über das Telefon

Leben Under Dig

Einleitung

Digitale Identitätssysteme entwickeln sich rasch zum De-facto-Zugangstor zu Staatsbürgerschaft, Handel und Freizügigkeit und schaffen einen zentralen Kontrollpunkt, der dazu genutzt werden kann, jeden, der sich dem widersetzt, digital auszulöschen oder an den Rand zu drängen.

Unsere Untersuchungen zeigen, dass digitale ID-Wallets oder ähnliche Systeme innerhalb von zwei Jahren in 90 % der Länder verfügbar sein werden, wobei die vollständige Einführung in fünf Jahren erwartet wird. Innerhalb eines Jahrzehnts werden gesetzliche Ausweise weitgehend überflüssig sein, was die Abhängigkeit von regionalen, kontrollierbaren digitalen Zugangsdaten für alles von Reisen bis zum Handel erzwingen wird.

Die Fassade der Freiwilligkeit

Das EU- und australische Recht macht die digitale ID ausdrücklich freiwillig.

In Artikel 57 der EU-Verordnung zur Schaffung des europäischen Rahmens für digitale Identitäten heißt es:

> *„Nutzer sollten nicht verpflichtet sein, eine europäische digitale Identitäts-Wallet zu verwenden, um auf private Dienste zuzugreifen, und sollten in* ihrem *Zugang zu Diensten nicht eingeschränkt oder behindert werden,* weil *sie keine europäische digitale Identitäts-Wallet verwenden.“*

Die Verpflichtung zur Nutzung digitaler Identitäten erfolgt indirekt.

Indiens Aadhaar wurde als „freiwillige“ ID eingeführt, wobei Diskriminierung aufgrund dieser ID gesetzlich verboten ist. In der Praxis haben Unternehmen – Mobilfunkanbieter, Spediteure, Vermieter – Aadhaar zu einer Voraussetzung für Dienstleistungen gemacht und es damit faktisch zur Pflicht erklärt.

Ohne digitale ID würde man in Indien ohne Bankkonto, ohne Telefon und möglicherweise ohne Wohnung leben.

Im Vereinigten Königreich sind die Behörden offener. Premierminister Keir Starmer kündigte an, dass eine digitale ID bis 2029 erforderlich sein wird, um im Vereinigten Königreich arbeiten zu können.

Unabhängig von der Regierungsform oder dem Entwicklungsstand finden wir weltweit dieselben Muster – wenn ein Programm für digitale Identitäten zunächst nicht verpflichtend ist, kann es indirekt zur Pflicht werden.

Zweck

Dieser Bericht entmystifiziert die Technologie der digitalen ID, skizziert globale Einführungstrends und präsentiert praktische Lösungen für Personen, die die Kontrolle über ihre Identität behalten möchten.

In drei Abschnitten behandeln wir die Geschichte der digitalen ID und ihre technischen Standards, geben einen Überblick über globale Programme und ziehen Lehren daraus.

> e *Die hierin enthaltenen Daten spiegeln den Stand unserer Recherchen zum Zeitpunkt der Veröffentlichung wider. Da sich die digitale ID rasch weiterentwickelt, können sich die Zahlen inzwischen geändert haben; Leser sollten wichtige Informationen überprüfen, bevor sie handeln. Dieser Bericht dient zu Bildungszwecken und stellt* keine *finanzielle oder rechtliche Beratung dar. Alle Marken sind Eigentum ihrer jeweiligen Inhaber.*

Was ist digitale Identität?

Ein kurzer Rückblick

Digitale Identitäten mögen neu erscheinen, basieren jedoch auf rund 20 Jahren Forschung und Entwicklung.

Die Grundlage der heutigen digitalen Identifikation bildet das Konzept der digitalen Identität, das erstmals vom kanadischen Informatiker Kim Cameron, dem damaligen Architect of Identity bei Microsoft, entwickelt wurde.

- In seiner Abhandlung *„The Laws of Identity“* aus dem Jahr 2004 legte Cameron, der Schöpfer *der digitalen* Identität die Grundsätze für ein interoperables Modell der digitalen Identität fest.
- Die Abhandlung beschrieb ein dezentrales Modell: Der Aussteller könnte eine Regierung, ein Unternehmen oder eine Einzelperson sein; das Subjekt könnte jede Person oder Sache sein; der Prüfer könnte jeder sein.

Camerons Definition der digitalen Identität war einfach – „eine Reihe von Aussagen, die ein digitales Subjekt über sich selbst oder ein anderes digitales Subjekt macht“

Kurz gesagt, Cameron stellte sich eine Methode vor, mit der beliebige Informationen über beliebige Subjekte mit beliebigen Personen ausgetauscht werden können, wobei Privatsphäre und Fairness gewahrt bleiben sollten.

Seine Ideen ebneten den Weg für die heutigen Single-Sign-On-Systeme, technische Spezifikationen für digitale Identitäten und die Argumentation, mit der diese Programme als globales Gut vermarktet werden.

Was ist digitale ID?

Digitale ID ist die formelle Verwendung kryptografisch überprüfbarer digitaler Berechtigungsnachweise zum Nachweis der rechtlichen Identität einer Person. Sie ist ein zentraler Bestandteil der sogenannten Digital Public Infrastructure (DPI), die Identitäts-, Zahlungs- und Datenaustauschsysteme umfasst.

Die digitale ID ist das elektronische Äquivalent zu einem Reisepass, Führerschein oder Personalausweis und wird oft in einer Digital ID Wallet gespeichert – einer App auf einem Smartphone.

Das Digital-ID-Wallet ist die gängigste Methode, um Berechtigungsnachweise persönlich vorzulegen, eine selektive Weitergabe zu ermöglichen und eine Integration mit anderen Anwendungen auf dem Gerät zu gewährleisten.

Ein Wallet ist jedoch kein obligatorischer Bestandteil eines Digital-ID-Programms; dieselben Zugangsdaten können auch über andere Mechanismen bereitgestellt und genutzt werden, wie zum Beispiel:

- Mobile Führerscheine (mDLs) – entweder in einem Wallet oder über eine spezielle App ausgestellt.
- Single Sign-On (SSO) – Web-Login-Dienste, die Zugangsdaten oder Identitätsprüfungen verwenden.
- Portale von Behörden und öffentlichen Dienstleistern – Online-Portale, die Single Sign-On akzeptieren.
- Identitätsprüfung – wird zur Authentifizierung bei Diensten von Drittanbietern (Banken, Versicherungen) verwendet

Kein digitales ID-Programm gleicht dem anderen; die genaue Zusammensetzung der Komponenten hängt von den politischen Zielen der Regierung und den von ihr ausgewählten Technologieanbietern ab.

e Wenn Sie mit einer der Komponenten auf der vorherigen Seite in Berührung kommen, nutzen Sie möglicherweise unbeabsichtigt eine digitale ID.

Eine moderne Definition

Wir definieren ein Digital-ID-Programm als ein nationales oder regionales Identitätssystem, das beide der folgenden Kriterien erfüllt:

1. Digitale Berechtigungsnachweise
   1.1 Das Programm stellt kryptografisch überprüfbare digitale Berechtigungsnachweise aus.
   1.2 Zugangsdaten können in einer Wallet, in der Cloud oder auf einer physischen Karte gespeichert werden
   1.3 Die Registrierung umfasst rechtliche Identitätsdaten und/oder die Erfassung biometrischer Daten.
2. Funktionale Interoperabilität
   2.1 Das System funktioniert sektor- und dienstleistungsübergreifend innerhalb des Zuständigkeitsbereichs.
   2.2 Es ermöglicht die formelle Integration von Drittanbietern (im In- oder Ausland), die die digitale ID nutzen.

e Diese Definition umfasst sowohl moderne Programme, die internationale Standards (eIDAS 2.0) anwenden, als auch speziell entwickelte Systeme wie Indiens Aadhaar oder Chinas Cyberspace ID.

Diese beiden Eigenschaften zusammen können es einem staatlichen *Anbieter ermöglichen, eine Person digital aus ihrem Land* zu *verbannen; aus der Perspektive eines besorgten Bürgers sind sie die folgenreichsten Merkmale.*

Das Spinnennetz des Vertrauens

Frühe Pioniere der digitalen Identität waren Technologieunternehmen, die Identitätsdienste für Unternehmen anboten, wie Microsoft und IBM. Die heutigen Ökosysteme entstehen in Zusammenarbeit mit Normungsgremien, Technologieunternehmen, Bankpartnern und Regierungen.

Diese Akteure schaffen die technische Grundlage und den politisch-wirtschaftlichen Antrieb, die digitale ID-Programme weltweit ermöglichen.

Zu den wichtigsten technischen Organisationen gehören:

Diese technischen Organisationen erstellen die Standards, die von Programmen zur digitalen Identität getestet oder übernommen werden.

- OpenID Foundation – verwaltet OpenID Connect (OIDC), das beliebteste Single-Sign-On-Protokoll, das im gesamten Web verwendet wird
- W3C (World Wide Web Consortium) – veröffentlicht die Verifiable Credentials (VC)-Spezifikation, die interoperable Sprache für kryptografisch signierte Claims, die von vielen modernen nationalen Digital-ID-Programmen verwendet wird.
- ISO (Internationale Organisation für Normung) – gibt Standards wie ISO 18013-5 für mobile Führerscheine heraus

Entwicklungs- und Finanzierungspartner:

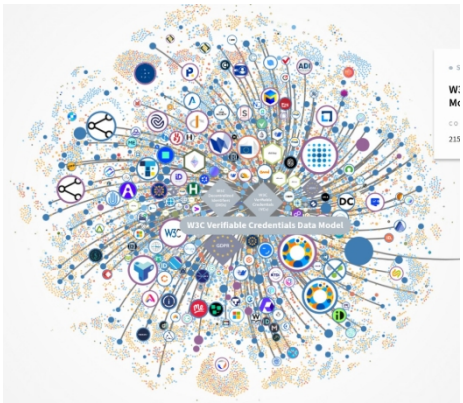
Diese Stiftungen und *Initiativen stellen* die *finanzielle Unterstützung und das Fachwissen bereit, um Identifikationssysteme zu verbessern, insbesondere in Ländern,* die *sich* dies aus *eigener Kraft nicht leisten können.*

- Weltbank – ID4D-Initiative **(Identification for Development)** – bietet technische Unterstützung, vermittelt Zuschüsse und politische Beratung für Länder mit niedrigem und mittlerem Einkommen. Mittlerweile verfügen über 50 Länder in Südamerika, Afrika und Europa über ID4D-Programme.
- Bill & Melinda Gates Foundation – kofinanziert ID4D und andere Pilotprojekte und setzt sich dafür ein, dass die rechtliche Identität als Menschenrecht anerkannt wird. Unabhängig davon hat die Gates Foundation MOSIP mitfinanziert, eine modulare Identitätsplattform, die von Indiens Aadhaar inspiriert ist und derzeit in 11 Ländern getestet wird.
- Vereinte Nationen – **Ziel für** nachhaltige **Entwicklung 16.9** – legt das globale Ziel „Rechtliche Identität für alle, einschließlich Geburtenregistrierung“ fest.
- ID2020 (US-amerikanische NGO) – arbeitet mit Regierungen und Technologieunternehmen zusammen, um Blockchain-gestützte ID-Lösungen für schutzbedürftige Gruppen zu entwickeln, z. B. Bangladeschs Impfpass, das Pilotprojekt für Obdachlosenausweise in Austin, Texas, und die Gesundheitsausweise für Flüchtlinge in Thailand.
- 50-in-5-Initiative – eine von den Vereinten Nationen unterstützte Koordinierungsinitiative, bei der sich 50 Länder verpflichten, ihre digitale öffentliche Infrastruktur (typischerweise die elektronische Identität) innerhalb von fünf Jahren zu modernisieren. Sie hilft Ländern mit niedrigem und mittlerem Einkommen durch Zuschüsse bei der Modernisierung ihrer Systeme.

