DIDAS

Stellungnahme DIDAS
zum
Diskussionspapier zum «Zielbild E-ID»

Digital Identity and Data Sovereignty Association
www.didas.swiss
Campus Zug Rotkreuz
Surstoffi 1
CH-6343 Rotkreuz
Switzerland

Inhalt

Vorwort

Sehr geehrte Damen und Herren

Der Verein Digital Identity and Data Sovereignty (DIDAS) bedankt sich für die Möglichkeit, im Rahmen der öffentlichen Konsultation zum «Zielbild E-ID» Stellung nehmen zu dürfen.

Digital Identity and Data Sovereignty Association (DIDAS) ist ein gemeinnütziger und nicht gewinnorientierter schweizerischer Verein, der mit dem folgenden primären Ziel gegründet wurde: „*Die Etablierung und Förderung der Schweiz als führendes Ökosystem bei der Entwicklung und Einführung von Technologien, Dienstleistungen und Produkten zur Wahrung der Privatsphäre, welche die digitale Identität und elektronisch überprüfbare Daten bewahren sowie anwenden.*“

Unsere Vision ist es, die digitale Zukunft einem breiten Spektrum von Branchen und Anwendungsfällen zu ermöglichen, in denen Privatpersonen, Unternehmen, Fachleute, Behörden, Gemeinschaften und sogar angeschlossene Geräte in der Lage sind, auf Basis ihrer Identität und damit zusammenhängende, proprietäre Daten auf elektronischem Wege einfach miteinander auszutauschen und dabei das Dateneigentum und die Privatsphäre zu wahren. Dabei sollen die Rechte an den Informationen und an die Compliance respektiert werden.

Um unsere Vision und Ziele zu erreichen, arbeiten wir mit technologieorientierten Startups, Gesellschaften, Behörden und NGOs zusammen.

Wir freuen uns über die Gelegenheit, hiermit unsere Stellungnahme zum Diskussionspapier «Zielbild E-ID» einreichen zu dürfen und positionieren uns als passionierte Schweizer Expertengruppe, welche für die weiteren Schritte in der E-ID Diskussion und der Entscheidungsfindung nützlich ist. Wir aspirieren Mehrwert zu schaffen, indem wir nach nachhaltigen Prinzipien, entsprechend schweizerischen Governance-Anforderungen, der Einhaltung resp. Etablierung von globalen Standards, ein inkrementell wachsendes Wissens-Ökosystem rund um Self-Sovereign Identity (SSI) ermöglichen. Wir sind auch international in die entstehenden Attribut-Ökosysteme als Experten eingebettet.

Die Stellungnahme ist eine Gemeindsschaftsarbeit aller Mitglieder des Vereins DIDAS unter der Federführung des Vorstandes. Da DIDAS als unabhängige Expertengruppe, aus Mitgliedern aller Stakeholdergruppen besteht, steht es unseren Mitgliedern frei auf eine Nennung zu verzichten. Um jedoch das Gewicht von DIDAS zu veranschaulichen, freuen wir uns folgend einige unserer Mitglieder explizit zu nennen: SWITCH AG,

AdNovum Informatik AG, Stadt Zug, Swisscom, Procivis, Verein Cardossier, HIN AG, Swiss Data Alliance, Hochschule Luzern, Prof. Tim Weingärtner, der Vorstand und alle Mitglieder des Vereins Digital Identity and Data Sovereignty (DIDAS).

Wir freuen uns, uns in der öffentlichen Diskussion mit unseren Experten und unserem Netzwerk jederzeit einzubringen und bedanken uns noch einmal für die Möglichkeit, uns in dieser öffentlichen Konsultation zum «Zielbild E-ID» einbringen zu dürfen.

Rotkreuz, den 30.09.2021

Vasily Suvorov
Präsident

Daniel Säuberli
Gründungs- und Vorstandsmitglied

Stellungnahme DIDAS
zum
Diskussionspapier zum «Zielbild E-ID»

I. Zusammenfassung unserer Stellungnahme

Wir sind fest davon überzeugt, dass Ökosysteme digitaler Attribute nach den Prinzipen von SSI (Self Sovereign Identity resp. die der selbstbestimmten digitalen Identität) in Kontext mit dem schweizerischen Wertesystem und unserem föderalistischen Staatskonstrukt sowie unserer internationalen Positionierung, den aktuell bestmöglichen Ansatz darstellen, um eine nachhaltig zukunftsfähige, flexible, datenschutzfreundliche und umfangreiche E-ID Funktionalität in der Schweiz zu etablieren.

Daher fordern wir, dass der Staat sich mindestens auf die Herausgabe von digitalen Identitätsattributen (oder digitalen Nachweisen) in Kontext der Weiterentwicklung der Vision E-ID, sowie auf die relevanten Gesetze auf Ambitions-Niveau 3 konzentriert. Wir sind der Überzeugung, dass der Erfolg der E-ID Initiative in der Schweiz nur dann erzielt werden kann, wenn Public-Private-Partnerships ermöglicht werden (PPP, als Zusammenarbeits-, nicht als Rechtskonstrukt), welche die staatlichen Identitätsattribute als Vertrauensanker resp. als Basis für den Aufbau eines oder mehrerer Ökosysteme verwenden können. Wichtig in diesem Zusammenhang ist auch zu verstehen, dass Ökosysteme bereits ohne diese Attribute entstehen und genutzt werden können, die durch die spätere Verfügbarkeit dieser staatlichen Attribute an Vertrauenswürdigkeit gewinnen können.

Wir sehen also die Rolle des Staats als einen wichtigen Teil des künftigen Ökosystems digitaler Nachweise, der dieses durch die relevanten, hoheitlich herausgegebenen und elektronisch verifizierbaren Attribute ermöglicht. Die SSI Mechanismen machen es dann weiteren Akteuren möglich, ihre Anwendungsfälle darauf auf- und auszubauen und durch Marktmechanismen und technologische Fortschritte (z.B. via digitaler Brieftaschen oder «Wallets») diese möglichst umfangreich der Gesellschaft zur Verfügung zu stellen. Aufgrund der konsumentenzentrierten Adaption von Wallets ist es in diesem Zusammenhang ausserordentlich wichtig, die Zivilgesellschaft von Anfang an in den Prozess einzubeziehen. Es ist zudem vorteilhaft zu fordern, die Wallets mit einem technologischen Vertrauensanker durch die Nutzung von Open Source Communities und -Lizenzen zu entwickeln.

