FUTURAE

User-centric authentication and fraud prevention

www.futurae.com

Vertrauen in der digitalen Schweiz der Zukunft

Sandra Tobler, Gründerin, VRP Futurae,
Board DIDAS, Member Steering Committee NCS

Welche **Bausteine** braucht eine **erfolgreiche, resiliente, zukunftsfähige Schweiz?**

1. Digitale Vertrauensinfrastruktur – die eID

Eine Übersicht der Governance Modelle

Zentralisiert
Eine einzelne biometrische Datenbank und ein staatlich kontrolliertes Register für universelle Identifikation.

Bsp. *Indien: Aadhaar*
CIDR – Zentrales Register Biometrie
1,34 Milliarden registrierte Personen

→Zentralisiert: Hohe Kontrolle, einzelne Fehlerquelle

Föderiert
Dezentrale Datenbanken, die über eine sichere, interoperable Datenaus-tauschschicht verbunden sind.

Bsp. *Estland: X-Road*
X-Road Datenaustausch
ca. 52.000 angeschlossene Organisationen
99 % der Dienste online

→Föderiert: Verteilt, interoperabel

Datenschutzorientiert
Staatlich ausgestellte Identität mit nicht verknüpfbaren Transaktionen und minimaler Datenweitergabe.

Bsp. Schweiz: e-ID
Nicht verknüpfbare Nachweise
Schweizer Datenschutzstandards
Einführung im Dezember 2026

→ Datenschutzorientiert: Minimale Datenerhebung

Schweizer Modell

1. Schweiz – vom Staat, privacy-by-design

Zweck & Status

Überblick
Eine staatlich ausgestellte, freiwillige und kostenlose elektronische Identität. Konzipiert, um physische Ausweise für die Online-Identifikation zu ersetzen & maximalen Datenschutz zu gewährleisten.

Wichtige Meilensteine
28. Sept. 2025: Referendum von den Wählern angenommen (50,39 % Ja-Stimmen).
1. Dez. 2026: Geplanter Start

Governance & Aufsicht

Rechtsgrundlage: Bundesgesetz über elektronische Identifizierungsdienste (E-ID-Gesetz).
Betreiber: Das Bundesamt für Justiz überwacht die Politik. Das BIT betreibt die Vertrauensinfrastruktur.
Anbieterkontrollen: Öffentliches Register für Datenabfragen/-zwecke. Das BJ kann nicht konforme Anbieter verwarnen und ausschließen.

Teilnahme & Nutzbarkeit
Freiwillige Nutzung: Bürger entscheiden sich für die Teilnahme.
Frühe Anwendungsfälle: Elektronische Führerscheine, Altersverifikation im Verkauf

Sicherheit & Datenschutz

Nichtverknüpfbarkeit per Design: Mehrere einmalig verwendbare E-IDs pro Person (über die swiyu-Wallet ausgegeben), wodurch Tracking über Dienste hinweg verhindert wird.
Datenminimierung: Der Zugriff auf die AHV-Nummer ist strikt auf gesetzlich autorisierte Anbieter beschränkt.
Nutzerkontrolle: Die Wallet bietet aktive Benachrichtigungen, Warnungen und integrierte Mechanismen zur Meldung von Missbrauch.

Estnisches Modell

2. Estland – föderiert und interoperabel

Zweck & Status

Überblick
Ein föderierter, interoperabler digitaler Staat, der auf dem „Once-Only“-Prinzip basiert. X-Road ist eine dezentrale Datenaustauschschicht, die unabhängige öffentliche und private Datenbanken miteinander verbindet.

Hauptmerkmale
Interoperabel: Verbindet hunderte unterschiedliche IT-Systeme sicher.
Open Source: Technologie wird in anderen Ländern eingesetzt.
E-Residency: Vereinfachte Verwaltung, ganz digital.

Governance & Aufsicht

Zentrale Gesetzgebung: Das Gesetz über Identitätsdokumente & das Bevölkerungs-registergesetz bilden den grundlegenden Identitätsrahmen. **Datenschutz**: Geregelt durch die DSGVO sowie nationale Datenschutzgesetze.
Sektoraler Ansatz: Anstelle eines übergreifenden E-Government-Gesetzes regeln spezifische Fachgesetze die Nutzung von X-Road.