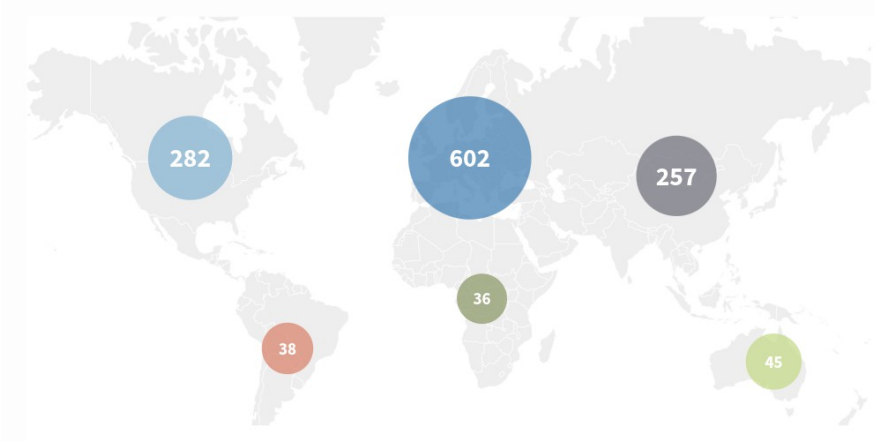
Diese Initiativen stellen die Identifizierung als grundlegendes Menschenrecht dar, machen diese Identitätsnachweise jedoch zu einer Voraussetzung für Grundbedürfnisse wie Nahrung, Gesundheitsversorgung und Bildung. Wir sollten uns fragen, ob eine Person ihre Identität nachweisen muss, um diese grundlegenden Dienstleistungen in Anspruch nehmen zu können.

Ziele im Bereich **der** rechtlichen **Identität**

Die Ziele der Vereinten Nationen für nachhaltige Entwicklung Ziel 16.9 zielt darauf ab, bis 2030 „allen Menschen eine rechtliche Identität zu verschaffen, einschließlich der Geburtenregistrierung“. Aus ihrer Sicht führt das Fehlen einer rechtlichen Identität zum Ausschluss aus der Gesellschaft sowie von Sozialleistungen, Gesundheitsversorgung und Bildung. Dieses SDG-Ziel ist das Leitprinzip für Tausende von Organisationen, die heute dezentrale Identitätssysteme aufbauen.



Das Web-of-Trust-Projekt veranschaulicht, wie groß und koordiniert diese Bemühungen mittlerweile geworden sind.



110	1278
Countries	Public Entities

Continent	Public Entities
Europe	602
North America	282
Asia	257
Oceania	45
South America	38
Africa	36

Digitale Identität: Die technischen Aspekte

Zwei Kernstandards

Digitale ID ist keine einzelne Software, sondern ein gemeinsamer Satz von Standards in Spezifikationen, die die Sprache bestimmen, die die Infrastruktur für digitale Identitäten spricht.

Die beiden wichtigsten Standards, die wir heute sehen, sind:

1. Das W3C-Modell für verifizierbare Berechtigungsnachweise (VC) – eine Spezifikation für die Ausstellung
   kryptografisch signierter Angaben zu einer Person (z. B. Name, Alter, beliebige Details). Es ermöglicht jedem Aussteller, eine Berechtigung zu erstellen, die jeder Inhaber vorlegen und jeder Prüfer validieren kann.
   a. Wird in allen EU-Mitgliedstaaten (eIDAS 2.0), im Vereinigten Königreich, in Thailand und in Japan verwendet
2. ISO 18013-5 – definiert das Format und die Sicherheitsanforderungen für mobile Führerscheine (mDLs). Es legt fest, wie ein physischer Führerschein gespeichert, ausgetauscht (QR, NFC, Bluetooth) und auf dem Gerät oder offline überprüft werden kann.
   a. Verwendet in den USA, der EU, Kanada, Australien und Afrika

Diese beiden Standards sind miteinander kompatibel. Der wesentliche Unterschied besteht darin, dass mDL für die Offline-Prüfung von Führerscheinen in persönlicher Nähe (Bluetooth oder NFC) optimiert ist, während VCs eher universell für jede Art von online geteilten Nachweisen (Diplome, Zertifikate) einsetzbar sind.

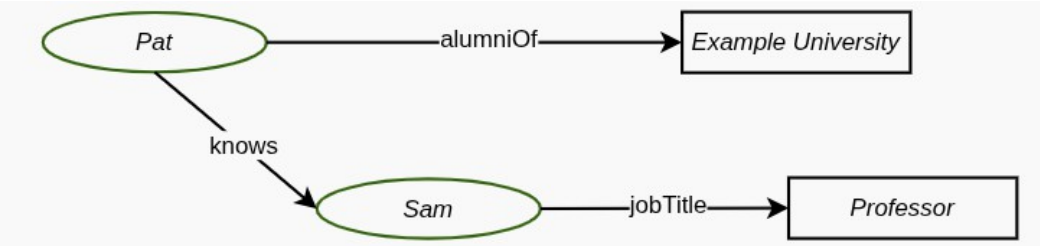


Figure 4 Multiple claims can be combined to express a graph of information.

In dieser VC-Credentia *sehen wir* die *Angabe, dass Pat Absolvent der Beispiel*-Universität *ist und Sam, einen Professor, kennt.*

Das Vertrauensdreieck

Beide Standards definieren die Beziehungen zwischen drei Parteien.

- Der Aussteller erstellt die Berechtigungsnachweise, signiert sie kryptografisch und stellt sie dem Inhaber zur Verfügung.
- Der Inhaber (der Nutzer) verwaltet seine eigenen Berechtigungsnachweise und legt sie dem Prüfer vor
- Der Prüfer erhält die Berechtigungsnachweise und verifiziert sie, indem er sich beim ursprünglichen Aussteller erkundigt

Verifizierer speichern eine Liste der öffentlichen Schlüssel vertrauenswürdiger Aussteller und können diese zur Überprüfung von Berechtigungsnachweisen nutzen. Dieser Berechtigungsnachweis kann bei vielen Diensten als vertrauenswürdig angesehen werden.

Beispiel aus der Praxis

Lassen Sie uns anhand eines Beispiels veranschaulichen, wie digitale Identitäten funktionieren:

- Fred möchte mit einer digitalen ID in seine Stammkneipe gehen
- Fred meldet sich für eine digitale ID an; sein nationales ID-System erstellt eine Berechtigung, die seinen Namen, sein Geburtsdatum, sein Geschlecht und ein Foto enthält. Das ausstellende System signiert die Berechtigung anschließend mit seinem privaten Schlüssel
- Die Berechtigung wird direkt an Freds digitale Identitäts-Wallet auf seinem Mobilgerät gesendet, wo sie gespeichert wird
- Wenn Fred in die Kneipe geht, wird er nach seiner digitalen ID gefragt. Er scannt sein Smartphone, das eine Anfrage der Bar erhält, in der die relevante Berechtigung (sein Alter) angefordert wird, die daraufhin weitergegeben wird
- Das digitale ID-Terminal der Bar überprüft die Signatur des Ausweises mit dem öffentlichen Schlüssel des nationalen ID-Systems

Da sich viele Länder und Organisationen auf den W3C-Standard als Grundlage für ihr Digital-ID-Programm einigen, könnten die prüfenden Stellen in jedem Land (Behörden, Reisekontrollstellen und Einzelhändler) Informationen von in anderen Ländern ausgestellten Digital-IDs erhalten.

Dies ist das interoperable Identitätsmodell, das Cameron als Erster theoretisiert hat, und damit geht die **Möglichkeit** einher**, dass Ihre digitale Identität nicht nur in Ihrem Land**, **sondern weltweit für ungültig erklärt wird**.

Da immer mehr Länder ihre Programme auf der Grundlage von VC und mDLs aufbauen, kann jede Verifizierungsstelle in jedem Land in einem anderen Land ausgestellte Berechtigungsnachweise akzeptieren, solange sie denselben Standard verwenden.

Das bedeutet: Wenn Ihre digitale Identität widerrufen wird, sind die Auswirkungen global – sie können Ihren Status und Ihre Anerkennung überall auf der Welt beeinträchtigen.

> *„Die Möglichkeit, eine Berechtigung in einem Ökosystem auszustellen, sie über eine* beliebige *Wallet vorzulegen und sie in einer anderen Rechtsordnung nahtlos und sicher online zu verifizieren, ist die Zukunft der digitalen Identität. Heute haben wir bewiesen, dass dies nicht nur eine Vision, sondern Realität ist.“*
> – Gail Hodges, Geschäftsführerin der OpenID Foundation

Datenschutzrisiken

Obwohl diese Standards eine Datenminimierung und selektive Offenlegung von Informationen ermöglichen, liegen Datenschutzmaßnahmen in der Verantwortung der Entwickler, und Nutzer können nicht überprüfen, ob Schutzmaßnahmen vorhanden sind.

Wer kann dies überprüfen?

Die Standards betonen, dass der Inhaber der digitalen ID zustimmen muss, bevor Informationen weitergegeben werden, aber die Inhaber können nicht überprüfen, welche Daten tatsächlich weitergegeben werden. Zugangsdaten können überall gespeichert werden, und mobile Führerscheine können in der Cloud (unter der Kontrolle des Ausstellers) gespeichert werden; diese Systeme können geöffnet oder Daten an Dritte weitergeleitet werden (z. B. Überwachung im Stil von PRISM oder Datenaustausch im Rahmen der Five-Eyes-Allianz), ohne dass die Nutzer davon wissen.

Lebensverläufe

Jede Verifizierung (Einkauf im Einzelhandel, Zahlung, Online-Anmeldung) kann protokolliert und an den Aussteller zurückgesendet werden. Aus einem historischen Protokoll lässt sich ein umfassender Lebensverlauf erstellen, der alle Interaktionen einer Person mit dem Ökosystem der digitalen ID detailliert aufzeichnet.

Digitaler Identitätsdiebstahl

Solange fortschrittliche Datenschutztechniken wie Zero-Knowledge-Proofs nicht weit verbreitet sind, erhält ein Verifizierer die Rohdaten der Anmeldedaten (vom Aussteller signiert) im Klartext. Jeder, der diese Daten empfängt oder abfängt, kann die Anmeldedaten anderweitig verwenden und so effektiv **die Identität des Inhabers stehlen.**

Die Kombination aus undurchsichtiger Datenweitergabe, Aggregation von Lebensverläufen und Identitätsdiebstahl macht diese Programme anfällig für Missbrauch.