Einer der wichtigsten Eigenschaften von SSI ist, dass sich die Entwicklung nachhaltig über eine solide Governance und den eingebetteten technologischen Möglichkeiten (wie z.B. Zero Knowledge Proof-Verfahren) sowie der Etablierung von Prinzipien steuern lässt, sodass die Grundrechte, Datenschutz, Privatsphäre und andere hoheitliche Anforderungen «by design» gewährleistet werden können. Dies gleichzeitig, ohne dass Wettbewerbsfähigkeiten verschiedener Marktakteure oder die Souveränität der Gesellschaft reglementiert oder eingeschränkt werden - oder werden müssen, sodass wir national und international digital agil und handlungsfähig bleiben.

Unsere Kommentare und Bemerkungen zum Diskussionspapier sind wie folgend aufgeteilt:

1. Antworten und Kommentare zum Kapitel 7 - Öffentliche Diskussion des Zielbilds E-ID
2. Kommentare zur Sektion 5.1.6. des Diskussionspapier „Offene Fragen zum SSI-Ansatz“
3. Kommentare zum Kapitel 5.2 - Warum SSI besser als PKI ist

II. Antworten und Kommentare zum Kapitel 7 - Öffentliche Diskussion des Zielbilds E-ID

1. Frage: Wo sehen Sie den besonderen Nutzen der E-ID und welche Anwendungsfälle stehen für Sie im Vordergrund?

Das Ambitionslevel bestimmt das Ausschöpfungspotential der digitalen Transformation und somit ganz direkt die Leistungs- und Wettbewerbsfähigkeit der Schweiz in einer zunehmend digitalen Welt. Um mit den Möglichkeiten der Digitalisierung Mehrwerte schaffen zu können, benötigen wir Ökosysteme, in denen über Organisations- und Ländergrenzen hinweg digitale Nachweise sicher und unfälschbar ausgetauscht werden können (z.B. beim Kauf von altersbegrenzen Gütern, der Ausweispflicht im internationalen Reiseverkehr, beim Nachweis einer Versicherungsdeckung, beim Verifizieren eines gültigen COVID-Zertifikats oder beim Sicherstellen von reibungslosen kommerziellen Prozessen zwischen Vertragspartnern).

Anforderungen an digitale Identitätsnachweise von Personen sowie vermehrt von Organisationen und Dingen (IoT) sind dafür die Basis. Qualifikationen und Berechtigungen aller Art (z.B. Ausbildungs- und Gesundheitsnachweise, Herkunftszeugnisse, Mitarbeiter- und Mitgliedschaftsausweise und so weiter) müssen innerhalb der Schweiz und auch mit unseren Internationalen Partnern nachhaltig souverän und anhand von internationalen Standards ausgetauscht werden können.

Die E-ID ist in einem solchen Ökosystem nur ein digitaler Nachweis unter vielen. In der Zusammenfassung des "Zielbild E-ID" wird die Frage nach der Vision einer zukünftigen E-ID aufgeworfen. Dabei werden zwei unterschiedliche Szenarien sinnbildlich dargestellt:

- E-ID als ein staatlich ausgestellter, digitaler Ausweis (analog dem Schweizer Pass), oder
- E-ID als "Vertrauens-Ökosystem" mit digitalen Nachweisen jeglicher Art, welche sowohl von öffentlicher als auch privater Hand herausgegeben werden können.

Diese beiden Szenarien schliessen sich gegenseitig NICHT aus, umreissen jedoch folgerichtig die Grunddiskussion, welche aktuell in der Schweiz geführt werden sollte: "Was wollen wir mit einer E-ID erreichen -Nicht nur heute oder morgen, sondern auch in Zukunft...".

Es geht also nicht weniger um die Frage, wie sich die Schweiz national und international in Bezug auf das Thema Digitalisierung strategisch aufstellen will.

DIDAS hat hinsichtlich dieser strategischen Frage eine klare Vorstellung. Bezugnehmend auf die in Kapitel 4 erwähnten Ambitionsniveaus erachtet DIDAS das Ambitionsniveau 3 als einzige mögliche Vision, welche genügend Mehrwerte für Nutzer, Unternehmen und öffentliche Hand ermöglicht, die Wettbewerbsposition und digitale Souveränität der Schweiz im In- und Ausland stärkt und eine solide und zukunftsfähige Vertrauensgrundlage für Innovation in der Digitalisierung und Geschäftsprozess-automatisierung schafft. Folgende Überlegungen stützen diese Einschätzung:

- Eine E-ID als Authentifikationsmittel mit dem primären Ziel, Zugang zu Onlinediensten zu gewährleisten ("Login"-Funktionalität) ist u.E. zu kurz gegriffen und entspricht nicht mehr den heutigen Marktbedürfnissen. Es existieren heute schon ausgereifte und am Markt eingeführte Produkte und Dienstleistungen (z.B. Single Sign-On, Social Logins, Identifizierungs- und Identitätsdienstleistungen, Passwort-Manager, passwortlose Authentifizierung), die diese Funktionalität ermöglichen und von Konsumenten akzeptiert werden. Der einzige Mehrwert einer E-ID unter diesem Blickwinkel ist eine höhere Qualität der Identitätsbestätigung resp. eine zusätzlich staatliche Zusicherung, was ausgesprochen wichtig, aber in Hinblick auf den geplanten Realisierungszeitraum (2025 / 26) nicht wirklich die Digitalisierungsherausforderungen adressiert.
- Der Nutzen einer staatlichen E-ID soll darin bestehen, dass schweizweit verlässliche digitale Identitätsnachweise für alle, so zum Beispiel auch für die Akteure im Gesundheits- und Sozialwesen geschaffen werden können, in einem Rechtsrahmen der es erlaubt einen Identitätsnachweis in den entsprechenden Prozessen einfach und sicher einzusetzen. Der Hauptanwendungsfall ist der Identitätsnachweis als Basis für digitale, branchenspezifische Prozesse - die Funktion des Passes, eines Handelsregisternachweises oder der ID wird somit in die digitale Welt transportiert. Analog zum Vorzeigen eines amtlichen Ausweisdokuments, soll der Inhaber einer E-ID gegenüber einem Service seine staatlich geprüften Attribute einfach, sicher und möglichst ohne Intermediär weitergeben können. Die E-ID soll für dieses Ausweisen verwendet werden können - eben als vertrauenswürdige, staatliche Basis-ID, resp. als Vertrauensanker für alle darauf aufbauenden weiteren Attribute oder *Credentials*. Damit können insbesondere Onboarding- und KYC- Prozesse unterstützt werden.
- Gleich wie in der physischen Welt erfordert die Abwicklung bestimmter Dienstleistungen oder Behördengeschäfte auch in der digitalen Welt die Identifikation der beteiligten Nutzerinnen und Nutzer. In vielen Anwendungsfällen genügt jedoch bereits der Nachweis eines bestimmten Merkmals, wie

