Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Justiz- und Polizeidepartement EJPD

**Bundesamt für Justiz BJ**
Direktionsbereich Zentrale Dienste
**Erreur ! Aucune variable de document fournie.**

November 2021

# Öffentliche Konsultation zum «Zielbild E-ID»

## Übersicht über das Ergebnis der öffentlichen Konsultation

**Inhalt**

## *Zusammenfassung*

*Die öffentliche Konsultation zum «Zielbild E-ID» dauerte vom 2. September bis zum 14. Oktober 2021. Im Rahmen der Konsultation reichten 60 Teilnehmende eine Stellungnahme ein. Fast die Hälfte sieht mit dem Neuanlauf für die E-ID die Chance, die Vision einer digitalen Vertrauensinfrastruktur auf Ambitions-Niveau 3 anzugehen (7 Kantone, 2 Parteien, 14 Organisationen, 2 Hochschulen und 4 Unternehmen). Die E-ID ist in einem solchen Ökosystem nur ein digitaler Nachweis unter vielen, in den Stellungnahmen Genannten. Als zugrundeliegender Technologieansatz wird von einer Mehrheit ein «Self-Sovereign Identity»-Ansatz explizit präferiert (8 Kantone, 2 Parteien, 11 Organisationen, 2 Hochschulen und 8 Unternehmen). Nebst den Erwartungen an eine sehr Benutzerfreundliche Anwendung und eine internationale Interoperabilität steht eine Mehrheit hinter den Werten «Privacy by Design» und «Datenhoheit beim Benutzer», fast die Hälfte erwähnt «Datensparsamkeit» explizit. Die Standpunkte zu weiteren Aspekten waren divers, aber reichhaltig für die kommenden, weiteren Diskussionen. Generell waren die Stellungnahmen optimistisch und stark mit Fokus auf die Chancen gerichtet, welche sich in der aktuellen Situation bieten.*


# 1 Allgemeines

Am 2. September 2021 wurde die öffentliche Konsultation zum Diskussionspapier zum «Zielbild E-ID» im Rahmen eines Beiratstreffens unter der Leitung von Bundesrätin Karin Keller-Sutter eröffnet. Mit einer öffentlichen, konferenziellen Diskussion am 14. Oktober 2021 wurde die Konsultation abgeschlossen.

Dieser Auswertungsbericht bezieht sich ausschliesslich auf die schriftlich eingegangenen Stellungnahmen. Aufgrund des engen Zeitplans und der damit verbundenen kurzen Frist zur Einreichung von Stellungnahmen wurden alle Stellungnahmen berücksichtigt, welche bis zum 4. November 2021 beim Bundesamt für Justiz eingetroffen sind. In diesem Bericht sind die eingereichten Stellungnahmen zusammengefasst.

Zur Stellungnahme eingeladen wurden die Kantone, die in der Bundesversammlung vertretenen Parteien, die auf gesamtschweizerischer Ebene tätigen Dachverbände der Gemeinden, Städte, Berggebiete und der Wirtschaft sowie weitere interessierte Organisationen und Unternehmen.

Stellung genommen haben 16 Kantone[1], 4 politische Parteien, 21 Organisationen, 3 Hochschulen und 16 Unternehmen. Insgesamt bezieht sich der vorliegende Bericht auf 60 Stellungnahmen. Eine Organisation (Schweizerischer Arbeitgeberverband) hat ausdrücklich auf eine Stellungnahme verzichtet.

Das zur Konsultation vorgelegte Diskussionspapier zum «Zielbild E-ID» stellt eine Auslegeordnung dar. Es führt die politischen Forderungen (Motionen) auf, stellt mögliche Definitionen und Dimensionen für eine zukünftige Schweizer E-ID und der damit verbundenen Infrastruktur in den Raum und breitet drei technische Lösungsansätze aus.

[1] Die Kantone Glarus und Waadt haben je zwei Stellungnahmen eingereicht. Diese wurden in der Auswertung jeweils zu einer Stimme zusammengefasst.

Um eine Auswertbarkeit der Stellungnahmen zu ermöglichen, wurden insbesondere drei Aspekte abgefragt:

- Welches sind die drei wichtigsten Anforderungen an eine staatliche E-ID als digitaler Ausweis?
- Welche Anwendungsfälle der E-ID stehen im Vordergrund?
- Welchen Nutzen bietet eine nationale Infrastruktur, die es dem Staat und Privaten ermöglicht, digitale Beweise (z. B. E-ID, digitaler Führerausweis, Mitarbeiteraus-weise, Ausbildungsnachweise) auszustellen und überprüfen zu können?

