SGMI SSIM SSMI

Schweizerische Gesellschaft für Medizinische Informatik
Société Suisse d'Informatique Médicale
Società Svizzera d'Informatica Medica
Swiss Society for Medical Informatics

eMpfEhlung-RecommaNdaTion-RaccomandaziOne-Recommendation

Die Schweizerische Gesellschaft für Medizinische Informatik publiziert zu aktuellen Themen Empfehlungen für Ihre Mitglieder und die Öffentlichkeit

La Société suisse d'informatique médicale publie des recommandations sur des sujets d'actualité à l'intention de ses membres et du public

Elektronische Identifikation (e-ID)

Identité électronique (e-ID)

La Società Svizzera d'Informatica Medica pubblica raccomandazioni su temi di attualità per i suoi membri e per il pubblico

The Swiss Society for Medical Informatics publishes recommendations on current topics for its members and the public

September 2025

SGMI-MENTOR – Elektronische Identifikation (e-ID)

Einführung

Hintergrund

Die eindeutige und fälschungssichere Identifikation seiner Bürger gehört seit Urzeiten zu einer Kernaufgabe eines Staats. Auch seit jeher ist damit ein grosses Potential für Machtmissbrauch, Unterdrückung und Überwachung vergesellschaftet. Durch die Errungenschaft der modernen Demokratie wurden Gesetze und Regulierungen erschaffen, welche diese Risiken verkleinern und den Schutz des Individuums stärken.

Trotz zunehmender Digitalisierung des Alltags ist dieser grundlegende Prozess der Identifikation aber bisher in der Schweiz mehrheitlich analog geblieben. Technologisch wurden verschiedene Varianten der rechtsgültigen digitalen Identifikation ausprobiert, welche sich aber alle bisher nicht durchzusetzen vermochten.

Die Schweiz ist eines der wenigen europäischen Länder, welches noch keine staatliche elektronische Identifikation anbietet.

Ausgangslage

Den Bedarf einer zuverlässigen elektronischen Identifikation hat auch die Schweizer Eidgenossenschaft erkannt und dem Volk im Jahr 2021 eine erste Vorlage zur Abstimmung vorgelegt. Diese wurde mit 64.4% Nein-Stimmen klar abgelehnt. Im Nachgang hat sich herausgestellt, dass die Stimmenden nicht «Nein» zur elektronischen Identifikation gesagt haben, sondern zur Art und Weise, wie diese damals angedacht war (Herausgabe über private Anbieter) [1].

Bund und Parlament haben daher einen neuen Anlauf genommen und eine neue Gesetzesvorlage erarbeitet, welche auf die Kritikpunkte der ersten Abstimmung – besonders die Governance- und Datenschutzbedenken - eingegangen ist. Diese wurde im Parlament in der Wintersession 2024 mit sehr hoher Zustimmung über alle Parteien hinweg angenommen (Nationalrat: fast 90%, Ständerat: 97%).

Ein Konglomerat aus verschiedenen Interessensgruppierungen hat das Referendum dagegen ergriffen, weshalb die Vorlage nun am 28. September 2025 zur Volksabstimmung kommt.

Die e-ID

Technische Grundlagen [2]

Die e-ID funktioniert wie eine digitale Identifikationskarte. Sie wird durch den Staat herausgegeben und ermöglicht die zweifelsfreie und rechtsgültige digitale Identifikation.
Die e-ID ist so angelegt, dass sie höchste Anforderungen an Sicherheit, Datenschutz, Datensparsamkeit und Vertrauenswürdigkeit erfüllt. Sie ist freiwillig. [1]

Technisch wird ein dezentraler und offener Ansatz verfolgt. Als Tool hierfür stellt das Bundesamt für Informatik (BIS) eine «Wallet» fürs Mobiltelefon zur Verfügung. Um Missbrauch zu verhindern, ist die digitale Identität in dieser Wallet kryptographisch an ein spezifisches Mobiltelefon gebunden und kann daher nicht kopiert werden.

Die initiale Ausstellung einer e-ID oder eines anderen digitalen Identifikationsnachweises (*credential*) erfolgt zwar durch eine zentrale ausstellende Stelle (*issuing authority*), der Identifikationsprozess findet später aber dezentral direkt zwischen dem Halter (*holder*) und einer Prüfstelle (*verifier*) statt. Dabei bleibt der Halter in Kontrolle seiner Daten.

