer Netzwerke. Diese sind weitgehend akzeptiert, aber weder reguliert noch vertrauenswürdig oder qualifiziert. Die dritte Option sind unsichere Video-Identverfahren, die bei der Ende-zu-Ende-Kontrolle der Datenströme zwischen Kamera und Dienstanbieter Schwächen aufweisen.

## Fazit

- \+ vereinfachte Authentisierung
- \+ ausgelagerte Identitätsprüfung
- \+ digitale Unterschrift
- \+ gesetzeskonforme Lösung
- \+ EU-Harmonisierung durch eIDAS
- \+ einheitlicher Umgang mit Identitätsmerkmalen
- \+ Hoheit über persönliche Daten
- \- vertrauensvolle Identitätsanbieter
- \- für kleine Unternehmen schwierig
- \- EU-weite Lösung nur regional
- \- Akzeptanz unklar




https://msg.direct/techrefresh

Stand: Oktober 2024

**msg systems ag**

Robert-Bürkle-Straße 1 | 85737 Ismaning/München | Telefon: +49 89 96101-0 | Fax: +49 89 96101-1113 | www.msg.group | info@msg.group