# 2 Verzeichnis der Konsultationsteilnehmenden

Ein Verzeichnis der Kantone, Parteien, Organisationen, Hochschulen und Unternehmen, die an der Konsultation teilgenommen haben, sowie der verwendeten Abkürzungen findet sich im Anhang.

# 3 Allgemeine Bemerkungen

## 3.1 Prozess und Diskussionspapier zum «Zielbild E-ID»

Das vom Bundesamt für Justiz gewählte Vorgehen mit der Erarbeitung eines Diskussionspapiers zum «Zielbild E-ID» und einer anschliessenden, öffentlichen Konsultation wurde durchwegs positiv aufgenommen, fast die Hälfte (26) hat sich explizit positiv zum Prozess oder zum Inhalt des Diskussionspapiers geäussert. Die Tatsache, von Anfang an die öffentliche Meinung abzuholen und damit breite Kreise in die Entwicklung miteinzubeziehen, wurde geschätzt. Es besteht der Wunsch von einigen Teilnehmenden, eine aktive Partizipation auch in kommenden Prozessschritten zu ermöglichen.

## 3.2 Ambitions-Niveau

Das Ambitions-Niveau 3 als finale Zielgrösse wird von fast allen Teilnehmenden genannt, welche sich explizit zum Ambitions-Niveau geäussert haben (29 von 31). Stellvertretend für viele definiert *digitalswitzerland* den Grund folgendermassen: «Der grösste Nutzen im Sinne eines volks- und betriebswirtschaftlichen Mehrwerts resultiert, wenn eine vertrauenswürdige, sichere und erweiterbare digitale Infrastruktur geschaffen wird.»

Ein schrittweiser Ausbau – von Ambitions-Niveau 1 auf 2 auf 3 – ist durchaus für einige Teilnehmende denkbar. *GLP* und *LU* begrüssen einen schrittweisen Ausbau dann, wenn es für die Umsetzungsgeschwindigkeit förderlich wäre.

*CloudTrust* spricht sich dediziert für Ambitions-Niveau 2 aus mangels in der Schweiz vorhandener Erfahrung, *FR* spricht sich für Ambitions-Niveau 1 aus.

## 3.3 Technologieansatz

Eine Mehrheit der Teilnehmenden (31) sieht den Technologieansatz «Self-Sovereign Identity» (SSI) als den bestmöglichen zur Erfüllung der geforderten Werteversprechen und Funktionen an. Von explizit genannten Präferenzen ist es sogar die grosse Mehrheit (31 von 38). Für *BFH* und *Vereign* ist es sogar der einzig mögliche Ansatz zur Erfüllung der Forderungen. *VD (DGS)* und *Switch* sehen kein Problem darin, dass SSI heute eine junge Technologie ist, weil bis zu einer möglichen Inbetriebnahme zusätzlich an Maturität gewonnen haben wird. *esatus* hält auf die stärkere Verantwortung der Benutzer beim SSI-Ansatz fest: «Bei SSI gehen Kontrolle und

Verantwortung an die Nutzer/innen über. Das müssen sie verstehen, daran müssen sie sich gewöhnen». *procivis* empfiehlt, dass begonnen werden muss, alle Stakeholder eines solchen Ökosystems von den Vorteilen von SSI zu überzeugen mittels einer konsequenten Kommunikations- und Ausbildungsstrategie. *GE* sieht ebenfalls den Bedarf von Kommunikationsmassnahmen zur Sensibilisierung und Akkulturation bei der Einführung eines souveränen Ansatzes.

Eine Umsetzung mittels «Public Key Infrastructure»-Ansatz (PKI) würde von einigen ebenfalls in Betracht gezogen, aber nur von *k§rm, SAV* und *swimag* als präferierten Ansatz genannt. Für die *Digitale Gesellschaft* ist die Nutzung des PKI-Ansatz als Übergangstechnologie zu SSI denkbar.