Globale Analyse digitaler Identitäten

Wie wir Programme klassifizieren

Status	Was das bedeutet
Vollständig	60 % der Bevölkerung nutzen eine digitale ID (Karte oder App), unabhängig davon, ob die Registrierung freiwillig oder de facto obligatorisch ist.
In Betrieb	Das nationale System ist mit einer App oder Web-Integration sowie veröffentlichten technischen Standards vollständig implementiert; die Einführung ist im Gange.
Bestätigt	Ein rechtlicher Rahmen und ein Umsetzungsplan mit klaren Fristen sind vorhanden.
Frühphase	Es gibt Pilotprojekte oder konkurrierende Standards, jedoch keinen festen Zeitplan für die landesweite Einführung.
Nicht verfolgt	Es gibt keine Initiativen seitens der Regierung oder des privaten Sektors zur Schaffung eines digitalen ID-Systems.

Globale Zusammenfassung

In den meisten Ländern ist das System bereits in Betrieb oder bestätigt, viele verfügen über digitale ID-Wallets, andere (typischerweise westliche Länder) lassen die Bundesstaaten MDLs ausstellen, und wieder andere haben Single-Sign-On-Systeme, die durch biometrische Verifizierung abgesichert sind.

Asiatische Länder (China, Indien, Singapur) verfügen über die umfassendsten Programme mit hohen Registrierungsraten. Sie verwenden zudem ihre eigenen proprietären Standards, die nicht auf Kompatibilität mit anderen Ländern ausgelegt sind. Ihre öffentliche Infrastruktur ist eng mit biometrischen Datenbanken verzahnt und wird für alltägliche Dienstleistungen genutzt.

Europa ist führend mit dem größten Staatenblock, der einen koordinierten und interoperablen Standard (eIDAS 2.0) nutzt. Eine digitale ID-Wallet muss den EU-Ländern bis Ende 2026 zur Verfügung stehen, und Unternehmen sind verpflichtet, diese Wallets bis November 2027 zu akzeptieren. Länder wie Dänemark und Estland schreiben eine digitale ID vor und haben eine Akzeptanzrate von über 90 % erreicht.

Nordamerika ist heterogen: Die USA und Kanada vermeiden die Einführung eines einheitlichen nationalen Ausweisprogramms und überlassen es den Bundesstaaten, mobile digitale Ausweise (MDLs) oder digitale Ausweis-Wallets auszustellen. In Kanada haben einige Provinzen die digitale Identifikation für den Führerschein vorgeschrieben, indem sie die Registrierung zur Verlängerung des Führerscheins zur Pflicht gemacht haben. In den USA verlangen einige Bundesstaaten bei der Verlängerung eines Ausweises die Erfassung biometrischer Daten – was bereits für einen digitalen Ausweis ausreicht.

Mexiko hat umfassende Maßnahmen ergriffen und verlangt bis Februar 2026 eine biometrische Identifizierung für alle, um Zugang zu grundlegenden Dienstleistungen wie Bankgeschäften und Mobilfunkdiensten zu erhalten – obwohl das Land mit der Herausforderung einer großen Bevölkerung ohne Papiere konfrontiert ist.

Südamerika hat mit Hilfe von Initiativen der Weltbank in einer Handvoll Ländern operative Erfolge erzielt, die auf Interoperabilität zwischen den Mercosur-Ländern ausgelegt sind. Länder außerhalb des Blocks

haben sich ebenfalls dazu bekannt und arbeiten an Programmen für digitale Ausweise.

Afrikas Hauptaugenmerk liegt darauf, die Bevölkerung ohne Papiere mithilfe von Zuschüssen und Initiativen der Weltbank in biometrischen Ausweissystemen und auf elektronischen Karten zu registrieren. Der westafrikanische Staatenbund ECOWAS nutzt eine interoperable elektronische Karte. In Afrika gibt es 15 Länder, die keine formelle digitale ID verfolgen.

Der Nahe Osten verfügt über zwei vollständige Programme in den Vereinigten Arabischen Emiraten und Saudi-Arabien mit robusten digitalen Ausweisprogrammen, während die übrigen Länder über funktionsfähige digitale Ausweise verfügen oder eine elektronische Identifikation anstreben.

Europa

- eIDAS 2.0 ist eine verbindliche EU-Verordnung, die ein interoperables System für digitale Identitäten für alle 27 Mitgliedstaaten schafft.
- Jedes Land muss bis Ende 2026 eine nationale ID-App auf Basis des EUDI-Wallets einführen; die Apps werden separat sein, aber identischen Standards folgen, was eine grenzüberschreitende Überprüfung ermöglicht.
- Obwohl die Wallet für Bürger „freiwillig“ ist, sind Unternehmen verpflichtet, sie bis 2027 zu akzeptieren – große Online-Plattformen eingeschlossen.

Beispiele aus der EU

- Norwegen – Identitätsanbieter aus dem privaten Sektor für Bankgeschäfte und amtliche Ausweise.
- Österreich – staatlich verwaltete physische Ausweise (= 50 % Abdeckung), die nun auf digitale Wallets umgestellt werden.
- **Schweiz** – 2024 wurde in einem Referendum ein Gesetz zur digitalen ID verabschiedet (50,4 % Zustimmung) mit Plänen, die ID für die Altersüberprüfung und den Kauf von mobilen Diensten verpflichtend zu machen.

Vorreiter bei der Einführung

Estland – Obligatorischer elektronischer Personalausweis seit 2002 (ab 15 Jahren). Die Karte speichert personenbezogene Daten, kryptografische Schlüssel und Fingerabdrücke (hinzugefügt 2021). Sie ermöglicht
> 600 Bürgerdienste und
> 2 400 Unternehmensdienste; derzeit wird eine Digital-ID-App (Eesti) eingeführt, die die Karte ersetzen soll.

Da die Karte obligatorisch ist, haben Esten ohne sie keine Rechte, und jedes wichtige Lebensereignis wird über diese Plattform erfasst.

Dänemark – „MitID“ verzeichnet eine Akzeptanz von 96,6 % (= 5,5 Mio. Nutzer, 2024). Alle Bürger ab 15 Jahren erhalten eine digitale Mailbox (Digital Post) und beziehen behördliche Post über dieses System.

MitID wird als Identifizierungsmethode für Banken, Versicherungsgesellschaften und Energieversorger genutzt. Es wird auch verwendet, um Bewerbungen einzureichen, Arzttermine zu vereinbaren und persönlich zur Altersüberprüfung vorgelegt.

Die MitID-App hat ihre Nutzer im Stich gelassen und erhält im Google Play Store eine erbärmliche Bewertung von 1,6 Sternen. Nutzer sagen, die App sei im Grunde nutzlos, stürze ständig ab, wenn man sich bei anderen Apps authentifiziert, und funktioniere nur mit Google Chrome. Eine frühere Version der App, NemID, legte nach einem DDOS-Angriff im Jahr 2013 das Bankensystem des Landes lahm. Willkommen im digitalen Dänemark.

Trotz der Misserfolge einzelner Staaten mit ihren jeweiligen Programmen bringt die Koordination und

Standardisierung zwischen den europäischen Ländern Europa auf Kurs, bis 2030 über ein vollständig integriertes und interoperables digitales ID-System auf dem gesamten Kontinent zu verfügen.

Vereinigtes Königreich

Fakten zur digitalen ID

Status: In Betrieb
Elektronische ID: Nein
Digitale Geldbörse:
Britcard
Obligatorisch: Ja, bis 2029 für das Recht auf Arbeit.
Biometrische Unterstützung: Gesichtserkennung
Standard: eIDAS-kompatibel (W3C VC)

Zeitplan und Einführung des Programms

- Premierminister Keir Starmer kündigte die Arbeitspflicht für 2025 an; sie wird bis 2029 in Kraft treten.
- Die Integration in den Führerschein ist für Ende 2025 geplant, und alle Ministerien der Zentralregierung müssen die digitale ID bis Ende 2027 neben Papierdokumenten akzeptieren.
- Der GOV.UK One Login SSO-Dienst ist bereits für Regierungswebsites verfügbar und wird später auch Drittanbieterplattformen (z. B. Banken, soziale Medien) zur Identitätsprüfung auf Anfrage angeboten.

Politischer Kontext

- Die Regierung stellt das Programm als Reaktion auf illegale Einwanderung dar und argumentiert, dass ein sicherer, digitaler Kontrollpunkt die Grenzen überwachen und gleichzeitig „die Asylprogramme am Laufen halten“ werde.
- Dieselbe Regierung gab im Haushaltsjahr 2024–2025 1,3 Milliarden Pfund für die Unterbringung von Asylsuchenden in Hotels aus.

Anmerkungen

- Für die Registrierung ist kein Smartphone erforderlich; dies deutet darauf hin, dass sich Bürger über alternative Kanäle wie Termine zur Erneuerung des Personalausweises registrieren können.
- Die Wallet ist der Öffentlichkeit noch nicht zugänglich; ihre einzige derzeitige Funktion ist die Veteranen-Karte, eine breitere Einführung steht noch aus.

Nordamerika

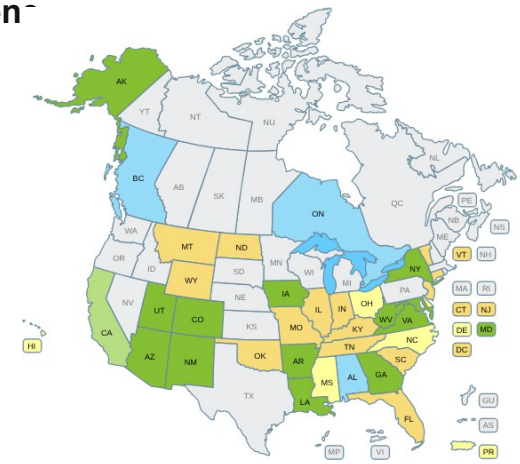
Vereinigte Staaten

Status: Frühphase / In Betrieb (mDL-Wallets)
Elektronischer Ausweis: Je nach Bundesstaat unterschiedlich, erweiterter Führerschein, mobile Führerschein-Wallets Digitales Wallet: Mobile Führerschein-Wallets von Google / Apple
Obligatorisch: Nein
Biometrische Unterstützung: Gesichtserkennung, Standard für amtliche Dokumente: ISO/IEC 18013-5, kompatibel mit eIDAS 2.0

Politischer Hintergrund

- Der **REALID Act** schuf einheitliche Standards für staatlich ausgestellte Ausweise. Das DHS plant, ab Mai 2025 REALIDs für Inlandsflüge vorzuschreiben.
- REALIDs erfordern keine digitale Komponente, doch mehrere bevölkerungsreiche Bundesstaaten in den USA verlangen biometrische Daten für die Erneuerung eines Ausweises, darunter Kalifornien, Texas, Illinois und Washington.
- Millionen US-Bürger sind mittlerweile in einem biometrisch gestützten Identifikationssystem registriert.

