DIDAS Stellungnahme
zur
Vernehmlassung BGEID – Oktober 2022

Eingereicht an:
Bundesrätin Karin Keller-Sutter
Vorsteherin des Eidgenössischen Justiz- und Polizeidepartements EJPD
Bundeshaus West
CH-3003 Bern
per Mail an: rechtsinformatik@bj.admin.ch

Eingereicht durch:
Digital Identity and Data Sovereignty Association (www.didas.swiss)
Campus Zug Rotkreuz
Surstoffi 1
CH-6343 Rotkreuz
info@didas.swiss

Sehr geehrte Bundesrätin Keller-Sutter
Sehr geehrte Damen und Herren

Wir bedanken uns hiermit, in Fortsetzung unserer Stellungnahme zum Diskussionspapier «Zielbild E-ID», im Rahmen der Vernehmlassung zum BGEID erneut Stellung nehmen zu dürfen.

Die Digital Identity and Data Sovereignty Association (DIDAS) ist ein gemeinnütziger und nicht gewinnorientierter schweizerischer Verein, der mit dem 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.“

Wir würdigen die offene Vorgehensweise der Bundesverwaltung und die hohe Qualität des Gesetzesentwurfs. Zudem ist das Verständnis und die Anwendung eines prinzipienbasierten, iterativen und kollaborativen Vorgehens, als kritische Erfolgsfaktoren für die Planung und Einführung einer nachhaltigen Vertrauensinfrastruktur, der Etablierung einer elektronischen Identität und weiterer digitaler Nachweise, sowie deren flächendeckende Verwendung, zu würdigen.

Es freut uns ausserordentlich, dass sich DIDAS und seine Mitglieder im vergangenen Jahr wertschaffend in den Prozess einbringen konnte. So ist die vorliegende Stellungnahme als eine Gemeinschaftsarbeit aller Mitglieder des Vereins DIDAS unter der Federführung des Vorstandes anzusehen.

Rotkreuz, im Oktober 2022

Daniel Säuberli Präsident	Ursula Sury Vizepräsidentin	Diego Benz Vorstand
Marco Dütsch Vorstand	Vasily Suvorov Vorstand	Tim Weingärtner Vorstand

I. Rekapitulation/Zusammenfassung unserer Stellungnahme zum Diskussionspapier «Zielbild E-ID» im Jahr 2021

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 Stellungnahme zum Zielbild E-ID kann unter folgendem Link nachgeschlagen werden: https://www.didas.swiss/wp-content/uploads/2021/10/Stellungnahme-DIDAS-FINAL-V1.0-website.pdf

II. Stellungnahme zur Vernehmlassung BGEID

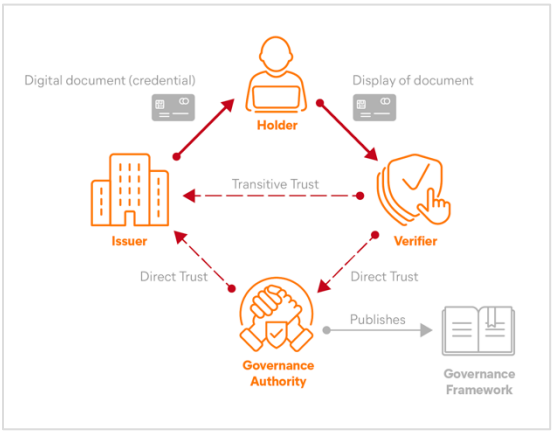
Die in unserer Stellungnahme zum Diskussionspapier E-ID veröffentlichte Meinung hat demnach weiterhin Gültigkeit. Für die nachhaltige Meinungsbildung und Lösungsfindung gelten die SSI-Prinzipien.

Es ist uns zudem ein Bestreben, einen «Balanced-approach» anzuwenden, der eine zeitnahe Etablierung des Ambitionsniveaus 3 ermöglicht und gleichzeitig die nötige Flexibilität im Gesetz verankert, um den sich schnell entwickelnden technologischen Möglichkeiten und der fortschreitenden Digitalisierung (resp. deren Akzeptanz in der Gesellschaft) gerecht zu werden.