Nutzung & Ergebnisse
Über 99 % der öffentlichen Dienstleistungen online verfügbar. Verbindet rund 52.000 Organisationen. Nutzung in Steuerwesen, Gesundheitswesen und E-Voting.

Sicherheit & Datenschutz

Technische Schutzmaßnahmen: e2e Encryption und Integritätsprüfungen bei allen Datenaustauschen.

Transparenz: Umfassende Protokollierung ermöglicht es Bürgern, genau nachzuvollziehen, wer ihre Daten über staatliche Portale eingesehen hat.

Incident Response: Nachgewiesene Widerstandsfähigkeit während der Sicherheitslücke des ID-Chips 2017 durch massenhafte Fern-Erneuerung von Zertifikaten.

Indisches Modell

3. Indien – Scale, Biometrie, Adoption

Zweck & Status

Überblick
Eine zentrale, 12-stellige digitale ID für Einwohner Indiens, die demografische und biometrische Identifikation ermöglicht. Sie wird umfassend für KYC Identitätsprüfung und Direct Benefit Transfers (DBT) eingesetzt, um die Governance und Inklusion zu verbessern.

Wichtige Meilensteine
2010: Erste Aadhaar-Nummer generiert.
2016: Aadhaar-Gesetz verabschiedet, UIDAI wird zur gesetzlichen Behörde.
2018: Das Oberste Gericht bestätigt die Gültigkeit mit Einschränkungen für die private Nutzung.

Governance & Aufsicht

Rechtliche Grundlage: Aadhaar-Gesetz (Gezielte Bereitstellung von finanziellen und anderen Subventionen, Leistungen und Diensten), 2016.
Behörde: Die UIDAI verwaltet Registrierung, Identifikation und Policies.
Gerichtliche Überprüfung: Das Urteil des Obersten Gerichtshofs von 2018 begrenzte die obligatorische Nutzung durch den Privatsektor, hielt aber die Verfassungsmäßigkeit für staatliche Subventionen aufrecht.

Skalierung
Reichweite ca.1,34 Mrd. aktive AadhaarInhaber, durchschnittlich 96 Mio. Transaktionen pro Tag
Methoden: OTP, Fingerabdruck, Iris und Gesichtserkennung

Sicherheitskontrollen

Datenschutz: Encryption at rest/in transit; strikte Datenlokalisierung innerhalb Indiens.
Biometrische Aufbewahrung: Für AUAs (Behörden, die nutzen) verboten. Nur die UIDAI hält zentrale biometrische Daten.
Audit-Rahmen: Dreistufiges Prüfungssystem (Selbstverpflichtung, jährliches Audit, GRCP) für Parteien des Ökosystems.

Unsere eigene Erfolgsformel

1. Vertrauen durch Zusammenarbeit, Datenschutz und Kontrolle

In der Schweiz ist das Vertrauen in den Staat hoch – aber beim Thema digitale Identität auch sensibel. Erfolgreich wird die eID nur, wenn klar ist, dass Daten unter Kontrolle der Bürger bleiben und Transparenz herrscht, wer wann welche Daten nutzt. Partizipationsmeetings und Zusammenarbeit durch Transparenz sind Vorzeigemodelle für Behörden (i.e. Github).