beispielsweise das Erreichen des erforderlichen Mindestalters beim Kauf von Gütern, die einer Altersbeschränkung unterliegen. Überall dort, wo keine spezifischen Regelungen gelten und ein Geschäftsvorfall mit einer unmittelbaren Zahlung abgeschlossen werden kann, ist üblicherweise kein weiterer Nachweis zur Abwicklung einer Transaktion erforderlich. In diesem Spannungsfeld zielen Konzepte wie namentlich der von Ihnen aufgegriffene Ansatz „Self-Sovereign Identity“ (SSI) darauf ab, datenschutzrechtlichen Anliegen wie dem Prinzip der Datenminimierung mittels selbstverwalteter Identitäten und Attributen bestmöglich zu entsprechen. Gleichermassen sollen auch die weiteren Ansprüche der handelnden Akteure, allen voran an die Benutzerfreundlichkeit, berücksichtigt werden, indem konzeptionell an altbekannte Abläufe aus der physischen Welt angeknüpft wird.

Ein derart ausgestaltetes Vertrauensökosystem bildet schliesslich die Basisinfrastruktur für eine digitale Landschaft, auf deren Grundlage sich bereits bestehende Anwendungen überhaupt erst in der Breite etablieren und neue Anwendungen gedeihen können.

DIDAS begleitet und unterstützt also eine Anzahl von unterschiedlichen Initiativen der öffentlichen und privaten Hand und ist aus diesem Grund der festen Überzeugung, dass ein wichtiger Erfolgsfaktor der Digitalisierung die zweifelsfreie Feststellung der Identitäten der involvierten Parteien ist. Dabei gilt es aber zu berücksichtigen, dass die Anforderung an die «Identifizierung» je nach Kontext unterschiedlich festgelegt wird. Angefangen von einer blossen Feststellung einer Existenz bis hin zum Beweis bestätigter Berechtigungen, ergeben sich unterschiedliche Erwartungen, welche Identitätsattribute und Nachweise in einem digitalen Prozess relevant werden. Eine solche Identitätsdefinition geht über die Bereitstellung von staatlichen Beweisen hinaus und berücksichtig auch verifizierte Informationen aus der Privatwirtschaft.

Digitalisierung bedeutet nicht, bestehende analoge Prozesse in der digitalen Welt «nachzubilden». Digitalisierung bedeutet, die Chancen zu nutzen, um «es anders zu tun» oder «fundamental neu zu denken». D.h., dass eine Nachbildung von komplexen Abläufen aufgrund «physischer» Hürden vermieden werden sollte[1]. In der digitalen Welt werden Prozessschritte automatisiert, verschmelzen oder verschwinden, was wiederum einen positiven Einfluss auf das Kundenerlebnis hat und Abläufe effizienter gestalten lässt.

[1] Beispiel: Bei einem Bewerbungsprozess stellt der Bewerber dem Unternehmen unterschiedliche beweiskräftige Informationen, wie Passdaten, Zertifikate und Arbeitszeugnisse von unterschiedlichen Ausstellern zur Verfügung. Diese Dokumente müssen im Vorfeld dem Bewerber «physisch» zugestellt werden, der Bewerber muss diese Dokumente in einem Dossier zusammenstellen und dann beim neuen Arbeitgeber einreichen. Es gibt heute «digitale» Vereinfachung (bspw. Dokument als PDF oder das Hochladen von Dokumenten), aber nach wie vor ist der Zeitaufwand für alle Beteiligten sehr hoch.

Um dieser Denkweise Rechnung zu tragen, muss die Identifizierung als integraler Bestandteil des Gesamtprozesses gesehen werden und ein zukünftiges «E-ID Ökosystem» sollte so ausgestaltet sein, dass solche Prozessinnovationen realisiert werden können.

DIDAS ERKENNT DIESBEZÜGLICH NUR IM AMBITIONSNIVEAU 3 DIE ERFÜLLUNG DIESER ANFORDERUNG. ES ERSTAUNT AUS DIESEM GRUND AUCH WENIG, DASS DIE EUID GENAU IN DIESE RICHTUNG ABZIELT.

2. **Frage: Welches sind für Sie die drei wichtigsten Anforderungen an eine staatliche E-ID als digitaler Ausweis?**

Damit sich digitale Lösungen durchsetzen, müssen diese in puncto Ausgestaltung im Publikum auf Akzeptanz stossen und klare Vorteile für alle beteiligten Akteure mit sich bringen. Aus diesen Zielen lassen sich drei konkrete Anforderungen an eine E-ID ableiten:

a. **Vertrauenswürdigkeit**

Das Vertrauen in elektronische Identifikationslösungen fusst wesentlich auf dem Schutz der Privatsphäre der E-ID-Benutzerinnen und -Benutzer. Dabei stehen datenschutzrechtliche Prinzipien wie "privacy by design" sowie Datensparsamkeit im Brennpunkt. Es darf bei der Verwendung (d.h. konkret bei der Überprüfung) der E-ID keine Kommunikation mit dem Issuer stattfinden [2]. Ebenso soll der Recovationstatus eines einzelnen Credentials nicht getracked werden können. Diese Kriterien lassen sich unseres Erachtens am ehestens mit Konzept SSI verwirklichen, da dieses auf offenen Grundprinzipien beruht.

Unter den diversen datenschutzrechtlichen Vorzügen dieses Ansatzes, ist insbesondere die Reduktion auf die je nach Anwendungsfall notwendigen Attribute bei der Datenübertragung an Dritte und die konsequente Vermeidung unnötiger Datenflüsse und der damit verbundenen Randdaten hervorzuheben.

Die staatlichen E-ID Attribute sollen exklusiv von einer staatlichen Stelle ausgegeben werden. Perspektivisch im gleichen Prozess, bei dem ein(e) Bürger*in den Pass und die ID erhält oder ein(e) Ausländer*in den Aufenthaltsausweis, jedoch in diesem Fall digital in eine kryptografisch geschützte, persönliche Wallet, mit Hilfe einer dezentralen Registry für die Verifizierung.