Dynamik bei digitalen Ausweisen auf Bundesstaatenebene



- Mobile Führerscheine (mDLs) werden über die großen Mobile-Wallet-Plattformen eingeführt. Für die Registrierung sind ein Selfie und ein Scan des physischen Führerscheins erforderlich.
- Die Secure Technology Alliance verfolgt die Fortschritte bei der Interoperabilität der mobilen Führerscheine (mDL) auf Bundesstaatenebene mit dem Ziel, dass alle Bundesstaaten den Standard ISO/IEC 18013-5 anwenden
  - 12 Bundesstaaten haben bereits die vollständige Konformität erreicht.
  - Weitere 14 Bundesstaaten sind dabei, den Standard aktiv umzusetzen.
- Laut der TSA-Website werden Ausweise wie folgt ausgegeben:
  - Apple Wallet wird in 11 Bundesstaaten unterstützt
  - Google Wallet wird in 9 Bundesstaaten unterstützt
  - Samsung unterstützt 6 Bundesstaaten
  - 9 Bundesstaaten haben ihre eigene proprietäre App für digitale Ausweise entwickelt
- Bundesstaaten wie Colorado, Iowa und New York verfügen über Apps, mit denen Unternehmen mDLs für den Einzelhandel überprüfen können
- Die aktuellen Akzeptanzraten sind relativ niedrig: In den meisten Bundesstaaten liegen sie zwischen 1 und 6 %, in Arizona bei maximal 15 %.

Obwohl es in den USA keine nationale digitale ID gibt, bildet ein Flickenteppich aus MDL-Wallets auf Bundesstaatenebene die technische Grundlage für ein landesweites System.

Kanada

Status: Bundesstaatenabhängig, in Betrieb
Elektronische ID: Nein
Digitale Geldbörse: Bundesstaatsabhängig
Obligatorisch: Von der Provinz abhängig, in British Columbia
zum Autofahren erforderlich Biometrische Unterstützung:
Gesichtserkennung
Standard: elDAS-kompatibel (W3C VC)

Einführung in der Provinz

British Columbia – Abgeschlossen
Die BC Services Card dient als digitale ID der Provinz für das Gesundheitswesen und eine Vielzahl von Behördendienstleistungen. 4,8 Millionen der 5,5 Millionen Einwohner (= 87 %) sind registriert. Die Registrierung war zwischen 2013 und 2018 an die Erneuerung des Führerscheins gekoppelt, und 2019 wurde eine eigene App für die digitale ID eingeführt.

Alberta – In Betrieb
„MyAlberta“ bietet Single Sign-On, eine physische Karte und eine digitale Wallet. Das System funktioniert, die Akzeptanz befindet sich jedoch noch in der Anfangsphase.

Quebec – Bestätigt, aber ausgesetzt
Das Programm wurde gesetzlich genehmigt, ist jedoch derzeit auf Eis gelegt, ohne dass ein Zeitplan für die Einführung vorliegt.

Provinzen in der Anfangsphase – Saskatchewan, New Brunswick, Nova Scotia, Prince Edward Island sowie Neufundland und Labrador haben keine festen Gesetze oder Zeitpläne; sie befinden sich weiterhin in der Pilot- oder Machbarkeitsphase.

Provinzen, die das Projekt nicht verfolgen – Manitoba, Yukon, die Nordwest-Territorien und Nunavut haben keine staatlichen Maßnahmen oder Pläne für ein digitales ID-System.

Kanadas Umfeld für digitale Identitäten ist ein Flickenteppich. British Columbia zeigt, wie die Registrierung effektiv erzwungen werden kann, indem die Identitätsnachweise mit dem Führerscheinrecht verknüpft werden, während andere Provinzen entweder noch in der Testphase sind, vorübergehend pausieren oder gar kein System anstreben. Eine Initiative der Bundesregierung oder eine Änderung der Provinzpolitik könnte diese Landschaft rasch verändern.

Mexiko

Status: Bestätigt
Elektronischer Ausweis: Ja, Einzigartiger
Bevölkerungsregistrierungscode (CURP) Digitale Geldbörse: Noch keine
Obligatorisch: Ja (vor Gericht angefochten) für Wohnraum, Mobilfunkdienste und Internetzugang
Biometrische Daten: Gesichtserkennung, 10 Fingerabdrücke, Iris-Scans
Standard: Proprietär

Zeitplan

- Im Jahr 2020 verabschiedete Mexiko sein erstes Gesetz zur Schaffung einer biometrisch gestützten digitalen Identifikationsdatenbank für jede in Mexiko lebende Person, genannt CUID (Cédula Única de Identidad Digital)
- Später stellte sich heraus, dass die IBRD der Weltbank Mexiko 225 Millionen Dollar für die Umsetzung dieses Systems geliehen hatte
- Das Gesetz stieß auf massiven Widerstand, und 25 Organisationen forderten den mexikanischen Senat auf, das Programm zu stoppen
- Im Juli 2025 wurde ein neues Gesetz verabschiedet, das die CURP (Clave Única de Registro del Población) vorschreibt, eine biometrische ID, die für jede Person erforderlich ist und für den Erwerb von Immobilien, Mobilfunkdiensten und Internetzugang benötigt wird

CURP

- Alle Einwohner müssen eine neue CURP beantragen, die als eindeutige Registrierungsnummer dient
- Die CURP enthält ein Foto, Scans aller zehn Fingerabdrücke sowie Iris-Scans
- Der mexikanische Zivildienst und die Nationalgarde werden Zugriff auf diese Daten haben; es besteht keine Verpflichtung, die Betroffenen über den Zugriff auf ihre Daten zu informieren

Interviews mit US-Beamten deuten darauf hin, dass das Gesetz im Austausch für die Aufhebung der US-Zölle verabschiedet wurde. Präsident Trump forderte im April die biometrischen Daten mexikanischer Migranten als Maßnahme zur Grenzkontrolle.

Da das Gesetz im Juli verabschiedet wurde, scheint es in erster Linie darauf abzuzielen, eine Datenbank aufzubauen, die für Datenaustauschabkommen genutzt werden kann, anstatt die Lebensbedingungen der Einwohner zu verbessern.

Mexiko, Heimat einer großen Bevölkerung ohne Papiere, die im grauen Markt tätig ist, steht vor einer Herausforderung. Die öffentliche Reaktion auf das CURP war überwiegend negativ, und einige Regionen Mexikos haben für die vollständige Autonomie von der Bundesregierung gestimmt.

Mexiko ist das perfekte Beispiel dafür, welche Maßnahmen ein Programm zur digitalen Identifizierung ergreift, wenn es verzweifelt um Akzeptanz ringt. Angesichts einer großen nicht registrierten Bevölkerung in Mexiko wird sich zeigen, ob diese ihre kollektive Macht nutzt und sich gegen das System entscheidet oder sich für die Teilnahme an dem biometrischen Programm entscheidet.

Asien

Ein Blick in die Zukunft für Länder, die sich an digitale ID-Programme halten. Die fortschrittlichsten digitalen ID-Systeme finden sich hier, auch wenn sie unorthodox sind – sie veranschaulichen, wie ein nationales ID-System zu einem Instrument für digitale Spaltung und Menschenrechtsverletzungen werden kann.

China

Status: In Betrieb (Nationale Online-Identitätsauthentifizierung, Cyberspace-ID) / Vollständig (WeChat)
Elektronischer Ausweis:
Ja Digitale Geldbörse:
Noch keine Obligatorisch:
De facto
Biometrische Unterstützung:
Gesichtserkennung Standard: Proprietär

Zeitleiste

- **2012** – **Ende der Anonymität im Internet:** Der Nationale Volkskongress verpflichtete Internetdienstanbieter, Mobilfunkbetreiber und Social-Media-Plattformen, von jedem Nutzer reale Identitätsdaten zu erfassen.
- **2015** – Internet-Realnamensystem: Alle Online-Konten müssen unter einem verifizierten echten Namen registriert werden; Plattformen überprüfen Registrierungen anhand von Selfies und anderen biometrischen Kontrollen.
- **2004–2025** – **Entwicklung des nationalen Ausweisprogramms:** Chinas elektronisches Ausweissystem wurde 2004 eingeführt und 2012 auf die Verwendung von zehn Fingerabdrücken für biometrische Daten ausgeweitet.

Cyberspace-ID

- Ursprünglich als „Nationales Online-Identitätsauthentifizierungssystem“ bezeichnet, entwarf China Gesetze für einen auf einer rechtlichen Identität basierenden Single-Sign-On-Mechanismus, der von Apps und Online-Diensten genutzt werden kann
- Im Juli 2024 wurde ein Pilotprojekt mit über 80 der beliebtesten Apps in China gestartet.
- Nutzer beantragen ihre ID, indem sie sich in einer neuen App anmelden, ihren Personalausweis einscannen und die Gesichtserkennung durchlaufen.
- Dieses Programm ist vorerst freiwillig.

China ist das perfekte Beispiel für ein Land, das bereits vor der Einführung seines offiziellen Digital-ID-Programms über alles verfügte, was für ein digitales ID-System erforderlich ist. Die Cyberspace-ID würde unserer Definition eines digitalen ID-Programms entsprechen, da sie mit vielen Diensten kompatibel ist.

Vor der Einführung von Cyberspace nutzten chinesische „Super-Apps“ wie WeChat und AliPay biometrische Verifizierung und waren mit Tausenden verschiedener Dienste wie Zahlungen, sozialen Medien, Messaging und Reisen integriert. Man könnte argumentieren, dass sie unserer Definition einer digitalen ID entsprechen.

Da fast 100 % der Bevölkerung eine dieser beiden Apps nutzen, könnte man sagen, dass Chinas digitales ID-Programm bereits vor Cyberspace ID vollständig war.

Cyberspace ID steckt noch in den Kinderschuhen: Seit der Pilotphase hat nur 1 % der Bevölkerung die Verifizierungs-App heruntergeladen, was darauf hindeutet, dass sie nicht sehr beliebt ist. Sollte Cyberspace ID weit verbreitet werden oder verpflichtend eingeführt werden, bedeutet dies, dass

Einzelpersonen über alle Apps in China hinweg verfolgt werden könnten.