Der vorliegende Vorentwurf des Bundesgesetzes enthält die zwingend notwendigen gesetzlichen Grundlagen, ist aber auch genügend offen formuliert und wird deshalb von unseren Mitgliedern als sehr gut beurteilt. Wir sind der Überzeugung, dass der Vorschlag für das E-ID-Gesetz eine solide Basis darstellt und den Rahmen für eine zukunftsträchtige Vertrauensinfrastruktur setzt, in welchem eine staatlich herausgegebene E-ID das Kernelement darstellt. Wir begrüssen die Schaffung eines Rechtsrahmens für diese Vertrauensinfrastruktur.

Die E-ID werden gemäss Vorentwurf BGEID in einigen Belangen als digitale Kopie eines anderen gültigen Ausweises realisiert (Art. 3). Dies betrachten wir nur dann als sinnvoll, wenn dadurch eine Umsetzung substanziell schneller erfolgen kann. Künftige Anpassungen sollen aufgrund der fortschreitenden Digitalisierung die E-ID als eigenständigen Nachweis etablieren können, ohne sich zwingend auf andere Ausweise abzustützen. Dadurch kann z.B. die E-ID einen eigenen Lebenszyklus erhalten und als gleichwertiges Ausweisdokument anerkannt werden, wobei den Inhaberinnen und Inhabern grundsätzlich in jeder Situation die Wahl des Nachweises zu gewähren ist.

In Ökosystemen elektronischer Nachweise kann somit der Staat die Rolle des «Enablers» übernehmen und das Ziel verfolgen, ein attraktives Umfeld für vielfältigste Anwendungen zu schaffen. Der Staat übernimmt zudem die Rolle der Governance Authority im sogenannten «Trust Diamond» und erlässt ein einheitliches Governance Framework.



Ein erfolgreiches Ökosystem elektronischer Nachweise lässt sich jedoch nur gemeinsam mit den beteiligten Aussteller/innen, Verifikator/innen und Inhaber/innen elektronischer Nachweise konzipieren, pilotieren und umsetzen. Um den Reifungsprozess entlang aller involvierter Stakeholder zu beschleunigen (aber auch um den Nutzenden die Möglichkeiten aufzuzeigen), sind explorative Pilotprojekte des Bundes in Zusammenarbeit mit Stakeholdern aus dem privaten

und öffentlichen Sektor von grosser Bedeutung. Damit kann das Ziel verfolgt werden gemeinsam zu lernen, ohne die Wahl spezifischer Technologien bereits in dieser Phase zu präjudizieren. Diese Projekte sollten vom Bund mit den nötigen finanziellen Mitteln ausgestattet werden. Wünschenswert wäre daher die Verankerung einer gemeinsamen Pilotierung mit gemischter Beteiligung der Akteure aus öffentlichem und privatem Sektor entlang einheitlicher Prinzipien, z.B. an geeigneter Stelle auf Verordnungsstufe.

Als weitere Massnahme zur Beschleunigung der Adaption elektronischer Nachweise, empfehlen wir einen weiterhin offenen und partizipativen Prozess und den Einbezug von Expertengruppen in die Gestaltung der Verordnungen und die weitere BGEID-Umsetzung. Eine Organisation wie DIDAS oder andere Expertennetzwerke könnten sich demnach dazu eignen, partnerschaftlich mit bestehenden Gremien und Institutionen wie z.B. Innosuisse, kollaborativ Projekte mit klarem Nutzen zu begleiten resp. zu orchestrieren.

Wir empfehlen es zudem, die im Ökosystem verwendeten Begrifflichkeiten einheitlich und angelehnt an internationale Standards zu definieren, wie z.B. Verifizierer, Vertrauensregister, Basisregister etc. In diesem Zusammenhang sollten auch Rahmenthemen wie Datensparsamkeit nicht im BGEID verankert werden, da sie ohnehin bereits durch bestehende Gesetze wie das DSG Gültigkeit haben. Sie sollten jedoch im Kontext mit neuen technologischen Mechanismen klar definiert werden.