Eine zentrale Datenhaltung und damit -auswertung ist technisch nicht vorgesehen (*privacy by design).* Der Bund stellt den Akteuren aber eine Vertrauensinfrastruktur bestehend aus einem Basisregister (*base registry*) und einem Vertrauensregister (*trust registry*) zur Verfügung.

Im Basisregister sind die dezentralen Identifikatoren (*DIDs*) und deren kryptografische Schlüssel *ohne personenbezogene Daten* hinterlegt. Hier wird unter anderem die Gültigkeit verwaltet.
Im Vertrauensregister erfolgt die amtlich bestätigte Zuordnung von vertrauenswürdigen Ausstellern oder Prüfstellen zu den DIDs.
Die persönlichen Daten der Nutzer werden dabei *nie* zentral gespeichert.

Diese zwei Register ermöglichen es, sowohl die kryptographische Gültigkeit ausgestellter Nachweise zu überprüfen, sowie diese amtlich geprüften ausstellenden Behörden oder Prüfstellen zuzuordnen. Dadurch wird sichergestellt, dass alle Akteure sich während des ganzen Identifikationsprozesses jederzeit gegenseitig vertrauen können.

Eine schematische Übersicht der beschriebenen Komponenten zeigt *Abbildung 1*.

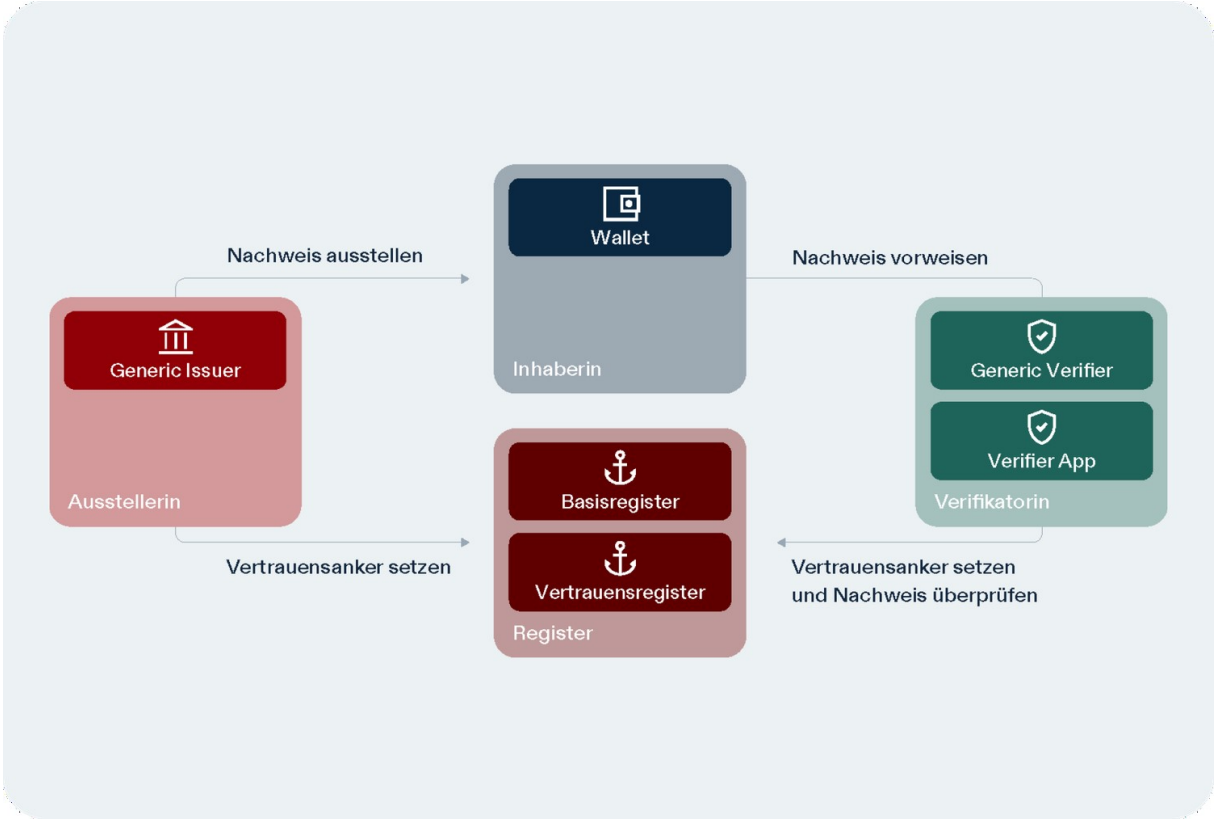

Abb. 1: Vereinfachte Übersicht der Komponenten der e-ID (nach [1], mit freundlicher Genehmigung)