Indien

Status: In Betrieb (Aadhaar)
Elektronische ID: Ja; Aadhaar – 12-stellige eindeutige ID
Digitale Geldbörse: mAadhaar
Verpflichtend: Freiwillig, aber durch Stellvertreter vorgeschrieben
Biometrische Daten: Gesichtserkennung, zehn Fingerabdrücke, Iris-Scans,
Standard: proprietär

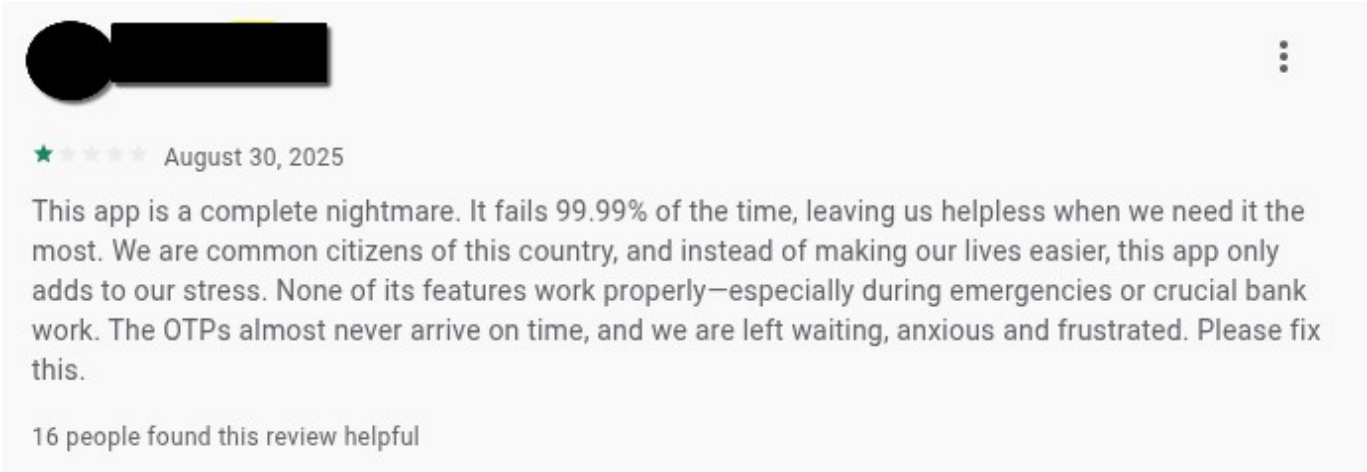
Indiens biometrisches ID-Programm, Aadhaar, ist das weltweit größte seiner Art. Einwohner registrieren sich durch Vorlage von Ausweisdokumenten, Fotos, Fingerabdrücken, Iris-Scans und demografischen Daten (Name, Geburtsdatum, Adresse).

Obwohl das Gesetz zur Formalisierung von Aadhaar erst 2016 verabschiedet wurde, ist das System bereits seit 2009 unter der Leitung der Unique Identification Authority of India (UIDAI) in Betrieb und erfasst mittlerweile
über 1 Milliarde Menschen.

Ein Urteil des Obersten Gerichtshofs aus dem Jahr 2013 machte Aadhaar „freiwillig“, indem es die Verweigerung von Sozialleistungen oder Dienstleistungen für Personen ohne Aadhaar untersagte; in der Praxis wird die ID jedoch indirekt vorgeschrieben:

- Große Banken verlangen Aadhaar für die Eröffnung neuer Konten.
- Mobilfunkbetreiber verknüpfen ihre Dienste mit Aadhaar und drohen bei Nichtbefolgung mit der Sperrung.
- Internationale Spediteure verlangen Kopien von Aadhaar für Sendungen.
- Beliebte E-Commerce-Plattformen nutzen Aadhaar für die Kundenidentifizierung (KYC).
- Vermieter verlangen häufig Aadhaar von potenziellen Mietern.

Obwohl die Aadhaar-ID in erster Linie als Identifikationsnummer dient, die online übermittelt wird, können Einwohner die mAadhaar-App nutzen, um Verifizierungsanfragen für Banktransaktionen und eKYC zu erhalten. Die App erhält in aktuellen Bewertungen schlechte Noten; es wird bemängelt, dass sie nie funktioniert und die Nutzer in kritischen Situationen hilflos zurücklässt.



Singapur

Status: Abgeschlossen (Singpass)
Elektronische ID: Ja
Obligatorisch: Durch Dienstleistungen
Biometrische Unterstützung: Gesichtserkennung, Fingerabdrücke, Iris-Scans
Standard: Unklar

Singpass ist Singapurs digitale ID-Wallet und Single-Sign-On-Plattform (SSO). Obwohl rechtlich nicht verpflichtend, ist ein Singpass-Konto erforderlich, um ein Bankkonto zu eröffnen und Zugang zu Gesundheitsdienstleistungen zu erhalten, wodurch es indirekt vorgeschrieben ist.

Die Plattform ist mit rund 1.400 digitalen Diensten in 340 Regierungsbehörden integriert. Die ID wird biometrisch durch Gesichtserkennung, Fingerabdrücke und Iris-Scans gesichert.

Entwickler können die offene API von Singpass nutzen, um Benutzer zu authentifizieren und Formulare mit persönlichen Daten vorab auszufüllen.

Über 4,5 Millionen Singapurer – etwa 97 % der berechtigten Bevölkerung – nutzen Singpass, was das Programm zu einem Erfolg macht.

Trotz seines Erfolgs ist das System nicht vor Sicherheitsverlet
Sicherheitsunternehmen Resecurity fand 2.377 kompromittierte Singpass-Konten, die im Dark Web gelistet waren. Diese gestohlenen Identitäten wurden anschließend für weitere Betrugsdelikte missbraucht.

Russland

Status: Abgeschlossen (Gosuslugi, Max)
Elektronischer Ausweis: Ja
Verpflichtend: Freiwillig, aber zunehmend wahrscheinlich
Biometrische Unterstützung: Gesichtserkennung, Fingerabdrücke, Stimmabdrücke, **Standard:** Unklar

Inspiriert von Chinas umfassendem App-Ökosystem entwickelt Russland eine „Super-App“ namens Max, die auf jedem im Land verkauften Gerät vorinstalliert sein und in das russische digitale ID-System integriert werden soll.

Zeitplan

- 2009 – Russland startet Gosuslugi, ein Portal für Behördendienstleistungen
- 2021 – Die Zentralbank verpflichtet alle Banken, biometrische Daten (Fingerabdrücke, Gesichtsbilder, Stimmproben) für das Einheitliche Biometrische System (UBS) zu erheben.
- Dezember 2022 – Nachdem bekannt wurde, dass Banken diese Daten in ihren eigenen Systemen speicherten und keine Nutzungsgebühren an das UBS entrichteten, unterzeichnete Putin ein Gesetz, das die Speicherung der Daten innerhalb des UBS vorschreibt, und übertrug die Kontrolle über den Zugriff dem Föderalen Sicherheitsdienst (FSB)
- September 2025 – Alle Geräte im Land müssen mit Max ausgeliefert werden
- Oktober 2025 – Gosuslugi wird zur Zustellung von Einberufungsbescheiden genutzt; Zuwiderhandelnde verlieren die Möglichkeit, das Land zu verlassen, Auto zu fahren oder sich als Unternehmer registrieren zu lassen.

Russland verfolgt einen aggressiven Ansatz in Bezug auf die digitale ID und nutzt sie für militärische Zwecke sowie zur Identifizierung von Demonstranten. Wir diskutieren dies im Abschnitt „Menschenrechte“ am Ende des Berichts.

Andere Länder

Pakistan – NADRA ist Pakistans obligatorischer biometrischer Ausweis in Form einer elektronischen Karte. Er wird von 90 % der Bevölkerung genutzt und ist für alles erforderlich, von der Eröffnung eines Bankkontos über Versand und Mobilfunkdienste bis hin zur Wohnungssuche. Das NADRA-System wird über die Pak ID-App in eine digitale ID umgewandelt, die bereits von 10 Millionen Bürgern genutzt wird.

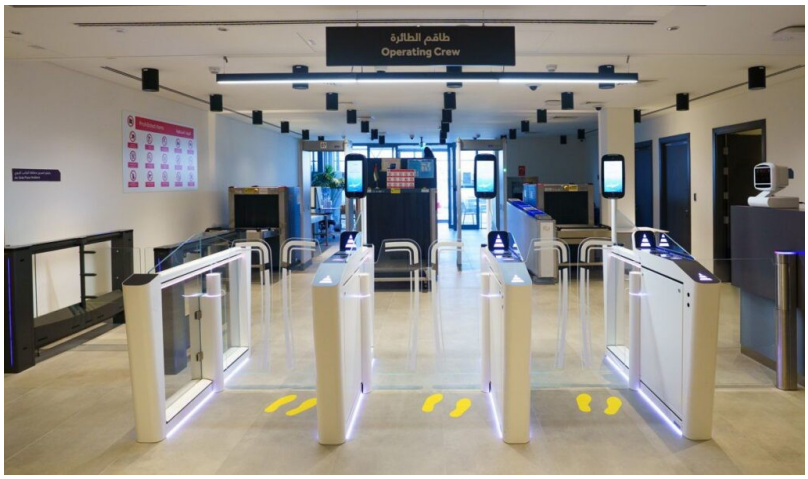
Naher Osten

Insgesamt hinkt diese Region in Asien bei fortschrittlichen digitalen Ausweisprogrammen hinter Europa hinterher. Saudi-Arabien sticht als einziges Land mit einem vollständigen Programm hervor – sechs weitere Länder verfügen über digitale Ausweisprogramme, und die übrigen stellen elektronische Ausweise aus.

Saudi-Arabien – Absher

- Eine digitale Geldbörse, die den physischen Personalausweis ersetzt und bereits an 28 Millionen Menschen ausgegeben wurde.
- Integriert in Nafath, den nationalen Single-Sign-On-Dienst (SSO), der Zugang zu > 500 staatlichen und privaten Diensten bietet.
- Die biometrische Authentifizierung basiert auf Fingerabdrücken und Gesichtserkennung; 94 % der Erwachsenen nutzen zudem digitale Geldbörsen und Bankkonten.

Vereinigte Arabische Emirate – UAE Pass



- Der UAE Pass wurde im Oktober 2018 eingeführt und bietet Funktionen für digitale Identität und digitale Signatur, gestützt auf biometrische Gesichtserkennung.
- Im Jahr 2020 wurde der UAE Pass zum einzigen Weg, um auf staatliche Dienste in Dubai zuzugreifen
- 2 Millionen verifizierte Nutzer bis 2022, etwa 20 % der Bevölkerung; aktuelle Zahlen liegen nicht vor
- Hochmoderne biometrische Erfassung bei Ein- und Ausreise mit berührungslosem Fingerabdruckscan, Iriserfassung aus der Entfernung und automatisierten Kontrollschleusen

Ozeanien

Australien

Status: In Betrieb (AGDIS, mylD)
Elektronischer Ausweis: Ja
Obligatorisch: Freiwillig, wird aber wahrscheinlich durch eine Vertretung vorgeschrieben Biometrische Grundlage: Gesichtserkennung, Dokumente **Standard:** Unklar

Wichtige Punkte

- Das Digital ID Act 2024 schuf die rechtliche Grundlage für das Australian Government Digital ID System (AGDIS). Die mylD-Wallet, die zusammen mit der myGov-SSO-Plattform eingeführt wurde, ermöglicht Bürgern den Zugang zu einem wachsenden Angebot an staatlichen Dienstleistungen.
- mylD bietet drei Sicherheitsstufen; die höchste erfordert einen Reisepass, amtliche Dokumente und die Registrierung mittels Gesichtserkennung.
- In Phase 2 (derzeit) können Bundes-, Landes- und Territorialregierungen als Aussteller oder vertrauende Parteien fungieren. Bis Dezember 2026 können Unternehmen des privaten Sektors – darunter Banken, Social-Media-Plattformen und Mobilfunkanbieter – einen Antrag stellen, um als akkreditierte Aussteller zugelassen zu werden.
- Ein Gesichtserkennungsdienst wurde vorab mit Gesichtserkennungsdaten aus den Führerscheinsystemen der Bundesstaaten gespeist
- Das System ist zentralistischer als die meisten westlichen Pendants und folgt nicht vollständig einem internationalen Standard, doch Australien testet die Interoperabilität:
  - Trust Exchange (TEx)-Pilotprojekt – begrenzter Datenaustausch mit einer Klinik in Queensland (Dez. 2024). VC-Proof-of-Concept – Die Commonwealth Bank of Australia und eine Klinik in Queensland testen W3C-Verifiable-Credentials-Wallets.