[2] Wichtig: Kein OCSP. Das Online Certificate Status Protocol (OCSP) ist ein Legacy-Netzwerkprotokoll, das es Clients ermöglicht, den Status von X. 509-Zertifikaten bei einem Validierungsdienst abzufragen.

b. Benutzerfreundlichkeit

Digitale Transaktionen, die den Einsatz der E-ID erfordern, müssen ebenso einfach handhabbar und transparent ausgestaltet sein wie alle übrigen digitalen Geschäftsprozesse, um im Publikum breit akzeptiert zu werden. Die Ermöglichung einer zweifelsfreien Identifizierung einer natürlichen Person in einem digitalen Prozess über unterschiedliche Schnittstellen (API, NFC, QR Code, BLE und Wifi). Diese Identifizierung sollte eineindeutig, staatlich legitimiert und authentifizierbar sein. Die E-ID als Ausweis ist somit das digitale Äquivalent des Schweizerischen Passes, Nukleus / Zuordnungspunkt für weitere Attribute und Nachweise zu dieser Identität (sog. *verifiable Claims*). D.h. dieser E-ID können eineindeutig weitere Informationen, Beziehungen und Delegationsverhältnisse zugeordnet werden, welche wesentlich zur umfassenden Beschreibung der Identität beitragen.

Was von den Benutzerinnen und Benutzern dabei als benutzerfreundlich empfunden wird, bestimmt sich in massgeblicher Weise nach dem jeweils aktuellen Stand der Technik und vorherrschender Trends. War der Einsatz zusätzlicher Geräte oder Karten zwecks Authentisierung beispielsweise noch lange gang und gäbe, dürfte ein entsprechend ausgestaltetes Verfahren heute auf breite Ablehnung stossen.

Demzufolge ist eine hohe Adaptionsfähigkeit an die jeweils aktuellen Ansprüche der Benutzerinnen und Benutzer an die Benutzerfreundlichkeit erforderlich. Der zu schaffende Rechtsrahmen für eine staatliche E-ID-Lösung sollte daher zwar klare Leitplanken setzen ("was"), jedoch namentlich betreffend die benutzerseitigen Systeme weitestgehend technologieneutral, auf offenen, internationalen Standards ausgestaltet sein ("wie"), um eine stetige Weiterentwicklung und Umsetzung von vielmöglichste Anwendungsfälle zu ermöglichen.

Die E-ID kann auch im Ausland (mindestens EU) in digitalen und analogen Prozessen einfach eingesetzt werden.

c. Vertrauensökosystem

Wie Sie in Ihrem Diskussionspapier darlegen, sehen sich Initiativen wie die Einführung nationaler E-IDs regelmässig mit dem "chicken or the egg"-Dilemma konfrontiert: ohne E-ID werden keine Anwendungsfälle geschaffen und ohne Anwendungsfälle wird keine E-ID benötigt.

Vor diesem Hintergrund erachten wir den neuen Anlauf, eine nationale E-ID zu schaffen, als grosse Chance, ein umfassendes Vertrauensökosystem zu etablieren, das einerseits die Anforderungen an eine vertrauenswürdige, staatliche E-ID erfüllt und andererseits den regulatorischen Rahmen für eine Vielzahl von Anwendungsfällen schafft (Staatlicher Vertrauensanker (und Governance) ist hier wichtig), um das grösstmögliche Potential des digitalen Wandels auszuschöpfen. Dabei soll die Offenheit des Systems für die Nutzung durch möglichst viele Diensteanbieter gewährleistet werden.

Das "Ambitions-Niveau 3" im Rahmen des vorgeschlagenen SSI-Ansatzes bietet unseres Erachtens daher den geeigneten Rahmen, um mit den Möglichkeiten der Digitalisierung Mehrwerte für alle beteiligten Akteure zu schaffen. In einem solchen Vertrauensökosystems wird die E-ID schliesslich einen von verschiedenen digitalen Nachweisen darstellen, wobei private und öffentliche Stellen wie Bildungsinstitutionen, Transportunternehmen, Tourismusbetriebe, Telecomprovider, Finanzdienstleister, medizinische Leistungserbringer und Krankenversicherer, Kulturdienstleistende oder dergleichen ebenfalls digitale Nachweise herausgeben können, womit sich der Gesamtnutzen des Vertrauensökosystems entscheidend erhöht und es allen Teilnehmern im Ökosystem ermöglicht, Domain- oder Branchenspezifische oder -übergreifende digitale Prozesse entlang von Interaktionen und Transaktionen neu zu denken sowie intermedär-frei und reibungslos ablaufen zu lassen.

3. **Frage: Welchen Nutzen sehen Sie in einer nationalen Infrastruktur, die es dem Staat und Privaten ermöglicht, digitale Nachweise (z. B. E-ID, digitaler Führerausweis, Mitarbeiterausweise, Ausbildungsnachweise) auszustellen und überprüfen zu können?**

Wir haben in unserer Antwort zu Frage 1 versucht, den Nutzen zu beleuchten, die E-ID nicht nur als digitalen Ausweis, sondern als **nationale Vertrauensinfrastruktur** zu betrachten. DIDAS ist der festen Überzeugung, dass nur unter einer solchen Betrachtungsweise, spürbarer Mehrwert für Zivilbevölkerung, Wirtschaft, öffentliche Hand und Politik entstehen kann. Damit kann der Schweiz ein wesentlicher Schritt in Richtung Teilnahme an den weltweit entstehenden digitalen Ökosystemen und der fortschreitenden Digitalisierung ermöglicht werden, jedoch ohne Kompromisse in Punkto Souveränität, Privatsphäre und Sicherheit einzugehen.