Eine E-ID-Lösung mittels Identity Provider (IdP) wird von den 3 Kantonen *AG*, *FR* und *GL* als präferierten Ansatz genannt. Der IdP-Ansatz wird aber von anderen Teilnehmenden als «nicht zukunftsfähig» bezeichnet und es wird breit anerkannt, dass der Ansatz die Forderungen der Motionen nicht vollständig erfüllen kann. Für *GE* ist eine Zwischenlösung mit föderierten, kantonalen Identitäten denkbar, bis eine zugängliche, sichere und souveräne Bundeslösung bereitsteht.

22 Teilnehmenden machten keine explizite Aussage zum präferierten Technologieansatz.

Zum Sicherheitsaspekt, ob bei der Umsetzung auf ein Hard-Token (physisches Gerät/Element zur Aufbewahrung von digitalen, privaten Schlüsseln) zurückgegriffen werden soll, sprachen sich *BE, BL, DIDAS, FR, Procivis, Sicpa, Swisscom* und *ZH* gegen ein Hard-Token aus zugunsten der Benutzerfreundlichkeit. Für die *Digitale Gesellschaft, Grüne* und *Threema* führt für eine sichere E-ID kaum ein Weg an einem physischen Token vorbei.

Unabhängig vom Ansatz fordert die *Piratenpartei* eine Geräteportabilität der E-ID.

# 4 Stellungnahmen zu den Hauptfragen des Diskussionspapiers

## 4.1 Wichtigste Anforderungen an die E-ID als digitaler Ausweis (Werte)

Unbestritten ist die in den Motionen geforderte Ausstellung der E-ID durch den Staat. Mehr als die Hälfte der Teilnehmenden (35) hat sich explizit dafür ausgesprochen. 26 Teilnehmende haben sich positiv zum Betrieb durch den Staat der dafür nötigen Systeme geäussert.

Benutzerfreundlichkeit wurde als Anforderung am Häufigsten genannt (41). Es wird von der grossen Mehrheit eine einfach nutzbare, simpel zu bedienende Lösung gewünscht. Viele Teilnehmenden (28) erwähnen, dass die einfache Nutzung mit einem einfachen Onboarding beginnen muss, *SSV* drückt es stellvertretend so aus: «[Die E-ID] soll für die Benutzer tiefe Einstiegshürden aufweisen […] sowie einfach und schnell einzurichten bzw. zu erneuern sein». Miteinzubeziehen in den Aspekt der Benutzerfreundlichkeit ist ebenfalls die von *BE, esatus, GE, SDA, swimag* und *Swico* geforderte barrierefreie Umsetzung.

«Die Thematik des Datenschutzes sowie der Schutz der Privatsphäre sind in das Zentrum der Öffentlichkeit gerückt und werden auch in Zukunft an Bedeutung zunehmen» schreibt *economiesuisse* und unterstreicht damit die Anforderung einer grossen Mehrheit (37) nach einer transparenten Lösung mit hohem Datenschutz. Privacy by Design (35) und eine hohe Benutzerkontrolle (Datenhoheit) (34) finden ebenfalls explizit Erwähnung durch die Mehrheit, die Datensparsamkeit von der Hälfte (31). *DuoKey* hebt zusätzlich die Wichtigkeit von Zero-Knowledge-Proofs hervor.

Die in den Motionen geforderte dezentrale Datenspeicherung respektive dezentrale Architektur wurde von 21 Teilnehmerinnen als wünschenswert aufgeführt. Der Aspekt kam in den Stellungnahmen jedoch deutlich weniger hervor als die oben genannten Grundprämissen.

Um Vertrauen in die E-ID zu entwickeln, fordert die Mehrheit (35) eine hohe Sicherheit der E-ID und des damit genutzten Systems. Für viele (24) ist zudem zentral, dass die Integrität und Aussagekraft einer E-ID sichergestellt ist. «Überdies muss im Falle eines Integritätsverlustes oder eines Angriffs auf das Trägersystem eine Revozierung durch den Besitzer der E-ID jederzeit möglich sein» äussert sich *AG* und auch weitere merken an, dass eine durchdachte Revokation einer E-ID möglich sein muss (6).