    Pilotprojekt im Hafen von Bridgetown – VC-basierte digitale Berechtigungsnachweise für die Bearbeitung von Schiffsmanifesten.
- Mehrere Bundesstaaten (Südaustralien, New South Wales, Queensland und Victoria) stellen bereits mobile Führerscheine nach ISO 18013-5 aus.

Neuseeland

Status: In Betrieb (RealMe) Elektronischer Ausweis: Ja
Obligatorisch: Durch Bevollmächtigung vorgeschrieben
Biometrische Unterstützung: Gesichtserkennung, Dokumente
Standard: Testet W3C-VCs

Das neuseeländische Programm wird in erster Linie über den Identitätsprüfungsdienst RealMe bereitgestellt. Die Registrierung erfolgt anhand von amtlichen Dokumenten und durch Einreichen eines Fotos von sich selbst. Die Registrierung bei RealMe ist erforderlich, um ein Bankkonto zu eröffnen, den Führerschein zu verlängern und sich zur Wahl anzumelden. Bislang haben 1 Million Neuseeländer den Dienst genutzt. Der RealMe Verified Identity Service wird auch für die Beantragung des physischen Altersnachweises (Kiwi Access) und für neuseeländische Sozialprogramme genutzt und ist dafür erforderlich.

Neuseeland experimentiert zudem mit einer digitalen Geldbörse, die den W3C-Standard für überprüfbare Berechtigungsnachweise (Verifiable Credentials) unterstützen wird; der Dienst befindet sich derzeit in der Testphase und soll voraussichtlich 2027 eingeführt werden.

Südamerika

Südamerika ist eine Hochburg für Projekte zur digitalen Identifizierung, die vor allem durch die Unterstützung von Initiativen der Weltbank vorangetrieben werden. Die Mercosur-Region ist eine der ersten weltweit, die den Einsatz interoperabler digitaler Ausweise erprobt.

Uruguay

- Regionales Modell – Uruguay und Brasilien betreiben das erste grenzüberschreitende digitale ID-System des Kontinents, wodurch ein einziger Ausweis in mehreren Ländern akzeptiert wird. Die Initiative ist Teil der von den Vereinten Nationen unterstützten „50-in-5“-Initiative (finanziert von der Gates Foundation), die 50 Nationen dazu verpflichtet, innerhalb von fünf Jahren einen Teil der Identifikationsinfrastruktur zu verbessern.
- ID Uruguay – der erste Digital-ID-Broker,
  gestartet im Jahr 2018
  - Fungiert als „Broker“, der Informationen von mehreren Identitätsanbietern abrufen kann, um Single-Sign-On (SSO) in der gesamten Region bereitzustellen
    - eigene Plattform
    - regionale Technologieunternehmen (z. B. Abitab, TuID Antel)
    - Brasiliens GOV.br

    Drei verschiedene Vertrauensstufen, wobei höhere Stufen eine Videoüberprüfung oder Fingerabdrücke erfordern
- Uruguay – 85 % der Erwachsenen besitzen einen physischen Ausweis; etwa 1,6 Millionen Bürger sind bei ID Uruguay registriert (Nutzungsintensität unklar).

Brasilien

- Brasilien ist Südamerikas erstes vollständiges Programm
  - Das GOV.br Digital Wallet wurde 2022 eingeführt und ermöglicht es jedem, einen nationalen Personalausweis in einen digitalen Ausweis umzuwandeln.
  - Etwa 153 Millionen Nutzer (ca. 72 % der Bevölkerung) nutzen die App mittlerweile, die auch als Reisedokument innerhalb des Mercosur (Argentinien, Bolivien, Chile, Ecuador, Paraguay, Peru) dient.
  - Für die Registrierung sind die nationale Ausweisnummer sowie eine biometrische Überprüfung per Selfie erforderlich
- Brasiliens digitale ID wird auf der **b-Cadastros-Blockchain** gespeichert
  Neben der digitalen ID synchronisiert b-Cadastros sechs staatliche Register (Steuerzahler, juristische Personen, Bauwesen, Wirtschaftstätigkeit, Steuern, Schulden) und wird täglich aktualisiert.
    - Das Land führt zudem ein CBDC-

Pilotprojekt durch. Andere Länder

- In Betrieb: Argentinien, Chile, Kolumbien, Guyana, Peru (obligatorisch), Venezuela.
- Bestätigt (Gesetzgebung verabschiedet, Entwicklung im Gange): Paraguay, Ecuador.
- Frühphase: Bolivien (Biometrie für Sozialprogramme, noch keine nationale ID).
- Keine Umsetzung: Suriname.

Angetrieben von ID4D, 50-in-5 und der Mercosur-Integration bewegen sich die meisten südamerikanischen Staaten auf interoperable, digital orientierte Identitätsrahmenwerke zu. Eine weitreichende regionale Kompatibilität ist bis 2030 realistisch.

Afrika

Afrika zeichnet sich durch seine Bemühungen aus, eine weitgehend undokumentierte Bevölkerung zu registrieren, finanziert durch Milliarden an Darlehen und Zuschüssen der Weltbank. Aufgrund des Mangels an Mobiltelefonen im Land haben sich die meisten Länder für elektronische Ausweise entschieden. Diese elektronischen Ausweise sind zwar technisch gesehen keine digitalen Ausweise, legen aber den Grundstein dafür.

ECOWAS, Wirtschaftsgemeinschaft westafrikanischer Staaten

Diese Gruppe von 12 Ländern startete 2022 eine gemeinsame Initiative für nationale biometrische Ausweise, die in allen Mitgliedsländern interoperabel sein soll. Die digitale Initiative WURI wird mit 395 Millionen US-Dollar von der Weltbank finanziert.

Ghana

Die Ghana Card ist eine ECOWAS-Karte, ein physischer Ausweis mit elektronischen Funktionen, der durch Gesichts- und Fingerabdruckdaten gesichert ist. Sie ist für Bankgeschäfte, die Gewerbeanmeldung und das Autofahren im Land erforderlich. Derzeit wird sie finanziell integriert und wird von 18 Millionen Ghanaern genutzt.

Nigeria

Nigeria baut ein elektronisches Ausweissystem auf, die National Identification Number (NIN), die die rechtliche Identität mit Fingerabdrücken und Gesichtsdaten verknüpft. 121 Millionen Nigerianer haben sich bereits registriert, weitere 60 Millionen Registrierungen sind erforderlich, um das Ziel der Weltbank von insgesamt 180 Millionen Registrierungen zu erreichen. Die NIN ist für SIM-Karten, Reisepässe und Bankgeschäfte erforderlich.

Andere Länder

Marokko und Ruanda verfügen über ähnliche biometrische Ausweisprogramme und haben diese Karte für Personen ab 16 Jahren zur Pflicht gemacht. Tansania gibt Smartcards aus, die für verschiedene Anwendungen genutzt werden können, und arbeitet an einem Pilotprojekt zur Erfassung biometrischer Daten von Säuglingen.

Zu den weiteren Ländern mit funktionierenden biometrischen Ausweisen gehören Nigeria, Tansania, Uganda, Kenia, Malawi und Äthiopien.

Zu den Ländern mit bestätigten biometrischen Ausweisprogrammen gehören Südafrika, Senegal, Somalia und Mauretanien.

12 weitere Länder befinden sich in der Anfangsphase ihrer biometrischen und elektronischen Ausweisprogramme.

Es gibt jedoch 15 Länder in Nord-, Ost- und Zentralafrika, über die nur begrenzte oder gar keine Informationen zu einem digitalen Ausweissystem vorliegen.

Afrika, Heimat von Entwicklungsländern mit gravierenden Problemen in der Wasser- und Nahrungsmittelinfrastruktur, hat keine Zeit verloren, digitale Ausweisprogramme einzuführen, insbesondere der westafrikanische Block.

Erkenntnisse aus der globalen Analyse

Ein Blick auf die einzelnen Regionen deckte Teile des Puzzles auf: gesetzgeberische Maßnahmen, neue Anforderungen, technische Umsetzung und Missbrauch des Systems.

In diesem Abschnitt diskutieren wir wiederkehrende Muster und wichtige Phänomene im Zusammenhang mit der digitalen Identifikation

Biometrie für Reisen

Die bislang größte internationale Initiative zur Erfassung biometrischer Daten von Reisenden ist das Einreise-/Ausreisesystem (EES) der EU, das am 12. Oktober 2025 in Kraft trat.

Dieses neue System ersetzt den Grenzbeamten, der den Reisepass abstempelt, durch eine biometrische Reisekontrollstelle. An dieser Kontrollstelle scannt die Person ihren Reisepass, und eine Kamera richtet sich auf ihren Kopf aus, um einen Gesichtsabdruck aufzunehmen.

Diese Kontrollpunkte finden Sie an großen Flughäfen und Grenzübergängen in 29 Ländern, darunter die 25 EU-Mitgliedstaaten sowie vier Nicht-Mitgliedstaaten: Island, Norwegen, die Schweiz und Liechtenstein.

Zu den EU-Mitgliedstaaten, die diese Anforderungen nicht erfüllen, sind Zypern und die Republ isoliert sind.

Das Programm wird schrittweise über einen Zeitraum von 6 Monaten eingeführt und soll im April 2026 vollständig umgesetzt sein. Während dieser Zeit ist es möglich, dass einige Flughäfen und Kontrollstellen weiterhin mit traditionellen Grenzbeamten und Passstempeln arbeiten, wobei es sich dabei jedoch wahrscheinlich nicht um große Flughäfen handeln wird.

Neben den EU-Staaten verlangen viele andere Länder Gesichtsscans und Fingerabdrücke, darunter die Vereinigten Staaten, Japan, China, Südkorea, Singapur, Indien, Argentinien, Kenia, Russland, Kuwait, Saudi-Arabien, die Vereinigten Arabischen Emirate und Australien.

Big Tech & die digitale **Fragmentierung**

Der EU-Rahmen für digitale Identitäts-Wallets (EUDI) bildet die Software-Grundlage für die kommenden digitalen ID-Wallets in jedem EU-Mitgliedstaat. In der Projektdokumentation werden Entwickler dazu ermutigt, die Google Play Integrity API und Apple App Attestation zu nutzen. Dabei handelt es sich um Dienste, die sicherstellen, dass ein Smartphone als echt zertifiziert ist. Große Anbieter können diese Prüfungen bestehen, alternative Betriebssysteme hingegen nicht.