Im Rahmen weiterer elektronischer Nachweise, ist es essenziell, wo möglich einheitliche Standards zu definieren wie auch Unterschiede in sektorieller Governance im Ökosystem zu ermöglichen. So sollen z.B. für eine Wohnsitzbestätigung immer die gleichen Attribute genutzt werden, währenddem in verschiedenen Sektoren unterschiedliche Attribute, z.B. für den Nachweis einer bestimmten Kompetenz (z.B. Spezialisierungen FMH bei Ärzten) verwendet werden sollen. Diese sektoriellen Unterschiede sollen sich möglichst nach internationalen Standards im jeweiligen Sektor ohne “Swiss Finish” richten. Diese Standards sollen durch eine autoritative Instanz in einem offenen und partizipativen 07Prozess verwaltet und kommuniziert werden.

Wir unterstützen zudem das Nutzen der AHV Nummer als einheitlichen Identifikator. Das Nutzen der AHV Nummer muss jedoch zwingend im Gesetz erwähnt werden, damit diese als interne Verifizierung überhaupt verwendet werden darf.

Wir unterstützen eine Ablauffrist für die E-ID, da sie ggf nicht widerrufen wird und auch über ihr Ablaufdatum hinaus als Identifikationsmittel akzeptiert werden könnte. Dabei sollten die technischen Möglichkeiten (z.B. expiration Date) genutzt werden.

DIDAS freut sich auf die weiteren Schritte und empfiehlt eine prioritäre Behandlung im Bundesrat. Weiterhin empfehlen wir das Vorantreiben von technischen Proof of Concepts und Minimal Viable Products (MVPs) unter Einbezug aller Stakeholder und der Zivilgesellschaft, um die vorgeschriebenen Perioden für den politischen Entscheid bestmöglich zu nutzen.

Detailierte Stellungnahme zu relevanten Abschnitten und Artikeln im Vorentwurf:

Artikel	Vorentwurf Bundesgesetz	DIDAS Stellungnahme
1.1	Art. 1 1 Dieses Gesetz regelt: a. den staatlichen elektronischen Identitätsnachweis natürlicher Personen (E-ID) und andere elektronische Nachweise; b. die Infrastruktur zum Ausstellen, Widerrufen, Überprüfen, Aufbewahren und Vorweisen von elektronischen Nachweisen (Vertrauensinfrastruktur); c. die Rollen und Verantwortlichkeiten bei der Bereitstellung und Nutzung dieser Infrastruktur.	Anpassung: a. den staatlichen elektronischen Identitätsnachweis natürlicher Personen (E-ID) und weiterer elektronischer Nachweise
1.2	2 Es hat zum Zweck: a. die sichere Identifizierung mittels E-ID unter Privaten und mit Behörden zu gewährleisten; b. den Schutz der Persönlichkeit und der Grundrechte von Personen zu gewähr- leisten, über die im Zusammenhang mit der Verwendung der E-ID Daten bear- beitet werden, insbesondere durch die Umsetzung der folgenden Grundsätze: 1. Datenschutz durch Technik 2. Datensicherheit, 3. Datensparsamkeit, und 4. dezentrale Datenspeicherung; c. zu gewährleisten, dass die E-ID und die Vertrauensinfrastruktur dem aktuel- len Stand der Technik entsprechen; d. die Standardisierung der E-ID sowie die Sicherheit der Infrastruktur und der Ausstellung und Überprüfung der elektronischen Nachweise zu gewährleis- ten, ohne die technische Entwicklung unnötig einzuschränken.	Ergänzung: e. die Rechtmässigkeit und Gültigkeit von elektronischen Nachweisen in digitalen sowie im physischen Räumen zu ermöglichen und diese auf Basis einer elektronischen Vertrauensinfrastruktur physischen Nachweisen gleichzustellen.
2.3	Sie enthält zudem die folgenden Daten: a. AHV-Nummer; b. E-ID-Nummer; c. Ausstellungsdatum der E-ID; d. Ablaufdatum der E-ID; e. f. SR 142.51 2 / 12 3 4 Angaben zum Ausweis, der im Ausstellungsprozess der E-ID verwendet wurde, insbesondere Typ, Nummer und Gültigkeitsdauer des Ausweises; Angaben zum Ausstellungsprozess	Ergänzung: Art. 25 Technische Entwicklung und fortschreitende Digitalisierung Zu ergänzen 25.3: Der Bundesrat kann vorsehen, der E-ID mit einem eigenen Lebenszyklus bzw. einem direkten Ausstellungsprozess zu versehen, falls die Zivilgesellschaft dies im Rahmen der fortschreitenden Digitalisierung fordert.
4.1	Art 4 Ausstellung 1 Wer eine E-ID will, muss deren Ausstellung dem Bundesamt für Polizei (fedpol) beantragen.	Ergänzung Art 4.5. - Es können zum Ausstellungszeitpunkt mehrere E-ID (oder weitere elektronische Nachweise) ausgestellt werden (z.B. für Multi-Device Unterstützung oder auch um die Ausstellung von Ausweisen minderjähriger an ihre gesetzlichen Vertreter zu ermöglichen).