Punkto Umsetzung spricht sich mehr als die Hälfte (33) dafür aus, das System auf internationalen Standards basierend und mit offenen Schnittstellen aufzubauen. *CloudTrust*, *HIN* und *Swico* fordern dabei eine Umsetzung «ohne Swiss Finish». 10 Teilnehmenden äussern zudem, dass Open Source Software genutzt respektive Entwicklung als Open Source Software gemacht werden soll. Zum Investitionsschutz auf Seiten der Kantone wird von einigen (6) eine Kompatibilität mit existierenden kantonalen Systemen verlangt.

Als Erfolgsfaktor wird von der Hälfte (30) eine gute Verbreitung und ein «Ankommen im Alltag» gesehen. Für *Switch* ist dabei klar, dass dafür eine Ausweitung der Anwendung über E-Government hinausgehen sollte. Für *SB* gehört eine zügige und niederschwellige Verbreitung in den Vordergrund gestellt.

Eine E-ID und deren Nutzung soll kostenlos sein, sowohl für den Bürger wie idealerweise auch für den Leistungserbringer (Relying Party, Verifier) findet ein gutes Drittel der Teilnehmenden (17). Niemand der Teilnehmenden sprach sich für eine Kostenbeteiligung durch den Nutzer aus. Für die *Grünen* und *k§rm* darf die E-ID und die gesamte digitale Basis-Infrastruktur des Staates nicht mit einem Geschäftsmodell verbunden sein.

*BL* und *privatim* merken an, dass eine Gewichtung der Kriterien unabdingbar ist, da sonst eine erhebliche Gefahr besteht, dass nicht vereinbare Anforderungen umgesetzt werden sollen und am Ende erneut keine taugliche Lösung zur Verfügung steht.

Klar gefordert wird von fast zwei Dritteln der Teilnehmenden (39), ohne konkrete Anwendungsbedürfnisse zu nennen, eine Kompatibilität respektive Interoperabilität mit europäischen und internationalen digitalen Identitäts-Ökosystemen.

## 4.2 Anwendungsfälle der E-ID (Funktionen)

Für die grosse Mehrheit (48) ist die E-ID ein digitaler Ausweis, dessen Primärfunktion der Identitätsnachweis ist; sowohl online (48) wie auch zur Nutzung in der analogen Welt (35). Das Bedürfnis nach Identifikationsnachweis wurde konkret für den Altersnachweis (17), die Bestellung von Registerauszügen (17), Bankkonto-Eröffnungen (11), die Bestellung Wohnsitzbescheinigungen (6) und Mobiltelefon-Abonnement-Abschlüssen (6) geäussert.

Die Nutzung einer E-ID für den Zugang zu E-Government-Anwendungen wurde ebenfalls von mehr als der Hälfte (35) gefordert. Dabei soll die E-ID das Onboarding für Plattformen erleichtern oder aber als Login genutzt werden können. *BE* und *VD (DGS)* wollen vermeiden, dass der Nutzer unterschiedliche Logins für E-Government und EPD führen muss. *CloudTrust* fordert vor diesem Hintergrund eine Zusammenführung von ZertES und Identitätsregulierung EPD mit dem neuen E-ID-Gesetz, *SB* eine Harmonisierung der E-ID mit der Identifikation unter VSB. SAV weist auf zusätzliche Bedürfnisse im Rahmen von eJustice 4.0 hin.

22 Teilnehmenden sprechen sich dafür aus, dass auch private Dienste auf die E-ID als Login zurückgreifen können sollen. *KS* fordert dem entgegen explizit keine Login-Möglichkeit für Online-Dienste von Privaten. *Switch* sieht das Login generell nicht als Aufgabe der E-ID.

Eine Mehrheit der Teilnehmenden (31) fordert, dass mit der E-ID die digitale Signatur respektive die qualifizierte elektronische Signatur ermöglicht oder vereinfacht wird. Es ist vielen ein Anliegen, diese Möglichkeit endlich in die Breite zu bringen. Für *SCTO* und *unimedsuisse* steht

die qualifizierte elektronische Signatur sogar zuoberst auf der Prioritätenliste (Konsent-Signatur, Willensbekundungen).

Die Nutzung der E-ID für E-Voting (5) und E-Collecting (5) wurden vereinzelt genannt.