Dies wird als Sicherheitsmaßnahme dargestellt, obwohl Hunderte von Entwicklern wissen, dass diese Dienste (Play Integrity) nicht einmal prüfen, ob ein Smartphone noch Sicherheitsupdates erhält.

Praktisch bedeutet dies, dass nur Smartphones großer Technologiekonzerne Digital ID nutzen können, während alle „Degoogled“-Smartphones oder alternative Geräte die Wallets nicht nutzen können.

Trotz einer fast einstimmigen ablehnenden Reaktion hielten die EUDI-Entwickler an der Anforderung fest.

Der EU-Digitalmarktgesetz verlangt Wettbewerb auf App-Marktplätzen, und diese Anforderung würde Nutzer zwingen, offizielle App-Stores der großen Tech-Konzerne zu nutzen, was illegal wäre.

Wir gehen davon aus, dass weitere Digital-ID-Wallets diesem Trend folgen werden, und in Kombination mit Googles neuem Verbot alternativer Apps (die nicht aus offiziellen App-Stores heruntergeladen wurden) werden wir eine **digitale Spaltung** erleben**.**

Die Bevölkerung wird sich in zwei Hälften spalten: eine privilegierte Hälfte, die Banking-Apps und digitale IDs nutzen kann, und die Randgruppe, die auf Open-Source-Alternativen zurückgreift.

Jetzt ist es an der Zeit, sich der marginalisierten Hälfte anzuschließen – sie wird weiterhin eine anständige Erfahrung machen. Erstens haben sie einen triftigen Grund, digitale IDs zu meiden.

Zweitens ist es einfach genug, Bankgeschäfte über den Webbrowser des Handys oder den Laptop zu erledigen.

Dank ihrer zahlenmäßigen Stärke kann die benachteiligte Hälfte alternative Entwickler unterstützen und ein gutes mobiles Erlebnis genießen, während sie frei von digitalen IDs bleibt und ihre Privatsphäre wahrt.

Die privilegierte Hälfte wird digitale IDs erhalten.

Compliance-Hühnchen

Behörden müssen bei der Umstellung der Nutzer auf eine neue Form der Identifikation, sei es neue physische Karten oder eine digitale ID-Brieftasche, ein heikles Spiel spielen.

Wenn beispielsweise eine digitale ID für Flüge erforderlich ist und eine große Mehrheit der Vielflieger sich nicht daran hält, könnte die Luftfahrtindustrie zusammenbrechen und die Wirtschaft erheblich beeinträchtigt werden.

Um den Prozess reibungsloser zu gestalten, wird das „Compliance-Chicken“-Spiel eingesetzt. Es wird eine Frist für die Einhaltung einer Anordnung gesetzt; wer diese Frist verpasst, muss mit Einschränkungen seiner Freiheiten rechnen.

Der REAL ID Act in den USA verlangte, dass staatliche Ausweise den neuesten Sicherheitsstandards entsprechen.

Die ursprüngliche Frist wurde 2008 festgelegt und nach Widerstand auf staatlicher Ebene sowie im Zuge der COVID-Pandemie dreimal verlängert. Die endgültige Frist wurde auf Mai 2025 festgelegt.

Diese 20-jährige Geschichte ist ein perfektes Beispiel für das „Compliance-Chicken“. Einschränkungen können nur dann erfolgen, wenn keine erheblichen Auswirkungen auf die betroffene Branche zu erwarten sind. Wer sich dagegen wehren will, muss es versuchen, Alternativen finden und andere darüber informieren.

Zahlungs-Apps & CBDCs

Bank- und Finanz-Apps gehören zu den ersten, die in digitale ID-Programme integriert werden, angesichts ihres Sicherheitskontexts und der Ausrichtung der Weltbank auf digitale ID.

Überraschenderweise liegt Indien mit seinem Unified Payments System (UPI) an erster Stelle – dem größten Zahlungssystem, das sofortige Zahlungen von Person zu Person und von Person zu Händler ermöglicht und 50 % des weltweiten digitalen Transaktionsvolumens abwickelt.

Die meisten Banken und Finanzdienstleister in Indien nutzen UPI, ebenso wie große Technologieanbieter wie Google Play. Im Durchschnitt verarbeitet UPI 7.500 Transaktionen pro Sekunde.

Im Oktober 2025 wurde Indiens UPI mit der digitalen ID von Aadhaar integriert, um Zahlungen zu authentifizieren. Jede Zahlung kann anhand der in Aadhaar gespeicherten biometrischen Daten verifiziert werden.

China folgt dicht dahinter mit seinem großen Tech-Oligopol zwischen WeChat Pay und AliPay, die fast alle Zahlungen im Land abwickeln und Bargeld damit praktisch überflüssig machen. China ist dabei, WeChat- und AliPay-Konten mit der nationalen Cyberspace-ID zu verknüpfen, wodurch eine Integration der digitalen ID erreicht würde.

In der EU ist Dänemark führend mit der Integration von MitID in Banken und das nationale Debitkartensystem Dankort – das überall genutzt und akzeptiert wird. Apps wie MobilePay, die mit MitID integriert sind, sind weit verbreitet.

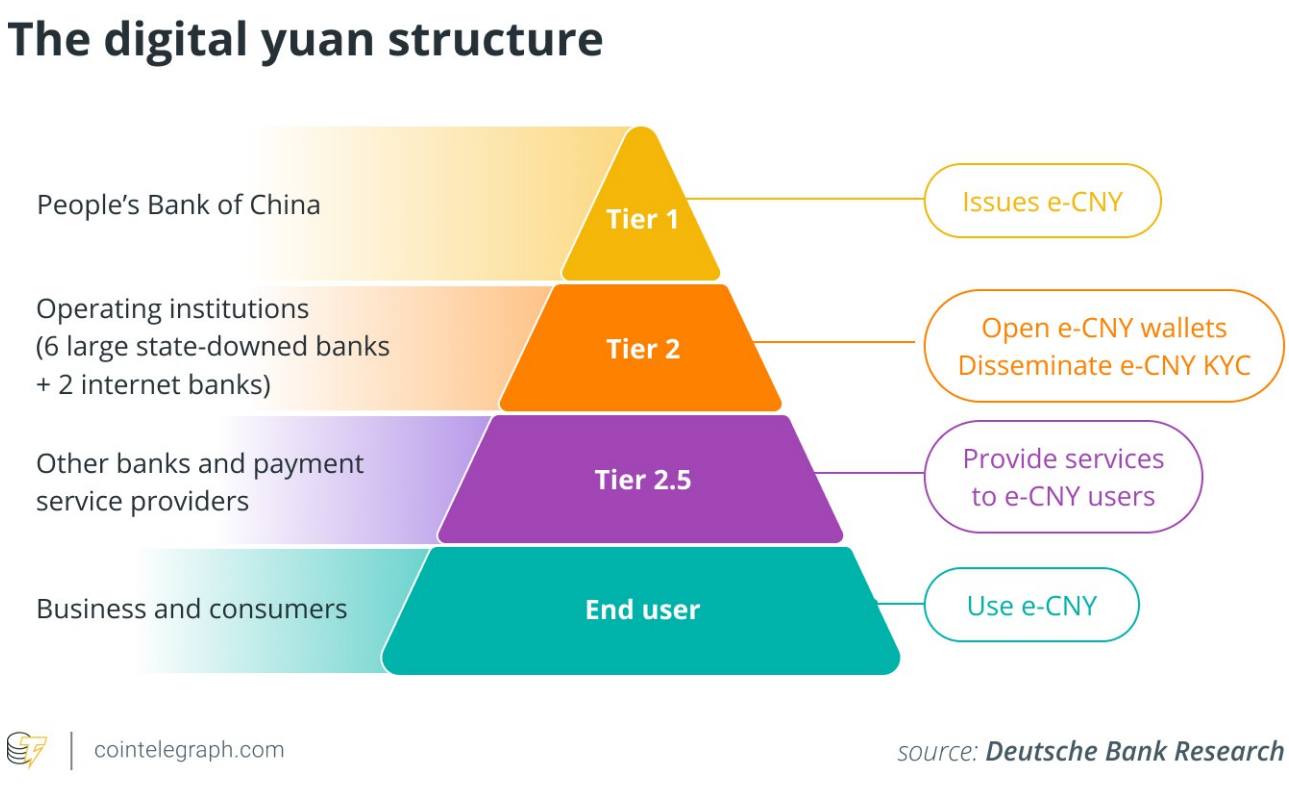
Andere EU-Staaten und Länder mit funktionierenden digitalen ID-Programmen werden digitale ID-integrierte Zahlungs-Apps einführen, sobald die Programme für private Unternehmen verfügbar sind; 2026 für Australien und 2027 für die EU.

CBDCs

CBDCs sind grundlegend mit digitalen IDs verknüpft, sie können ohne die Verknüpfung mit der Identität einer Person nicht funktionieren und sind zwei der drei Komponenten der digitalen öffentlichen Infrastruktur.

Laut dem Atlantic Council prüfen 137 Länder CBDC-Projekte, obwohl nur eine Handvoll Länder bereits Projekte gestartet oder öffentliche Pilotprojekte durchgeführt haben. Der CBDC-Tracker des Atlantic Council visualisiert den Status von Projekten weltweit.

Zwei bemerkenswerte Pilotprojekte, die weit verbreitet sind, sind Chinas digitaler Yuan (e-CNY) und Indiens e-Rupie, das erste und das zweitgrößte Pilotprojekt.



Diese CBDCs sind im Verhältnis 1:1 an ihre jeweilige Landeswährung gekoppelt und fungieren nach ihrer Genehmigung als gesetzliches Zahlungsmittel. Sie sind keine Kryptowährungen und haben keine marktbestimmten Preise – sie sind digitale Versionen bestehender Währungen.

CBDCs werden von der Zentralbank des Landes ausgegeben und anschließend über zugelassene Banken verteilt. Verbraucher können eine nationale CBDC-App oder eine zugelassene Bank- oder Finanzdienstleistungs-App herunterladen. Dort führen sie die Verifizierung durch und wählen eine Methode zum Aufladen ihrer CBDC (Banküberweisung, Debitkarte).

CBDCs haben in der Regel tägliche Ausgaben- und Transaktionslimits. Chinas E-Yuan hat je nach Verifizierungsgrad unterschiedliche Limits, da „anonyme“ Konten bereits mit einer Telefonnummer erstellt werden können.

Trotz dieser ambitionierten Pilotprojekte sind CBDCs noch nicht weit verbreitet. Der chinesische E-Yuan macht 0,13 % des gesamten Geldumlaufs aus, und die indische E-Rupie macht weniger als 1 % der gesamten digitalen Transaktionen in Indien aus.

Diese Programme befinden sich noch in einem frühen Stadium, und Pilotprojekte in anderen Ländern wurden unter Verweis auf Datenschutzprobleme verzögert.

CBDCs als digitale Zahlungsmittel sind die zweite Säule der **digitalen öffentlichen Infrastruktur** und können problemlos auf der digitalen ID aufbauen**,** sobald eine ausreichende Akzeptanz erreicht ist.

Soziale Medien

Länder mit Gesetzen zur Altersüberprüfung tendieren naturgemäß zur Nutzung digitaler Identitäten.