4.4	4 Zum Zweck der Gesichtsbildverifikation der antragstellenden Person können wäh- rend dem Ausstellungsprozess biometrische Daten erhoben und mit dem Gesichtsbild aus dem ISA oder dem ZEMIS verglichen werden.	Ergänzung: Die biometrischen Daten können nach der Verifikation an einem revisionssicheren Ort ausserhalb des täglichen Zugriffs aufbewahrt werden oder sind zu vernichten.
7.1	Art. 7 Sorgfaltspflicht 1 Die Inhaberin oder der Inhaber einer E-ID muss die notwendigen und zumutbaren Massnahmen treffen, damit ihre oder seine E-ID nicht missbräuchlich verwendet wer- den kann.	Ergänzung Sorgfaltspflicht: Die Ausstellerin der E-ID hat die Pflicht die Inhaberin auf dem aktuellen Informationsstand bezüglich der verantwortungsvollen Nutzung der E-ID in physischen und digitalen Räumen zu halten.
8	Art. 8 Anlaufstellen der Kantone Die Kantone bezeichnen die Stellen, die in Zusammenhang mit der Ausstellung und dem Einsatz der E-ID Unterstützung anbieten.	Ergänzung: Die Ausstellerin stellt die dazu benötigten technischen Schnittstellen einheitlich zu Verfügung.
9	Art. 9 Pflicht zur Akzeptanz der E-ID Jede Behörde oder andere Stelle, die öffentliche Aufgaben erfüllt, muss die E-ID ak- zeptieren, wenn sie eine elektronische Identifizierung vornimmt.	Art 9 und 10: Die Freiwilligkeit der Nutzung der E-ID für Inhaberinnen und die Pflicht zur Akzeptanz der E-ID durch Träger öffentlicher Aufgaben sollen möglichst umfassend gelten. Die Akzeptanzpflicht soll sich auch auf Prozesse erstrecken, bei denen eine Person persönlich erscheint.
10	Art. 10 Vorweisen einer E-ID Wer in einem Prozess einer Person, die persönlich erscheint, die Möglichkeit bietet, die E-ID oder Teile davon vorzuweisen, muss dieser Person die Wahl lassen, sich stattdessen mit einem Ausweisdokument nach dem AwG6, einem Ausländerausweis nach der Bundesgesetzgebung über Ausländerinnen und Ausländer, Integration und Asyl oder einem Ausweis nach Artikel 13 Absatz 1 des Ausländer- und Integrations- gesetzes vom 16. Dezember 20057 auszuweisen, sofern die Anforderungen insbeson- dere an die Sicherheit des Prozesses auch auf diese Weise erfüllt werden können.	Anpassung: Die Inhaberin einer E-ID kann bei einer Interaktion in der physischen Welt nicht dazu verpflichtet werden, sich mithilfe der E-ID auszuweisen. Sie kann sich stattdessen mit einem gleichwertigen gültigen Ausweis gemäss AwG oder einem Ausländerausweis nach der Bundesgesetzgebung über Ausländerinnen und Ausländer, Integration und Asyl oder einem Ausweis nach Artikel 13 Absatz 1 des Ausländer- und Integrationsgesetzes vom 16. Dezember 2005 ausweisen.