Augenscheinlich ist die Vielzahl der genannten Anwendungsfälle, welche nicht direkt mit der E-ID und deren Identifikation zu tun haben. Unter der weiter oben beschriebenen Vision eines Ambitions-Niveau 3 ist dies jedoch konsequent. Digitale Führerausweise (17), Zugangsmittel auch für physische Örtlichkeiten (15), Ausbildungsnachweise und Arbeitszeugnisse (14), Mitarbeiter und Mitgliederausweise (13), Vollmachten/Auskunftsrechte (4) und daneben Nennungen von 37 Teilnehmenden für weitere digitale Nachweise aller Art wurden als mögliche oder nötige Elemente gefordert um die Digitalisierung in der Schweiz voranzubringen. Für die *ZHAW* ist die Sicht zudem nicht auf Personen beschränkt, sondern erstreckt sich weiter über Organisationen und Dinge.

## 4.3 Nutzen einer nationalen Vertrauensinfrastruktur für vom Staat und Privaten ausgestellte digitale Beweise

Fast philosophisch stellt *govtechpodcast* die Frage: «Welche öffentlichen Güter – analoge und digitale, Güter, Dienstleistungen und Infrastrukturen – muss der Staat bereitstellen, um ein freies und zugleich solidarisches Zusammenleben zu ermöglichen?»

Die Stellungnahmen liefern eine mögliche Antwort: Die Breite der gewünschten Anwendungsfälle und die Forderung für ein Ambitions-Niveau 3 decken sich mit dem mehrheitlichen Wunsch (34), eine Infrastruktur zu schaffen, die eine breite Nutzung für digitale Nachweise aller Art zulässt, unter welchen die E-ID nur noch einer von vielen Nachweisen darstellt.

*Swisscom* sieht im aktuellen Anlauf zur nationalen E-ID eine grosse Chance, ein umfassendes Vertrauensökosystem zu etablieren. Gemäss *Post* reduziert eine gemeinsame Basis für Markt-Teilnehmenden die Komplexität der Nutzen- und der Aufwandseite. Mehr als die Hälfte (32) verspricht sich von einer nationalen, digitalen Vertrauensinfrastruktur Kostenvorteile, Effizienzsteigerungen und eine Vereinfachung heutiger Prozesse. *SB, ZH und ZHR* sehen die Vorteile einer nationalen Infrastruktur nebst einer Aufwandreduktion auch in der Minimierung von Fehlerquellen respektive in der Verbesserung der Datenqualität. In Bezug auf die Nutzer eines Ökosystems erwähnt *SH*, dass die Anwender/innen aus der Wirtschaft von digitalisierten Prozessen ungleich stärker profitieren können als Privatpersonen. Und *NE* sieht sogar einen ökologischen Aspekt einer nationalen Infrastruktur, weil dadurch der Strassenverkehr reduziert werden könnte.

*SBB* stellt dazu die Anforderung, dass die vom Bund gewährleistete Vertrauensinfrastruktur einen Wettbewerb innovativer Kundenlösungen im Ökosystem digitaler Nachweise erlaubt. Für *ti&m* bietet ein «Trust Network» ein hohes Innovations- und Entwicklungspotenzial für den Wirtschaftsstandort Schweiz. 14 Teilnehmenden fordern Offenheit für Aussteller und Überprüfer. *Switch* fordert dabei maximale Offenheit in der Anwendung, also keine Einschränkungen für Relying Parties (Verifier) und Offenheit im Einschluss von Attributsausstellern (Issuer) unter einer zu definierenden Governance.

Mehrere Teilnehmende (7) merken an, dass mit einer gemeinsamen Infrastruktur eine effiziente und flexible Weiterentwicklung möglich wird. *TG* erwähnt dabei noch speziell die höhere Ausbreitungsgeschwindigkeit von Weiterentwicklungen und Erweiterungen.

Von vielen Teilnehmenden wurde zudem genannt, dass gleiche Standards und die damit verbundene gleichartige Anwendung Nutzen schaffen (18) und eine gemeinsame Infrastruktur

Skaleneffekte nutzbar macht (16). Auch wird die Integration von digitalen Nachweisen in bestehende Systeme als einfacher eingeschätzt (13) und ein genereller Sicherheitsgewinn (12) erwartet.

Gemäss der Meinung von 24 Teilnehmenden kann eine gemeinsame, digitale Infrastruktur das Vertrauen der Bevölkerung «ins Digitale» verstärken. Als wichtig dafür wird erwähnt, dass die Infrastruktur mit dem erwarteten Vertrauensanker Rechtssicherheit für alle Beteiligten mit sich bringt, sofern die Infrastruktur langfristig gedacht ist und eine gesamtheitliche Governance angewendet wird (25).