Was die Schienen-, Strassen-, Strom- und Telekomnetze für die industrielle Entwicklung der Schweiz bedeuteten, wird ein digitales Vertrauensnetzwerk (oder digitale Vertrauensinfrastruktur) für die Schweiz im einundzwanzigsten Jahrhundert bedeuten. An dieser Stelle möchten wir, um eine möglichste grosse Entfaltung der nationalen E-ID

Infrastruktur zu erreichen, drei zusätzliche Anforderungen miteinbringen, welche bei der Konzeption und Realisierung zwingend berücksichtigt werden sollten:

a. Schutz der Identität und Privatsphäre jedes einzelnen, Sicherstellung der Datenintegrität

Die Wahrung der Identität, der Schutz der Privatsphäre und die Sicherstellung der Integrität sind die wichtigsten Erfolgsfaktoren und zentral in der Ausgestaltung eines E-ID Ökosystems. Erst wenn die Teilnehmer vertrauen haben, dass sie nicht ausspioniert werden oder zu viele Informationen von sich preisgeben müssen, dass sie geschützt vor unberechtigten Dritten und die ausgetauschten Daten integer und nicht manipuliert sind, dann partizipieren sie aktiv und das Ökosystem beginnt zu leben. Aus diesem Grund erachten wir *Datenschutz und -minimierung, Wahlfreiheit und Kontrolle über die eigene Identitätsdaten, sowie gesicherte Kommunikationsverfahren auf einer zuverlässigen, belastbaren Infrastruktur als die wichtigsten Gestaltungsprinzipien*, die es zwingend zu berücksichtigen gilt.

b. Internationale Interoperabilität

Digitalisierung hört nicht an der Landesgrenze auf. Aus diesem Grund ist DIDAS der Auffassung, dass die internationale Interoperabilität und damit auch die Anlehnung an internationalen Standards (bspw. EUid, eIDAS, W3C) zwingend zu erfolgen hat. Wir sind der festen Überzeugung, dass dies schon von Anfang berücksichtigt, werden sollte. Ein «isoliertes Swiss E-ID Ökosystem» würde u.E. *das Potential massiv beschneiden*. Die Schweiz ist eine kleine, offene Volkswirtschaft, die heute schon rege im wirtschaftlichen und sozialen Austausch mit anderen Ländern steht. *Wir begrüssen, dass der Autor des Diskussionspapieres auf diesen Tatbestand hingewiesen und den Verweis zur EUid gemacht hat. Gerne möchten wir die Wichtigkeit an dieser Stelle nochmals klar unterstreichen.*

c. Ausgestaltung des Ökosystems unter Einbindung der Privatwirtschaft und Zivilgesellschaft, klarer Rollen und nachhaltiger Prinzipien

Der Staat spielt zweifelsohne eine zentrale Rolle in der Definition und Ausgestaltung, sowie im Betrieb digitaler Ökosysteme. DIDAS ist der festen Überzeugung, dass es ohne privatwirtschaftliche Beteiligung nicht gehen wird. Aus diesem Grund ist es von Anfang an wichtig, die unterschiedlichen Rollen präzise zu definieren und entsprechend die unterschiedlichen Kompetenzen und Verantwortlichkeiten gebührend zu berücksichtigten. Ein E-ID Ökosystem ist ein sich entwickelndes Gebilde, *es ist aktuell nicht vorhersehbar, welche Anwendungsfälle in 5 oder 10 Jahren relevant sind,* welche zusätzlichen Innovationen notwendig werden, um diese zu realisieren. Um diese Innovationen zu ermöglichen, ist Wettbewerb wichtig und damit auch die Einbindung von unterschiedlichen privatwirtschaftlichen Akteuren (Herausgeber von Nachweisen,

Integratoren, Technologiepartner, Dienstleistungsanbieter für Privatkunden und Unternehmen, etc.).

U.E. soll der Staat sich auf die Ausgestaltung des Vertrauensrahmen («*Governance Framework*»), die Anerkennung der Teilnehmer und Partner, die Spezifikation der Qualitätslevels, die Zertifizierung der Prozesse und Technologien sowie die Ausstellung der staatlichen Nachweise konzentrieren. Eine derartige Rollendefinition heisst nicht, dass der Staat die Zügel wieder aus den Händen gibt, sondern dass er unter kontrollierter Einbindung der Privatwirtschaft die Entwicklung des E-ID Ökosystems vorantreibt.

Es ist auch wichtig zu bemerken, dass wenn ein Attribut im Ausland verifiziert werden sollte (z.B. ID bei einer Reise, ein Altersattribut oder ein COVID-Zertifikat, etc), die SSI nicht nur ein einzelnes Netzwerk als die Basis für Nationalinfrastruktur ermöglicht, sondern auch sogenannte «Network of Networks» (oder Netzwerk der Netzwerke).

Durch Interoperabilität der Wallets und «*Institutional Agents*» ist es möglich, verschiedene miteinander kompatible SSI Netzwerke zu betreiben. Insbesondere hilft es, das Huhn-Ei-Problem zu lösen, indem hoheitliche Anwendungsfälle des Bundes und der Kantone durch das dafür gestaltete Netzwerk und den dafür geeigneten Vertrauensrahmen (Governance Framework) umgesetzt und betrieben werden können, jedoch falls vom Benutzer gewünscht, seine verfügbaren verifizierbaren Attribute anhand von Standards über weitere (z.B. internationale) Netzwerke verifiziert werden können (z.B. Krankenversicherungsdeckung bei Spitalaufenthalt im Ausland, Gültiger COVID-Immunitätsnachweis im Ausland). Diese «Basisanwendungsfälle» können durch kompatible Wallets[3] und Systeme der kommerziellen und öffentlichen Akteure erweitert werden, ohne dass sie einen direkten Zugriff auf das «hoheitliche Netzwerk» brauchen. Dieser Ansatz wird einerseits helfen, die Aufgaben des Staats bezüglich E-ID und anderen verifizierbaren Attribute unabhängig von ausländischen Akteuren umzusetzen. Andererseits wird er aller Art anderen öffentlichen und kommerziellen Akteuren in der Schweiz und im Ausland es ermöglichen, darauf andere, wertvolle Anwendungsfälle auszubauen. Dies würde für die Schweizer Wirtschaft wie auch für die Behörden einen grossen Nutzen darstellen. So könnten die verschiedensten Ökosysteme entstehen, in denen spezifische Services und Prozesse in einem Vertrauensraum angeboten und abgewickelt werden können.

3 Beim Thema Wallet sehen wir (mind. vorübergehend) einen Nutzen in einer Open-Source Swiss-Wallet, welche erstens in der eigenen Geschwindigkeit weiterentwickelt und zweitens mit unseren Eigenheiten versehen werden könnte. Aber schlussendlich sollte jede (genügend sichere Wallet) verwendet werden können.

III. Kommentare zur Sektion 5.1.6. des Diskussionspapier „Offene Fragen zum SSI-Ansatz“

1. Welche Governance-Ebenen gibt es und wer ist dafür zuständig (z. B. Governance Ebenen nach Trust over IP Framework: Ökosystem, Credentials, Provider, Utility)?