Bei der dezentralen Identifikation können vom Nutzer nur selektiv die Daten ausgetauscht werden, welche für den jeweiligen Identifizierungsprozess nötig sind. Beispielsweise wird bei einer Altersverifikation nur die Information ausgetauscht, dass die Person über 18-jährig ist (*wahr* oder *falsch*) ohne weitere persönlichen Daten - nicht einmal dem Geburtsdatum.

Das Bundesamt für Technologie (BIT) stellt neben der Wallet-App auch eine Verifizierungs-App und andere technische Komponenten zur Verfügung. Alle Apps und Komponenten sind *open source.*

Stärken

Der Privacy-by-design-Ansatz ist sicherlich eine der grössten Stärken der nun präsentierten Lösung, da hierdurch die hohen Anforderungen an Privatsphäre und Datenschutz grundlegend abgedeckt werden können. Weiter fördert die offene Bereitstellung der Quellcodes der nötigen Applikationen das Vertrauen. Die technologische Grundlage ist schliesslich so ausgelegt, dass sie von einer Vielzahl an Akteuren genutzt werden kann und diese dabei von dem hohen Vertrauen in eine amtliche Personenidentifikation profitieren können.

Gegenüber der nicht fälschungssicheren physischen ID ist die e-ID durch modernste kryptographische Verfahren gesichert und kann so auch im digitalen Leben sicher angewendet werden. Mit ihr gelingt es, ein relevantes, bisher fehlendes, Grundelement für eine konsequente und nachhaltige Digitalisierung zu legen.

Probleme

Durch den konsequenten dezentralen Ansatz und die Datenschutzüberlegungen ist die Handhabung im Alltag möglicherwiese für den technisch weniger bewanderten Bürger erschwert. Das eigene Mobiltelefon muss zwingend verfügbar sein, zudem dauert der Prozess der dezentralen Überprüfung mit Abscannen eines QR-Codes und Bestätigung der Datenfreigabe eine gewisse Zeit, was möglicherweise im Alltag zu Verzögerungen führt (z.B. Einlasskontrolle). Letztendlich muss für die zentrale Überprüfung der Gültigkeit eines Nachweises auch jederzeit eine Internetverbindung zu den zentralen Registern bestehen, was aber bei anderen digitalen Anwendungen auch der Fall ist.

Formal bleibt es zwar dem Nutzer überlassen, welche Daten er teilen will, praktisch wird er aber ggf. mehr Daten als nötig teilen, wenn dies die Prüfstelle verlangt und er sonst eine Dienstleistung nicht beziehen kann. Hier sind im aktuellen Gesetz keine zusätzlichen Regulierungen zum Schutz der Benutzerdaten vorgesehen.

Das technische Hauptproblem für die Anwender dürfte die Bindung an ein bestimmtes Mobiltelefon sein. Dies ist kryptographisch notwendig, verhindert aber, dass die Identifikationsnachweise auf ein anderes (neues) Gerät übertragen werden können. Entsprechend müssen mit dem neuen Gerät auch neue Nachweise beantragt werden.
Der Bund stellt zwar in Aussicht, dass mittelfristig zentrale, verschlüsselte Backups angelegt werden können, was dann aber wieder den dezentralen Ansatz relativiert.

Das Referendumskomitee führt zudem Argumente eines digitalen Überwachungsstaats ins Feld, in welcher jeder Bürger zur e-ID gezwungen wird und jeder digitale Schritt authentifiziert/identifiziert und für soziale Kreditsysteme verwendet wird. Hierbei scheint eher ein generelles Misstrauen in den Staat und die Gesellschaft vorzuliegen als belastbare Bedenken bezüglich der vorgeschlagenen technischen Umsetzung.

Zuletzt ist die e-ID in der aktuellen Form vorerst ein rein Schweizerisches Produkt. Eine Anerkennung im Ausland liegt bisher nicht vor und müsste neben diplomatischen auch technischen Hürden überwinden (z.B. fehlende dezentrale Prüfinfrastruktur).