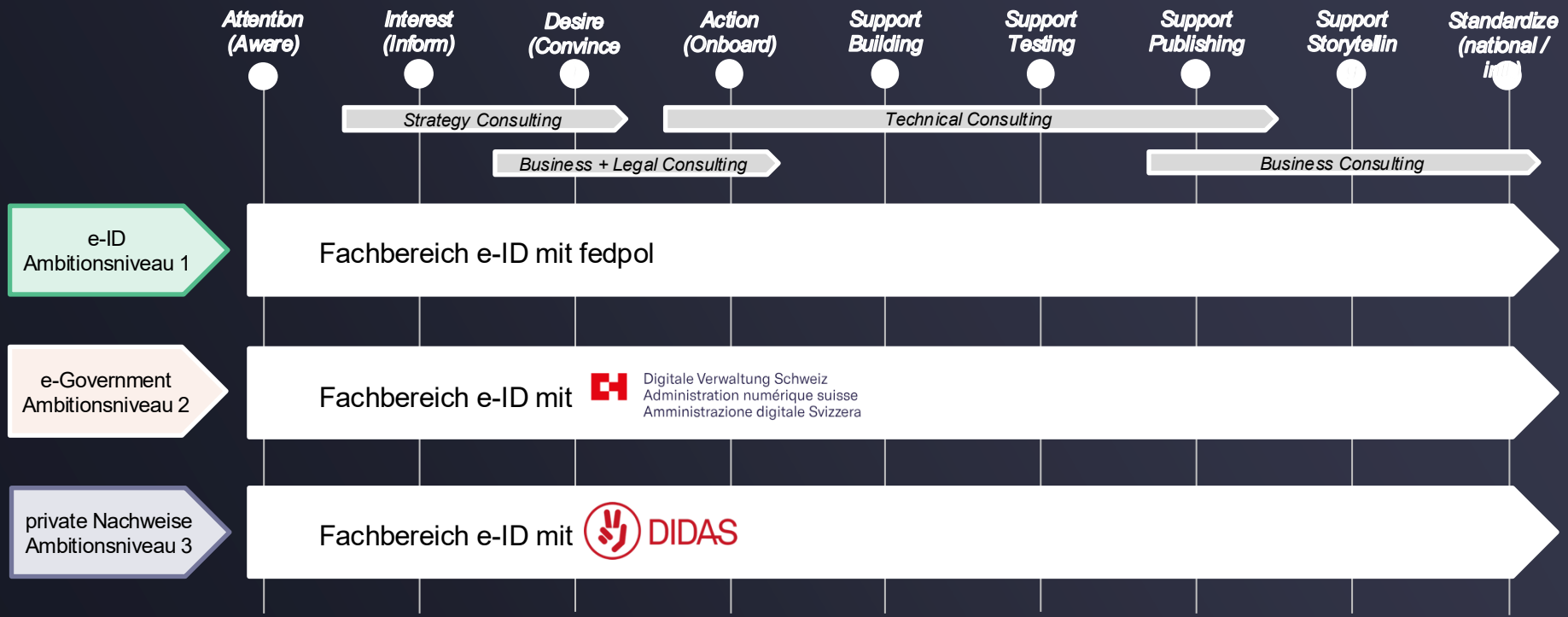
2. Konkreter Nutzen im Alltag

Die eID muss Dienste spürbar einfacher machen inkl. verbesserte Inklusion bei Behördengängen , vereinfachte Altersüberprüfung beim Einkauf etc.

3. Breite Akzeptanz durch Kooperation

Die eID darf kein reines föderales Projekt sein. Erfolgreich wird sie, wenn Kantone und Gemeinden einheitlich mitziehen und mit der Privatwirtschaft ein funktionierendes Ökosystem aufbauen, anstatt Insellösungen entstehen.

DVS und DIDAS sind swiyu Orchestrator



2. Open Source
der Goldstandard für Transparenz und digitale Souveränität

JA, aber…

1 Nicht bei hochspezialisierter Fachsoftware
Bei spezifischen Anwendungen, wo es kein ausgereiftes Open-Source-Projekt gibt.

2. Nicht wo besonders hohe Sicherheitsanforderungen erforderlich sind
Der offene Quellcode kann ein Risiko darstellen. Wenn eine Schwachstelle im Code entdeckt wird, ist sie sofort für alle (auch für staatliche Angreifer) sichtbar. Ebenso in Bereichen, in denen Patches nicht sofort überall eingespielt werden.

3. Nicht wo fehlende Support-Strukturen und Haftung besonders heikel sind
Da es keine garantierten Service-Level-Agreements (SLAs) bei reinen Community-Projekten gibt, sind sie für kritische Infrastrukturprojekte ein zu hohes Risiko.

4. Nicht bei "Legacy"-Abhängigkeiten
Da wo veraltete Infrastruktur die Komplexität erhöht. Eine neue Open-Source-Lösung müsste mit proprietären Datenbanken kommunizieren, die keine offenen Schnittstellen haben. Dies kann zu instabilen Bastellösungen führen, die teurer sind als Alternativen.