Fragen zur Rollenverteilung der Umsetzung einer Infrastruktur standen noch nicht im Zentrum des Diskussionspapiers zum «Zielbild E-ID». Für die *HSLU* ist aber bereits klar, dass der Bund nicht alle dort aufgeführten Komponenten entwickeln oder zur Verfügung stellen muss. Und die *Piratenpartei* fordert, die staatliche Infrastruktur auf ein technisches Minimum zu beschränken. Der *SGV* findet die Wallet-Idee gut, will aber keine Lösung aus Staatshand. Für *VD* ist gesetzt, dass der Staat für das Gesamtsystem und dessen Betrieb sorgen muss.

# 5 Bemerkungen zu weiteren Aspekten

## 5.1 Gesetzgebung

Knapp ein Viertel der Teilnehmenden (14) fordert eine technologieneutrale Gesetzgebung. *NW* und *OW* begründen es stellvertretend für einige so: «Ein technologieneutraler Rechtsrahmen wird begrüsst, um eine einfache Weiterentwicklung zu ermöglichen.»

Für die *SP* ist es ein Anliegen, dass weder ein direkter noch ein indirekter Zwang zur Nutzung der E-ID entsteht. *Swico* möchte beim Bund viele Kompetenzen ansiedeln und eine Delegation an kantonale Stufen auf das Notwendigste beschränken. Und *swimag* weist auf die Wichtigkeit der Rechtsdurchsetzung von bestehenden Datenschutzgesetzen hin.

*SDA* bringt ein, dass durch die vorgängige Definition von Ambitions-Niveau und Lösungspräferenz ein Präjudiz für die Rechtssetzung geschaffen werde und dass durch mögliche Umsetzungen parallel zum Gesetzgebungsprozess beschaffungsrechtliche Herausforderungen entstehen können.

## 5.2 Governance

Direkte Fragen zur Governance hat das Diskussionspapier zum «Zielbild E-ID» nicht gestellt. *ZH* verortet die Governance beim Bund. *digitalswitzerland* rät, die Gesamtkontrolle für die Entwicklung des ganzen Ökosystems nicht einer einzelnen Instanz anzusiedeln. *DIDAS* fordert eine klare Rollentrennung Staat/Privat. Governance-Fragen bereits in der Konzeptionsphase zu bedenken, empfiehlt *esatus*.

Zur Standardisierung der Credentials sollten nach *Switch* Sektor-Organisationen einbezogen werden, nur so liessen sich viele Anwendungsfälle ohne bilaterale Vereinbarungen zwischen Aussteller und Prüfer schaffen.

*Threema* regt an, dass Kommunikationskanäle und Prozesse zum Melden und Beheben von Sicherheitslücken definiert sein müssen.

Die richtige Governance zu finden, wird von *IG Health* so beschrieben: «Balanceakt zwischen notweniger Regulierung, die Vertrauen schafft, und flexibler Lösung, welche den Aufbau und die dynamische Entwicklung von privaten und öffentlichen Ökosystemen zulässt.»

## 5.3 Risiken

Von den Teilnehmenden wurden unterschiedliche Hinweise auf mögliche Risiken geäussert: *KS* sieht durch die generelle Verlagerung ins Digitale eine Gefahr zur noch stärkeren Einschränkung von Öffnungszeiten und Ämtern. Es solle dadurch nicht zu einem Abbau oder zu einer Verteuerung von staatlichen Dienstleistungen kommen. *SGV* sieht einen noch schwachen Einbezug der Privatwirtschaft im Projekt und die lange Dauer bis zur Einführung einer E-ID als Risiko. *Threema* rät, die E-ID nicht zu überladen, um die Komplexität nicht unnötig zu erhöhen.

*ZH* weist mit Nachdruck auf datenschutzrechtliche Voraussetzungen hin (u.a. Profiling, Verwendung von Personendaten) und dass diese Thematik noch diskutiert werden muss. *NEDIK* fordert eine Priorisierung des Daten- und Systemschutzes, weil bei Mängeln kein Nutzen für die Nutzer gestiftet werden kann, sondern im Gegenteil zusätzliche Risiken geschaffen werden.