Das ToIP-Framework bildet einen guten Rahmen zu den Governance-Überlegungen und sollte u.A. als Basis verwendet werden. Sobald der Richtungsentscheid für eine zukünftige Schweizer E-ID zu Gunsten SSI ausfällt, sollte der Bundesrat die Gremien bestimmen, welche in Zusammenarbeit mit den europäischen Initiativen zur Errichtung eines digitalen Vertrauensnetzwerkes die technischen Standards festlegt. Dabei kann weitestgehend auf die W3C-Standards zurückgegriffen werden, die laufend weiterentwickelt werden.

Was die einzelnen Ökosysteme (Mobilität, Gesundheit, Ausbildung, Finanzwesen, Verwaltung, Justiz u.a.) betrifft, soll auf die bestehenden Netzwerke, Strukturen und Verbände aufgebaut werden. Wenn der Richtungsentscheid einmal gefällt ist, können auf dieser Basis die verschiedenen organisationübergreifenden Prozesse neu gedacht und entwickelt werden.

Wir erachten es als wichtig, wenn schon frühzeitig die Privatwirtschaft sowie weitere Institute in die Definition des Governance-Frameworks miteinbezogen werden. Insbesondere bei Ambitionsniveau 3, welches nicht nur staatliche Beweise, sondern auch Nachweise von weiteren autoritativen Stellen herausgegeben werden, ist die Zusammenarbeit und gemeinsame Akzeptanz essentiell.

2. Muss der Staat auf gewissen Komponenten das Monopol haben? Müssen Wallets staatlich zertifiziert werden? Wird die Auswahl von Wallet und Institutional Agent dem User überlassen? Gibt es eine Regelung, welche Teile kooperativ, welche in Konkurrenz erstellt und betrieben werden?

Nein, ein Monopol irgendeines Akteurs im Rahmen von SSI widerspricht dem Kerngedanken von SSI. Der Staat verfolgt in einem SSI-Ansatz die vertrauensbildenden Massnahmen, mit anderen Worten, er ermöglicht den "Human Trust". Dies bedeutet, dass er die Gesamtverantwortung für das Governance Framework trägt, Standards vorgibt, die Qualitätslevels und -regeln definiert, sowie Prozesse, Technologien und Infrastrukturen zertifiziert[4]. U.E. wird aber vom Staat nicht erwartet, dass er die Technologie bereitstellen

[4] Wie schon erwähnt, betrachten wir das Konzept von «Network of Networks» als den besten Ansatz, die Vertrauensinfrastruktur für SSI Ökosystem aufzubauen.

muss. Die Wahlfreiheit bei allen Komponenten, die nicht zwingend staatlich betrieben werden müssen, soll maximiert werden. Zur Einhaltung der Mindestanforderungen gemäss Governance-Framework kann eine Zertifizierung der Wallets zielführend sein.

3. **Wer betreibt die Registry? Ist eine eigene, nationale Registry nötig oder schliesst man sich einem bestehenden, internationalen Ökosystem an? Wollen oder sollen Kantone, Städte oder private Unternehmen Speicher-Knoten (Nodes) betreiben dürfen? Welche Technologie wäre zu bevorzugen? Welche Rolle spielt die Datenmenge? Wie löst man Interoperabilitätsfragen zu anderen Registries? Besteht für den Issuer sogar die Wahlfreiheit der Registry?**

Der Entscheid über die Technologie, den Aufbau und Betrieb des Registry soll an den Kriterien der Performanz, der Resilienz, der internationalen Interoperabilität und der Effizienz gemessen werden.

Aufgabe des Bundes ist es obige Kriterien zu definieren und deren Einhaltung durchzusetzen. Der Betrieb des Registry kann in Eigenregie oder im Auftrag des Bundes erfolgen. Kein Kriterium soll die Einbindung der verschiedenen politischen Verwaltungsebenen sein.

Der Aufbau und der Betrieb des Registry ist eine Infrastrukturaufgabe zu Gunsten der gesamten Volkswirtschaft und soll demzufolge auch von der Allgemeinheit finanziert werden. Nichtsdestotrotz schlagen wir vor, dass der „Network of Networks“ Ansatz bei der Umsetzung der SSI -Infrastruktur als wichtiger Bestandteil der detaillierten Ausarbeitung des Designs berücksichtigt werden soll, sodass NoN ermöglicht werden können und die Skalierung von Anwendungsfällen nicht behindert wird. Die Wahl der Registry soll also primär einen sicheren, stabilen Rahmen für den staatlichen Vertrauensanker liefern. Den Issuern sollen die Freiheit zur Wahl einer Registry belassen werden.

4. **Wer darf Issuer sein? Bleibt das System völlig offen zum Gewinn zusätzlicher Anwendungsfälle oder werden die Issuer spezifisch ausgewählt oder berechtigt?**

Bei Ambitionsniveau 3 gehen wir von einem offenen System aus. Eine SSI-basierte E-ID ist der Eckstein des gesamten SSI-Ökosytems, worauf sich öffentliche und private Issuer stützen können, um ihre eigene Verifiable Credential herauszugeben. Der Rolle

des Staats soll sich auf die Herausgabe der E-ID fokussieren. Das Issuing von weiteren staatlichen, institutionellen und privaten Issuer soll möglich sein. Es sollte ein Trust-Level geben, damit hochprioritäre Dienste stärker gesichert sind. Analog der Domain-Name Vergabe im Internet sollte es eine geringe Gebühr als "Spam-Schutz" geben.

Dies lässt sich mit dem „Networks of Networks“ Ansatz einfach umzusetzen, wobei das für z.B. Staatliche Issuers gestaltete SSI-Netzwerk (oder Registry) besondere Regeln (Governance Framework) hat.

5. **Wie werden Backups und Transfers von Credentials ermöglicht? Wie können zentrale Backups und damit attraktive Hacker-Angriffsziele vermieden werden? Welche Rolle spielt eine mögliche kryptografische Verbindung zwischen Wallet und Verified Credentials?**

Das Backup soll beim Bürger dezentral erfolgen, um einen zentralen Angriffspunkt zu vermeiden. Die Mindestanforderungen an Backups von Wallets inklusive damit verknüpfter Credentials soll im Governance-Framework geregelt werden. Wir empfehlen, sich an den aktuellen Stand der internationalen Entwicklungen anzulehnen. Wir sehen heute schon Ansätze, die die wichtigsten Antworten auf diese Fragen geben. Des weiteren verweisen wir auf die aktuell laufenden Arbeiten innerhalb der EU («Toolbox for a EU Digital Identity Framework»).