5. Nicht bei kurzfristigen Projekten ohne "Exit-Strategie"
Open Source spielt seine Stärken über lange Zeiträume aus (keine Lizenzgebühren, Anpassbarkeit).
Bei kurzfristigen Pilotprojekten oder Ad-hoc-Lösungen ist der Aufwand für die Einrichtung einer Open-Source-Infrastruktur (Server, Know-how-Aufbau) oft größer als einfach eine Cloud-Software (SaaS) zu lizenzieren.

3. Zusammenarbeit mit lokalen Startups

“Zu viel Risiko, die sind ja nicht mehr da in einigen Jahren!”

Die allgemeine **5-Jahres-Überlebensrate** aller ETH Spin-offs liegt bei **93 %.***

*Letzte Daten aus dem ETH Transfer Office

Vorteile mit lokalen Startups zusammenzuspannen

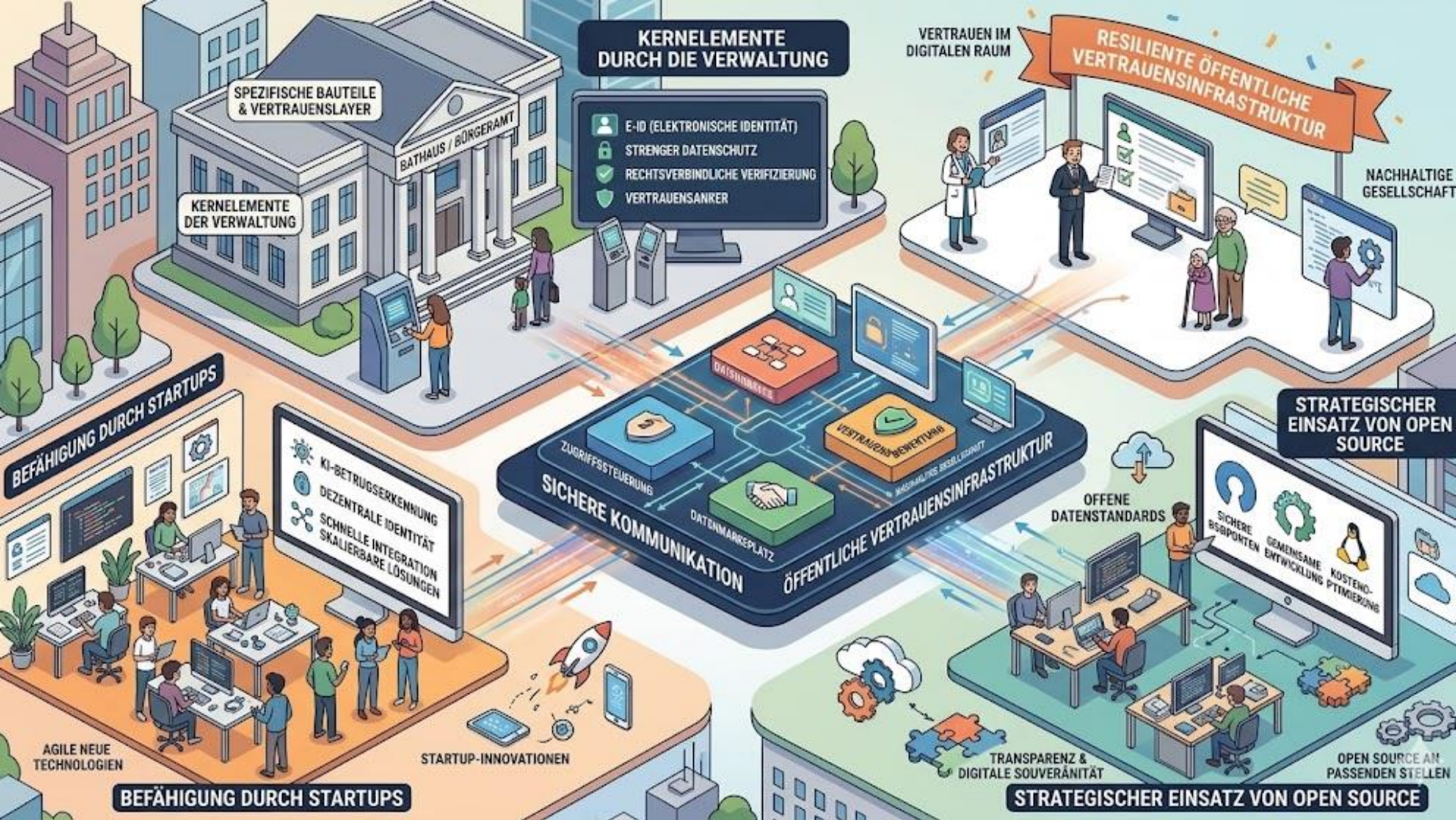
1. Wirtschaftliche Effizienz und Innovation
Startups können schnell MVPs liefern, die spezifische Probleme lösen und auch helfen einen Kulturwandel herbeiführen. Die Einbindung lokaler Player bricht die Abhängigkeit von großen Anbietern (Vendor Lock-in). Dies sorgt für wettbewerbsfähige Preise und innovativere Lösungen. Die Verwaltung als Referenzkunden helfen dem Startup international zu skalieren und **Steuereinnahmen in der Schweiz zu generieren.**