Zum jungen Technologieansatz SSI ist vielen klar, dass noch Grundsatzfragen geklärt werden müssen. *nets* gibt zu bedenken, dass SSI zu einem teuren Experiment werden könnte.

## 5.4 Weitere Hinweise

*BE* findet es wichtig, in der Kommunikation um die E-ID alle Altersklassen anzusprechen. Darunter ist nicht die einseitige Informationsbereitstellung zu verstehen, sondern auch, dass auf Social Media gestellte Fragen und Anregungen ernstgenommen, beantwortet und – wo sinnvoll – berücksichtigt werden.

In Bezug auf das Alter empfehlen *SH* und *Sicpa* das Augenmerk zusätzlich auf die Frage nach dem vorausgesetzten Alter für den Einstieg in die Welt der digitalen Identität zu legen. Einerseits ist das Smartphone in der Oberstufe im Alltag der Schüler angekommen, andererseits gibt es Fragestellungen zur Authentifizierung mittels biometrischen Systemen.

Stellungnahmen mit detaillierteren Antworten zu SSI-spezifischen Fragestellungen wurden von *DIDAS*, *DuoKey* und *SFTI* eingereicht. Zur Nachvollziehbarkeit des Nicht-Gewesen-Sein in einem dezentralen System weist *vereign* auf die Möglichkeit eines beim Benutzer geführten Blockchain-Audit-Trails hin.

## 5.5 Weiteres gewünschtes Vorgehen

*digitalswitzerland, economiesuisse, Sicpa* und *Swico* wünschen sich im weiteren Prozess weiterhin den Einbezug unterschiedlicher Anspruchsgruppen, für eine inklusive Pilotierung respektive als Beitrag zum Vertrauensaufbau. *VD* sieht die Kantone und Gemeinden als primäre, im Prozess miteinzubeziehende Partner, da diese die wichtigsten Online-Dienstleister darstellen würden, welche auf eine Identitätsüberprüfung angewiesen sind. *OBP* findet eine transparente Erarbeitung von Arbeitsergebnissen unter Einbezug aller relevanter Parteien ebenfalls wichtig.

Beim Gesetzgebungsprozess wäre es *SDA* und *Swico* ein Anliegen, bereits als paralleler, vorgezogener Dialog über das Gesetz diskutieren zu können.

Der *GLP* ist es wichtig, ein E-ID-Ökosystem im Gleichschritt mit anderen Staaten zu entwickeln.

# 6 Weitere Ergebnisse der öffentlichen Diskussion

## 6.1 SIK-Umfrage

Bereits vor der Veröffentlichung des Diskussionspapiers zum «Zielbild E-ID» hat die Schweizerische Informatikkonferenz SIK in Kooperation mit dem Verein Schweizerische Städte- und Gemeinde-Informatik SSGI am 27. Juli 2021 eine Umfrage zur Anwendung der E-ID bei Behörden und in der Wirtschaft gestartet. Ziel war die Fokussierung auf die wirkungsvollsten und breit akzeptierten Anwendungsfelder sowie die Koordination zwischen den Behörden aller Staatsebenen. Die Umfrage wurde am 30. September 2021 geschlossen.

Unbestritten bei den 119 Umfrageteilnehmenden war der Wunsch nach einer einheitlichen E-ID ausgestellt durch den Staat. Als Erfolgsfaktoren für die zukünftige E-ID-Lösung wurden ein breites Anwendungsfeld, Vertrauenswürdigkeit, einfacher und kostengünstiger bis kostenloser Zugang, Interoperabilität und internationale Kompatibilität genannt. Datensicherheit und Datenschutz wurden als entscheidende Aspekte und die Datensparsamkeit sogar als Schlüsselelement für die Akzeptanz der E-ID gesehen. Über die technische Umsetzung dieser Anforderungen waren sich die Umfrageteilnehmer nicht einig. Über die Hälfte sprach sich für einen zentralen E-ID-Dienst (IdP) aus, ein Drittel für eine dezentrale Lösung wie sie von der EU mit der selbstbestimmten Identität (SSI) angestrebt wird.