13.1	Art. 13 Widerruf 1 Die Ausstellerinnen können die von ihnen ausgestellten elektronischen Nachweise widerrufen.	Ergänzung: Inhaber können die erhaltenen elektronischen Nachweise ohne Kenntnis der Ausstellerin löschen.
13.2	2 Sie widerrufen diese unverzüglich, wenn: a. die Inhaberin oder der Inhaber dies verlangt; b. die gesetzliche Vertretung von Minderjährigen bis zum vollendeten vierzehn- ten Lebensjahr oder von Personen unter umfassender Beistandschaft dies ver- langt; c. der begründete Verdacht auf Missbrauch des elektronischen Nachweises be- steht;	Ergänzung: Es sollte auch möglich sein, nicht—revozierbare elektronische Nachweise auszustellen, ggw benötigen diese den Konsensus der Inhaberin und Ausstellerin beim Ausstellungsprozess.
14	Art. 14 Form und Aufbewahrung von elektronischen Nachweisen Die Inhaberin oder der Inhaber erhält den elektronischen Nachweis als Datenpaket und bewahrt ihn mithilfe selbst gewählter technischer Mittel unter ihrer oder seiner alleinigen Kontrolle auf.	Art. 14 Form und Aufbewahrung von elektronischen Nachweisen Die Inhaberin oder der Inhaber erhält den elektronischen Nachweisen als Datenpakete und bewahrt sie mithilfe selbst gewählter technischer Mittel unter ihrer oder seiner alleinigen Kontrolle auf. Ergänzung: Die technischen Mittel, insbesondere elektronische Brieftaschen, müssen Zertifizierungsanforderungen erfüllen, falls die E-ID mit anderen elektronischen Nachweisen in derselben Brieftasche interagieren soll. oder: Die technischen Mittel, insbesondere elektronische Brieftaschen, müssen Zertifizierungsanforderungen erfüllen, falls eine E-ID darin gespeichert ist oder gespeichert werden kann.
15.1	Art. 15 Übertragbarkeit von elektronischen Nachweisen 1 Elektronische Nachweise können nicht einer anderen Inhaberin oder einem anderen Inhaber übertragen werden.	Input: Im Falle einer gesetzlichen Vertretung soll für den Vertreter ein elektronischer Nachweis ausgestellt werden können, der ihn als Vertreter eines Subjekts resp. Inhabers ausweist. Des Weiteren sollen Mechanismen zur Verfügung gestellt werden können, die es einem Vertreter ermöglichen im Namen eines vertretenen Subjekts zu handeln. Dies soll für personenbezogene elektronische Nachweise gelten.
16	Art. 16 Vorweisen von elektronischen Nachweisen	Ergänzung 16.4: Verifikatoren dürfen im Sinne der Datensparsamkeit zu jedem Zeitpunkt nur die Daten abfragen, welche für die Erfüllung des jeweiligen kommunizierten Geschäftsfalls im Sinne des Inhabers nötig sind. —–> Wird im Datenschutzgesetz bereits zu genüge abgedeckt, sollte ggf im digitalen Raum in Zusammenhang mit der E-ID jedoch speziell behandelt werden.