2. Stärkung des lokalen Ökosystems: Aufträge der öffentlichen Hand sind für Startups oft wertvoller als Risikokapital. Dies schafft hochqualifizierte Arbeitsplätze vor Ort und bindet Talente in der Schweiz.

3. Digitale Souveränität: Durch die Zusammenarbeit mit lokalen Innovatoren behält die Verwaltung die Kontrolle über ihre Daten und Infrastruktur. Man ist weniger abhängig von globalen Playern.

4. Attraktivität als Arbeitgeber: Eine moderne, technologisch aufgeschlossene Verwaltung ist für junge Fachkräfte attraktiver als eine, die an veralteten Systemen festhält.

Swiss Cybersecurity Startup Map (https://cysecmap.swiss/


KERNELEMENTE DURCH DIE VERWALTUNG
E-ID (ELEKTRONISCHE IDENTITÄT)
STRENGER DATENSCHUTZ
RECHTSVERBINDLICHE VERIFIZIERUNG
VERTRAUENSANKER
SPEZIFISCHE BAUTEILE & VERTRAUENSLAYER
RATHAUS / BÜRGERAMT
KERNELEMENTE DER VERWALTUNG
VERTRAUEN IM DIGITALEN RAUM
RESILIENTE ÖFFENTLICHE VERTRAUENSINFRASTRUKTUR
NACHHALTIGE GESELLSCHAFT
BEFÄHIGUNG DURCH STARTUPS
KI-BETRUGSERKENNUNG
DEZENTRALE IDENTITÄT
SCHNELLE INTEGRATION
SKALIERBARE LÖSUNGEN
AGILE NEUE TECHNOLOGIEN
STARTUP-INNOVATIONEN
BEFÄHIGUNG DURCH STARTUPS
DATENHUB
ZUGRIFFSSTEUERUNG
VERTRAUENSBEWERTUNG
DATENMARKTPLATZ
SICHERE KOMMUNIKATION
ÖFFENTLICHE VERTRAUENSINFRASTRUKTUR
STRATEGISCHER EINSATZ VON OPEN SOURCE
OFFENE DATENSTANDARDS
SICHERE BSIBIONTEN
GEMEINSAME ENTWICKLUNG
KOSTENO-PTIMIERUNG
TRANSPARENZ & DIGITALE SOUVERÄNITÄT
OPEN SOURCE AN PASSENDEN STELLEN
STRATEGISCHER EINSATZ VON OPEN SOURCE

FUTURAE

User-centric authentication and fraud prevention

Vielen Dank

www.futurae.com

futurae-technologies-ag

@_futurae

@FuturaeTech

Disclaimer

The recipients of this document understand and agree that the information included therein is confidential. Each recipient thus undertakes to keep the information secret and not to make it publicly available, directly and indirectly, nor to distribute it without prior written agreement of Futurae Technologies AG.
Futurae Technologies AG and its employees do not accept any responsibility or liability for the accuracy, content, completeness, legality, or reliability of the information contained herein.