6. **Welche Sicherheitsmechanismen sind für den Zugriff zur Wallet nötig?**

Dies soll auf Basis gängiger Standards für die geforderten Sicherheitsniveaus im Governance-Framework geregelt werden. Bei den Anwendungsfällen, die vom Staat definiert und geregelt sind (e.g. KYC, Auszüge aus dem Strafregister usw.), sollen die Wallets zertifiziert werden und entsprechend die höchste Sicherheitsmechanismen verwenden (z.B. Einsatz von *Secure-Elements* (TPM, HSM, SIM, etc.) und Biometrie). Es braucht aber auch die Möglichkeit, gewisse Credentials (z.B. E-ID) an das Device zu binden, damit es nicht kopiert werden kann.

7. **Wie können Verified Credentials auf mehreren Geräten benutzt werden? Wann wäre dies nötig? Reicht es, wenn mit dem einen Smartphone immer eine Verbindung zum Verifier aufgebaut werden kann, unabhängig davon, auf welchem anderen Gerät man gerade den nach der E-ID-fragenden Prozess initiiert hat?**

Man will seine Credential von den verschiedensten Geräten aus verwenden können. Aber es sollten keine Schlüssel kopiert/dupliziert werden, sondern immer eine Delegation von Rechten (mit abgeleiteten Schlüsseln) vorgenommen werden. In Zukunft, wenn mehr Apps und Dienste nativ SSI (resp. *DIDComm*) implementieren, wird das Abscannen eines QR-Codes immer seltener werden und die Apps kommunizieren mittels DIDComm mit dem lokalen Wallet.
Dies soll im Governance-Framework geregelt werden.

8. **Wer definiert Credential-Schema, braucht es eine ausgewiesene Stelle zur Definition und Koordination (z. B. eCH) oder werden die Definitionen branchenabhängig entwickelt?**

Wie bei aller Kommunikation muss sich die Standardisierung an der Grösse des Ökosystems (resp. Subsystems) ausrichten. Je mehr Stakeholder involviert, desto wichtiger, schwieriger und langwieriger wird die Standardisierung. Aber sie ist zentral für eine Verbreitung und Interoperabilität. Der Bund kann mitgestalten und schlussendlich das Schema für die E-ID festlegen. Aber die Schemata (und Name) der einzelnen Claims (Attribute) muss international abgestimmt sein. Wir erwarten also, dass Branchenorganisationen die Schemadefinitionen der in der Branche autoritativ herausgegebenen Verifiable Credentials in eigener Regie entwickeln und verwalten werden. Der Einsatz dieser Credentials kann in der Folge aber durchaus branchenübergreifend erfolgen (z.B. Befähigungen, Atteste, Diplome, etc.).

9. **Benötigt es überhaupt einen staatlichen Authentifizierungsdienst? Wäre eine Verknüpfung von Ausstellungsprozess und Hinterlegen von Authentifizierungsfaktoren sinnvoll, um vom aufwändigen Identifikationsprozess bei der Ausstellung zu profitieren und um eine hohe Sicherheit beim Authentifikationsprozess zu ermöglichen?**

Spezifisch für die Herausgabe von verifizierbaren Attributen oder «Verifiable Credentials» der Basisidentität (E-ID-Attribute) an Wallets des Nutzers könnte ein solcher

Authentifizierungsdienst sinnvoll sein. Beim Einsatz des Wallets, hingegen, wird kein solcher Authentifizierungsdienst[5] benötigt.

[5] Es braucht keinen staatlichen IdP (der würde viel zu viel mitbekommen). Aber eine lauffähige Komponente (Docker-Image) für Kantone und Gemeinden würde sicher Sinn machen, natürlich OpenSource (ist eh er nur Packaging und Config, analog VON Images)

IV. Kommentare zum Kapitel 5.1.4. - „Nachteile des SSI-Ansatzes“

1. Relativ junger Ansatz, einige Grundsatzfragen sind noch nicht abschliessend geklärt und Standards sind noch nicht komplett.

Ja, der Ansatz ist noch jung, einige Fragen müssen noch geklärt werden. Unseres Erachtens soll dies aber aus zweierlei Gründen den Bund nicht hindern, diesen Ansatz weiterzuverfolgen:

1) Der Ansatz baut auf erprobte kryptographische Verfahren und bewährten Technologien auf, die heute schon in unterschiedlichen Anwendungsfällen genutzt werden.

2) Seit dem Aufkommen des Ansatzes (2015) haben wir eine rasante Entwicklung von Innovation und Verbesserungen gesehen. Ein Richtungsentscheid der Europäischen Gemeinschaft mit ihrer globalen regulatorischen Reichweite und der Schweiz als führende Nation in der Blockchaintechnologie, deren skalierbare Anwendungen allesamt auf ein digitales Vertrauensnetzwerk angewiesen sind, wird die weitere Entwicklung und damit die Lösung der noch offenen Fragen sehr positiv beeinflussen. Wir sind zuversichtlich, auch in Hinblick auf den geplanten Einführungszeitraum der neuen E-ID (2025/26), dass für die heute noch nicht abschliessend geklärten Themen praktikable Lösungsvorschläge vorliegen. Aber SSI funktioniert und kann bereits jetzt verwendet werden. Mit dem Aufbau des Ökosystems resp. der Anwendungen wird das System (und die Bevölkerung) erst erwachsen. Warten ist keine Option.

2. Das breite Bewusstsein für die Möglichkeit dieses ganzheitlichen Ansatzes (im Vergleich zu einem Login) muss zuerst entstehen.

Dies ist Richtig. Dies hat aber weniger mit SSI als vielmehr mit der Digitalisierungskompetenz der Schweizer Bevölkerung und der schweizer Unternehmen zu tun. Hier ist es zwingend notwendig an der Kommunikation zu arbeiten sowie relevante, für die Anwender attraktive Anwendungsfälle zu ermöglichen, respektive zur Verfügung zu stellen.

Momentan werden konkrete Anwendungsfälle mit institutionellen und privaten Akteuren umgesetzt. Dabei wird die kaskadierte Nutzung von Verifiable Credential innerhalb eines Ökosystem demonstriert. Sie zeigen gut das Potential eines SSI-basierten Ökosystems auf. Durch solche Beispiele wird das Bewusstsein gesteigert.