Insgesamt muss aber zu allen erwähnten Problemen bedacht werden, dass diese oft ihn gleicher oder ähnlicher Form auch für die physischen Ausweise oder andere digitale Produkte gelten. Zudem besteht weiterhin die Möglichkeit die klassischen Ausweise zu nutzen, wenn dies sinnvoller ist. Dadurch wird es nötig sein, die Usability der e-ID so zu optimieren, dass sie im Alltag einfacher zu nutzen ist als die analogen Alternativen.

Nutzen fürs Gesundheitswesen

Eine elektronische Identifikation ist auch für die Digitalisierung im Gesundheitswesen eine dringend benötigte, bisher fehlende Basiskomponente. Mögliche Anwendungsgebiete sind daher vielgestaltig.

In erster Linie ist hier natürlich ebenfalls die zuverlässige digitale Identifikation von Personen zu nennen. Über eine e-ID könnten beispielsweise Aufnahmen oder Terminvereinbarungen digital angeboten werden. Auch die Eröffnung des elektronischen Patientendossiers (EPD) könnte dadurch vereinfacht und der breiten Öffentlichkeit zugänglicher gemacht werden.

Auf Seite der Gesundheitsfachpersonen bietet die elektronische Identifikation ebenfalls neue Möglichkeiten. Beispielsweise könnte die Authentifizierung als zugelassener Arzt über einen elektronischen Ausweis erfolgen, womit die digitale Interaktion mit Patienten und anderen Personen aus dem Gesundheitswesen wesentlich vereinfacht würde.

Nicht zuletzt scheint auch ein grosses Potential im Bereich der digitalen Signatur von Berichten, Zeugnissen, Rezepten oder Aufklärungsdokumenten zu bestehen.

Auch im Gesundheitswesen bietet der dezentrale, patientenzentrierte Ansatz Vorteile, indem der Patient jederzeit die Datenhoheit über seine sensibelsten Daten behält.

Fazit

Die Schweizer Eidgenossenschaft verfolgt mit der nun zur Abstimmung vorgeschlagene e-ID-Lösung einen innovativen und modernen Ansatz, der so auf der Welt einzigartig ist. Es wird nicht nur eine digitale Variante der Plastikkarte erschaffen, sondern ein Vertrauensökosystem aufgebaut, dass die Digitalisierung in vielen Bereichen vorantreiben wird. Diese Entwicklung ist nicht zuletzt auch im Gesundheitswesen sehr willkommen und dringend nötig.

Es gelingt, den schwierigen Spagat zwischen Vertrauen (benötigt zentrale Autorität) und Selbstbestimmung (dezentrale Autonomie) zu machen.

Missbrauch kann grundsätzlich bei keiner Form der Identifikation ausgeschlossen werden. Hier sind eine gut funktionierende Basisdemokratie und ein intaktes Rechtssystem zur Kontrolle nötig und wichtig. Beides ist in der Schweiz aus unserer Sicht gegeben.

Die SGMI empfiehlt daher die Annahme der Vorlage und unterstützt die e-ID als grundlegender Bestandteil des zukünftigen digitalen Gesundheitswesens.

Dank

Herzlichen Dank an Prof. Serge Bignens, *Berner Fachhochschule*, für die Mitarbeit am MENTOR und die französische Übersetzung. Besten Dank an die restlichen Vorstandmitglieder der Schweizerischen Gesellschaft für Medizininformatik (SGMI) für die kritische Durchsicht des Manuskripts.

Korrespondenz

Deutsche Version

Dr. med. Lukas Dürst
Kantonsspital Graubünden
Loëstrasse 170
7000 Chur

lukas.duerst@ksgr.ch

Version française

Prof. Serge Bignens
Berner Fachhochschule
Technik und Informatik
Lehre
Höheweg 80
2502 Biel

serge.bignens@bfh.ch

Quellen

[1] Schweizer Eidgenossenschaft, «elektronische Identifikation». Zugegriffen: 27. August 2025. [Online]. Verfügbar unter: https://www.eid.admin.ch/de/

[2] Schweizer Eidgenossenschaft, «swiyu Technologie». Zugegriffen: 27. August 2025. [Online]. Verfügbar unter: https://swiyu-admin-ch.github.io/introduction/