16.2	2 Das Vorweisen und Überprüfen eines elektronischen Nachweises erfolgt ohne dass die Ausstellerin davon Kenntnis hat.	Anpassung: 2 Das Vorweisen und Überprüfen eines elektronischen Nachweises erfolgt ohne dass die Ausstellerin oder dritte davon Kenntnis haben, ausser der Inhaber erwünscht dies explizit. Ergänzung 16.4. Ein expliziter Wunsch muss für jeden Geschäftsfall einzeln geäussert werden. Deren Verweigerung darf durch die Ausstellerin oder Verifikatorin nicht als Hindernis für den Bezug eines bestimmten Dienstes verwendet werden.
17.1	1 Der Bund stellt ein öffentlich zugängliches Register (Basisregister) zur Verfügung, das Daten enthält über: a. die Ausstellerinnen elektronischer Nachweise; b. die Verifikatorinnen; c. den Widerruf von elektronischen Nachweisen.	Input: Die Daten der Verifikatorinnen müssen nicht zwingend im Basisregister publiziert werden.
17.3	3 Die Ausstellerinnen und Verifikatorinnen tragen ihre Daten in das Basisregister ein.	Input: Diese Eintragungen müssen freiwillig sein. Es besteht Wahlmöglichkeit für die eingesetzten Wallets, aber auch bei der Wahl der Issuer und Verifier. Somit könnten auch Issuer oder Verifier gewählt werden, die andere Basisregister (als das hier geregelte) oder andere Methoden verwenden. Dies ist auch in Bezug auf eine Internationalisierung wichtig.
18	Art. 18 System zur Bestätigung von Identifikatoren	Input: Diese Begrifflichkeit erscheint uns sehr umständlich. Wir schlagen den Begriff "Vertrauensregister" vor.
18.2	2 Der Bundesrat kann vorsehen, dass der Bund auch die Zuordnung von Identifikatoren und Schlüsseln von privaten Ausstellerinnen und Verifikatorinnen bestätigt.	Input: Aus unserer Sicht ist der Einbezug bzw. die Zulassung und Bestätigung von ausgewählten privaten Ausstellerinnen und Verifikatorinnen für ein erfolgreiches E-ID-Ökosystem zwingend notwendig. Dies darf daher nicht nur als Möglichkeit formuliert werden. So soll die Rolle von Akkreditierungsstellen bereits frühzeitig ermöglicht werden und z.B. Daten aus relevanten Registern (z.B UID-Register, dem Handelsregister, etc.) weiterverwendet werden.

23	Art. 23 Quellcode der Vertrauensinfrastruktur Der Bund veröffentlicht den Quellcode der von ihm zur Verfügung gestellten Elemente der Vertrauensinfrastruktur.	Ergänzung: und die Rechte Dritter gewahrt werden.
26.1	Art. 26 1 Die Ausstellerinnen und Verifikatorinnen elektronischer Nachweise entrichten für ihre Einträge im Basisregister und im System zur Bestätigung von Identifikatoren eine Gebühr.	Ergänzung: Die Preisgestaltung, insbesondere für Einträge in das Basisregister, hat moderat zu erfolgen.
27	Art. 27 Internationale Abkommen	Ergänzung 27.3: Es ist sicherzustellen, dass sich die benötigten technischen Mittel zur Erfüllung der Verträge im Sinne dieses Bundesgesetzes bereits gestellt werden und die Prinzipien von Privacy-by-design, der Offenheit (Code), Interoperabilität und Portabilität von digitalen Nachweisen in verbundenen Netzwerken beibehalten werden.

Die Stellungnahme ist eine Gemeinschaftsarbeit 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:

adnovum	acrea making digital work	ALPINUM LAW
Berner Fachhochschule Haute école spécialisée bernoise Bern University of Applied Sciences	OPEN BANKING PROJECT.CH BEI Business Engineering Institute St. Gallen	cardossier
With input from EPFL	Swiss Data Alliance	DRAKKENSBERG AG
DSwiss SECURE DIGITAL SERVICES	esatus	HIN
HSLU Hochschule Luzern	INACTA.	KAISER ODERMATT & PARTNER ADVOKATUR & NOTARIAT
kimura	DIE POST	procivis e-government as a service
SICPA	Stadt Zug	SCION ASSOCIATION
swisscom	Crypto Valley	SWITCH
TRUST SQUARE BEYOND TECHNOLOGY SWISS MADE	Vereign	walkerproject inspiration. impact.