Sofern der Bundesrat in absehbarer Zukunft einen Richtungsentscheid fällt, entsteht bei vielen Firmen in der Schweiz die notwendige Investitionssicherheit und sie werden beginnen, schon vor Inkrafttreten des neuen E-ID Gesetzes, Pilotprojekte und vereinzelte Anwendungsfälle gemäss den SSI-Prinzipen umzusetzen.

Somit hätte die öffentliche und private Hand bereits ab heute die Möglichkeit, einen wesentlichen Beitrag zu einer erfolgreichen Einführung in fünf Jahren zu leisten und ihre Kunden und Kundinnen auf diesen ganzheitlichen Ansatz vorzubereiten.

3. **Die Verantwortung zur Verwaltung von Verified Credentials wird vollständig dem User übergeben, was Hilfeleistungen durch den Issuer praktisch verunmöglicht.**

Die Issuer haben grundsätzlich gewisse, aber begrenzte Möglichkeiten, der Verwaltung der Verified Credentials durchzuführen (sie geben die Verified Credentials heraus und widerrufen sie). Das ist ein Grundsatz im SSI-Ansatz. Die Verwaltung (oder besser gesagt die Nutzung) der Verified Credentials geschieht im Wallet oder durch den Walletanbieter. Abhängig von den individuellen Bedürfnissen bezüglich Sicherheit, Convenience und Privatsphäre werden die User unter verschiedenen Walletanbietern und Wallets wählen können.

Es gibt aber noch eine wenig beachtete vierte Rolle neben Issuer, Holder und Verifier - nämlich die der Agency. D.h. eine Dienstleistung welche ein User/Holder (resp. sein Wallet) nutzt um z.B. Backups, Social Recovery sicherzustellen, oder um eine gewisse Offline-Fähigkeit zu ermöglichen, sprich, dass in seinem Namen (mit delegierten Credentials) gewisse Aktionen durchgeführt werden, auch wenn der User resp. sein (Haupt) Wallet nicht online ist. Die Agency kann auch gleich der Mediator sein, welche sowieso jedes Mobile-Wallet braucht.

Zu berücksichtigen ist jedoch, dass die forensische Auswertbarkeit schwierig ist, da das System dezentral und kryptografisch gut geschützt ist. Dies kann beim Missbrauchsfall der E-ID oder anderen Nachweisen dazu führen, dass es schwierig wird nachzuweisen, dass man etwas «nicht gewesen» ist. Nichtsdestotrotz hilft das kryptografisch gut geschützte und dezentrale System gerade die missbräuchliche Verwendung digitaler Nachweise zu minimieren. Wo es die Sicherheitsanforderungen verlangen, können Verifyingsprozesse auditierbar und datensparsam aufgezeichnet werden. Die grösste Missbrauchsgefahr liegt in der Zugriffskotrolle des Wallets,

weswegen Mindestanforderungen an Hard- und Software (e.g. Biometrics, Secure Element, etc.) zwingend sind.

4. **Hochsichere Wallets für spezielle Anwendungen müssten auf Secure Elements in Smartphones aufbauen. Derzeit sind aber noch nicht alle Smartphones damit ausgestattet und die dazu benötigten Entwicklerwerkzeuge sind noch nicht vollständig und einfach verfügbar.**

Auf jeden Fall braucht eine E-ID ein Wallet mit Secure-Element, ansonsten ist sie beliebig auf andere Devices kopierbar (siehe DE ID-Wallet). Damit sich die digitalen Signaturen (QES) endlich durchsetzen, braucht es die neueste Generation von Smartphones sowieso, welche ein FIPS zertifiziertes Element haben (aktuell etwa 65% der aktuell benutzten Mobiltelefone in der Schweiz).

Die Entwicklung ist aber in vollem Gange und wird nie abgeschlossen sein. Zudem werden die meisten Anwendungen in einem zukünftigen digitalen Vertrauensnetzwerk nicht Hochsicherheitsanwendungen sein. Risikobasierte Mindestanforderungen für Hard- und Software von Wallets, Verifying und Issueing agents und andere Systemkomponenten können höchstmögliche Sicherheit garantieren. Benchmark soll nicht die maximale Sicherheit sein, sondern eine Verbesserung des heute real existierenden Sicherheitsniveaus (Beispiele: Altersverifikation mittels ID eines älteren Geschwisters, Papierdokumente als Ausbildungszeugnisse).

Kommentar zum Kapitel 5.2 - Warum SSI besser als PKI ist

Im Gegensatz zu PKI können bei SSI einzelne Attribute eines Verified Credential präsentiert werden sowie Zero-Knowledge-Proofs. Dies ermöglicht es, den in den Motionen geforderten Datensparsamkeit-Ansatz optimal gerecht zu werden.

Zudem ermöglicht SSI im Gegensatz zu PKI die kombinierte Abfragen aus verschiedenen Verified Credential durchzuführen (z.B. Basis-Identität und Delta-Verified Credential). Somit vermeidet man das Duplizieren von Attributen und erhöht die Aktualität/Qualität der Daten (z.B. Name, Adresse, etc.)

Ein ganz zentraler und wichtiger Punkt ist die sogenannte *Revocation*. Bei der PKI ist das ein zentraler Dienst, welche eine Liste von revozierten Zertifikaten veröffentlicht. Um ihn zu verwenden, braucht es eine Kommunikation mit dem Dienst (OCSP) oder mit der Liste kann ein einmal gesehenes Zertifikat anhand seiner SerialNum getracked werden. Z.B. kann man einmal pro Tag abfragen, ob ein bestimmtes Mitarbeiter-Cert (z.B. CEO) revoziert wird. Im Falle von Sovrin wird dafür ein sog. Kryptographischer-Akkumulator verwendet, welcher im Ledger gespeichert ist. Dieser ist Privacy-Preserving. Und der Proof, dass ein Credential (noch) gültig ist, macht der Holder beim Erstellen eines Proof, und ist auch nur für genau diesen Zeitpunkt gültig.

Die internationale Gemeindschaft (e.g. EU, WHO, IATA, weitere) orientiert sich an souveränen und offenen digitalen Identitätsökosystemen. Somit wäre eine PKI-basierte Lösung eine Schweizer Insellösung.Diese ist im Sinne von Datensparsamkeit, Interoperabilität, Portabilität, der Nutzung von globalen Standards, sowie der nachhaltigen Etablierung einer lokalen Governance auch als Brückenlösung NICHT zu bevorzugen.