Australiens Online Safety Act verpflichtet alle sozialen Netzwerke, das Alter ihrer Nutzer zu überprüfen. Die digitale Identität wurde in einer Ausschusssitzung als Lösung für die Altersüberprüfung (2.76) vorgeschlagen und ist als optionale Wahl vorgesehen. Alternativ könnten Nutzer die Altersüberprüfung über die Plattformen selbst durchführen.

Der britische Online Safety Act trat im Juli 2025 in Kraft und schreibt Altersüberprüfungen für schädliche Inhalte vor, und die Hälfte aller US-Bundesstaaten hat Gesetze verabschiedet, die Altersüberprüfungen für den Zugriff auf Pornografie vorschreiben.

Diese Verfahren zur Altersüberprüfung entsprechen fast der Registrierung für eine digitale ID; die durch eine digitale ID gestützte Altersüberprüfung ist der logische nächste Schritt, um den technischen und administrativen Aufwand dieser Programme zu reduzieren.

Menschenrechtsverletzungen

Sobald die Schlüsselkomponenten der digitalen öffentlichen Infrastruktur – digitale Identität, digitale Zahlungen und Datenaustausch – festgelegt sind, öffnet dies die Tür zu Menschenrechtsverletzungen in einem bisher nie dagewesenen Ausmaß.

Chinas 2014 angekündigtes Sozialkreditsystem (SCS) bewertet chinesische Bürger, Unternehmen, Organisationen und staatliche Stellen anhand rechtlicher, moralischer und beruflicher Standards.

Es sammelt Daten aus Online-Einkäufen, Äußerungen und Interaktionen mit Behörden und durchsucht generell das Internet, um chinesische Bürger zu identifizieren und auf schwarze Listen zu setzen.

Die schwarze Liste des Obersten Gerichtshofs mit „diskreditierten“ oder „unwürdigen“ Personen ist online einsehbar – und kann von staatlichen oder privaten Stellen öffentlich durchsucht werden.

Verleumdungsklagen sind in China weit verbreitet, und wenn der Verlierer das Gericht nicht von einer aufrichtigen Entschuldigung überzeugen oder seine Geldstrafen nicht rechtzeitig bezahlen kann, wird er auf die Liste gesetzt.
Zu den weiteren Vergehen zählen die Nichtzahlung von Steuern und Geldstrafen sowie Drogenkonsum.

Personen auf der schwarzen Liste dürfen keine Flugzeuge oder Züge besteigen und sind von größeren Anschaffungen ausgeschlossen – einschließlich des Besuchs einer Privatschule für ihre Kinder.

Im Jahr 2018 sperrte das SCS 17,5 Millionen Flugbuchungen und 5,5 Millionen Zugtickets.

Es hat sich zudem gezeigt, dass China seine COVID-Kontrollinfrastruktur nutzt, um Proteste zu unterbinden: Im Jahr 2022 wurden die Gesundheitspässe von Bankprotestierenden „rot“, was sie daran hinderte, am Tag des Protests zu reisen.

Weiter nördlich nutzt Russland digitale Ausweise zur militärischen und sozialen Kontrolle. In Moskau gibt es über 220.000 Überwachungskameras, das sind etwa 16 Kameras pro 1.000 Einwohner. Nun scannen diese Kameras Gesichter, um diejenigen aufzuspüren, die sich der Einberufung entziehen, so Moskaus Militärkommissar, Oberst Maxim Loktev.

Gestützt auf biometrische Gesichtsdaten können diese Kameras nun dazu genutzt werden, Gesetzesbrecher und Dissidenten aufzuspüren. Die Wissenschaftsjournalistin Asya Kazantseva wurde am Tag Russlands (22. September 2022) zusammen mit anderen Aktivisten von der Moskauer Polizei mithilfe des Gesichtserkennungssystems der Moskauer U-Bahn festgenommen.

In den Städten Pakistans hat die Verknüpfung der nationalen Registrierungsnummer NADRA mit Mobilfunkdiensten und Bankkonten zu politischer Unterdrückung geführt.

Im Jahr 2022 warnte der Innenminister Anhänger der vorherigen Regierung, dass ihre biometrischen Ausweise gesperrt werden könnten, wodurch ihnen der Zugang zu Bankkonten verwehrt würde.

Diese Verbote gehen über den Einzelnen hinaus; einem YouTuber, der der pakistanischen Regierung kritisch gegenüberstand, wurde sein Bankkonto eingefroren, ebenso wie das seiner gesamten Familie – und aller Personen, mit denen er Kontakt hatte, einschließlich eines Papageienverkäufers.

Diese abschreckenden Anwendungen einer einheitlichen digitalen öffentlichen Infrastruktur deuten darauf hin, was den Bevölkerungsgruppen, die sich daran halten, bevorstehen könnte.

Lösungen

Das Problem der digitalen ID ist universell und wird nicht verschwinden. Wer gegen das Programm ist, muss sich gegen die vielen Schritte wehren, die dorthin führen, nämlich elektronische Ausweise und die Erfassung biometrischer Daten. Möglicherweise müssen sie auch auf den Zugang zu Waren und Dienstleistungen verzichten, wenn diese hinter einer Barriere versteckt werden.

> @ Dies ist keine rechtliche oder finanzielle Beratung; diese Informationen dienen ausschließlich zu Bildungszwecken.

Allgemeine Lösungen

Vorbereitung

Vorbereitung ist die beste Strategie; stellen Sie sicher, dass Sie sich mit Nahrungsmitteln, Tauschgeschäften und Gemeinschaftssystemen versorgen, die nicht auf digitale Systeme angewiesen sind. Mögliche Aktivitäten sind:

- Üben von Bargeld- oder Tauschgeschäften unter Gleichgesinnten
- Aufbau informeller Kreditkreise.
- Stärken Sie die Beziehungen zu vertrauenswürdigen Vermittlern, die Ihnen bei Finanztransaktionen helfen können, oder auch zu Teilnehmern des Digital-ID-Programms, die bereit sind, Sie später zu unterstützen

Wählen Sie immer die Abmeldung

Das scheint offensichtlich, hängt aber vom Kontext ab. Ein Opt-out kann wie folgt aussehen:

- Ablehnung der biometrischen Erfassung
- Das Versäumen, ein Telefon oder ein kompatibles Telefon mitzubringen
- Sprechen Sie mit einem Vorgesetzten
- Vermeidung von Büros mit biometrischer und digitaler ID-Infrastruktur und Suche nach ländlichen Büros

Sozialer Widerstand

Je mehr deiner Freunde und Nachbarn sich dem digitalen ID-System entziehen, desto besser – also verbreite die Nachricht. Teile diesen Bericht und führe ernsthafte Gespräche über die Zukunft.

- Veranstalten Sie Gemeindediskussionen in Ihrer Stadt
- Hängen Sie Flyer und Aufkleber auf
- Sprechen Sie das Thema ganz natürlich an

Konkrete Lösungen

Technologie

Digitale IDs funktionieren möglicherweise nur auf gängigen Geräten gemäß den Rahmenbedingungen für digitale IDs, und dies weitet sich auf immer mehr Banking-Apps aus. Eine Möglichkeit, die Nutzung digitaler IDs vollständig zu vermeiden, ist die Verwendung eines Telefons, das diese nicht unterstützt. Verwenden Sie alternative, von Google unabhängige Betriebssysteme wie GrapheneOS oder LineageOS. Verwenden Sie Open-Source-Computer auf Linux-Basis.

> A Wenn dir diese Arbeit wichtig ist, unterstütze uns doch durch den Kauf eines Datenschutz-Smartphones oder -Laptops, das dich vor Digital ID schützen kann.
>
> Verwenden Sie den Aktionscode NOID4ME an der Kasse – 75 $ Rabatt auf jedes Smartphone oder jeden Laptop.
> **https://abovephone.com**

Bankwesen

Wenn Digital ID privaten Unternehmen zur Integration zur Verfügung steht, bleibt nur noch wenig Zeit, bevor auf gespeicherte Gelder nicht mehr zugegriffen werden kann. Zu den verantwortungsvollen Maßnahmen während dieses Prozesses können gehören:

- Behalten Sie die Bundes- und Landesgesetze Ihres Landes im Blick, um über Änderungen und Fristen informiert zu sein
- Erweitern Sie Ihre Suche nach Kreditgenossenschaften oder lokalen Banken, die möglicherweise Ausnahmeregelungen haben
- Probieren Sie Kryptowährungen aus und suchen Sie nach Sofortbörsen, Peer-to-Peer-Marktplätzen und dezentralen Börsen.
- Nehmen Sie den Dialog mit der Bank auf und üben Sie sozialen Druck aus, um biometrische Kontrollen abzuschaffen
- Eröffnen Sie ein Konto mit einer an Gold/Silber gebundenen Bankkarte: https://member.upma.org/#/auth/login
  - Beachten Sie, dass diese Bank bei Abhebungen per Banküberweisung eine eigene biometrische Verifizierung durchführt
- Nutzen Sie eine Neobank oder ein Fintech-Unternehmen, das unter einem anderen regulatorischen Rahmen agiert:
  - Wir haben unten einige Optionen aufgeführt, aber bitte beachten Sie, dass diese ihre eigenen Anforderungen an die Identitätsprüfung haben und die Nutzung dieser Dienste keine dauerhafte Lösung darstellt.
  - **Revolut** – https://www.revolut.com
    N26 – https://n26.com
    Wise (ehemals TransferWise) – https://wise.com

Reisen

Viele Länder haben biometrische Grenzkontrollen für Ausländer eingeführt. Es mag legale Möglichkeiten geben, die Grenze zu überqueren, ohne sich in das biometrische System einzutragen, jedoch ist dies eine zeitkritische Angelegenheit, da die Kontrollpunkte im Laufe der Zeit immer standardisierter werden. |

- Behalten Sie die Reisebestimmungen der für Sie wichtigen Länder im Blick

- Reisen Sie zunächst in ein Land ohne biometrisches Ein- und Ausreisesystem und suchen Sie sich von dort aus einen Weg
- Kleiner ist besser: Reisen Sie zu kleineren Flughäfen und Grenzübergängen
- Kaufen Sie Tickets persönlich, um eine digitale Vorabprüfung zu vermeiden

Fazit

Wir stehen vor einem Netzwerk digitaler Identitäten, das von Regierungen und Banken weltweit unterstützt wird. Privatpersonen und Unternehmen könnten zur Nutzung digitaler Identitäten gezwungen werden, da deren Verbreitung zunimmt und Alternativen versagen.

Die wichtigste Maßnahme, die man jetzt ergreifen kann, ist der Aufbau lokaler Gemeinschaften, die Sensibilisierung für diese Themen und die Sicherstellung, dass grundlegende Güter und Dienstleistungen nicht hinter einer digitalen ID-Barriere verschlossen bleiben.

Above wird seinen Teil zur Entwicklung, Verbreitung und Förderung von Lösungen beitragen, und wir freuen uns auf eine engere Zusammenarbeit zwischen lokalen und internationalen Gemeinschaften.

Wir sind dankbar für die Gelegenheit, dazu beizutragen, die Welt zum Besseren zu verändern.