Mit Blick auf die Anwendungsfälle stand in den Antworten der öffentlichen Verwaltung der rechtsverbindliche elektronische Verkehr mit der Bevölkerung und der Wirtschaft im Zentrum. Dieser reicht von der digitalen Signatur von Dokumenten über die elektronische Geschäftsabwicklung in Portalen und elektronischen Behördendiensten bis hin zur Vereinfachung der Ausübung der Bürgerrechte über E-Collecting und E-Voting. Die gleiche E-ID soll nach den Umfrageteilnehmenden auch im Alltag für die sichere Kommunikation von Unternehmen mit ihren Kundinnen und Kunden, für die rasche und sichere Abwicklung von elektronischen Miet- und Kaufverträgen oder für den Altersnachweis beim Kauf von Alkohol eingesetzt werden können.

## 6.2 Konferenzielle Diskussion

Als Schlusspunkt der öffentlichen Konsultation wurde eine konferenzielle Diskussion durchgeführt. In diesem Rahmen haben sich Teilnehmende aus Politik, Wirtschaft, Organisationen, Kantonen und Gemeinden sowie der Eidgenössische Datenschutzbeauftragte (EDÖB) geäussert. Die Meinungsäusserungen anlässlich dieser Konferenz bestätigten die Stossrichtung der eingereichten Stellungnahmen im Rahmen der öffentlichen Konsultation zum «Zielbild E-ID». Die Aufzeichnungen der Stellungnahmen der Konferenz können auf der Webseite vom Bundesamt für Justiz angesehen werden.

# 7 Zugang zu den Stellungnahmen

Die vollständigen Stellungnahmen zum Diskussionspapier zum «Zielbild E-ID» können beim Bundesamt für Justiz eingesehen werden. Diese sind zusammen mit diesem Bericht integral im Internet veröffentlicht unter: *Startseite BJ > Staat & Bürger > Laufende Rechtsetzungsprojekte > Staatliche E-ID > Öffentliche Konsultation zum "Zielbild E-ID"*.

**Verzeichnis der Eingaben**
**Liste des organismes ayant répondu**
**Elenco dei partecipanti**

**Kantone / Cantons / Cantoni**

| | |
|---|---|
| **AG** | Aargau / Argovie / Argovia, Departement Finanzen und Ressourcen |
| **AI** | Appenzell Innerrhoden / Appenzell Rh.-Int. / Appenzello Interno, Ratskanzlei |
| **AR** | Appenzell Ausserrhoden / Appenzell Rh.-Ext. / Appenzello Esterno, Informatikstrategie-Kommission |
| **BE** | Bern / Berne / Berna, Amt für Informatik und Organisation KAIO |
| **BL** | Basel-Landschaft / Bâle-Campagne / Basilea-Campagna, Regierungsrat |
| **FR** | Freiburg / Fribourg / Friburgo, Staatskanzlei |
| **GE** | Genf / Genève / Ginevra, Le Conseiller d'Etat, Département des infrastructures |
| **GL** | Glarus / Glaris / Glarona, Regierungsrat |
| **GL (stva)** | Glarus / Glaris / Glarona, Strassenverkehrs- und Schiffahrtsamt |
| **LU** | Luzern / Lucerne / Lucerna, Finanzdepartement |
| **NE** | Neuenburg / Neuchâtel, Le Conseil d'Etat |
| **NW** | Nidwalden / Nidwald / Nidvaldo, Staatskanzlei |
| **OW** | Obwalden / Obwald / Obvaldo, Staatskanzlei |
| **SH** | Schaffhausen / Schaffhouse / Sciaffusa, Regierungsrat |
| **TG** | Thurgau / Thurgovie / Turgovia, Departement für Inneres und Volkswirtschaft |
| **VD** | Waadt / Vaud, La cheffe du département des infrastructures et ressources humaines |
| **VD (DGS)** | Waadt / Vaud, Direction générale de la santé DGS |
| **ZH** | Zürich / Zurich / Zurigo, Staatskanzlei |

**Parteien / Partis politiques / Partiti politici**

| | |
|---|---|
| **Grüne** | Grüne<br>Les Vert·e·s<br>I Verdi |
| **GLP** | Grünliberale glp<br>Vert'libéraux pvl<br>Verdi liberali pvl |
| **Piratenpartei** | Piratenpartei Schweiz<br>Parti Pirate Suisse<br>Partito Pirata Svizzero |
| **SP** | Sozialdemokratische Partei der Schweiz SP<br>Parti Socialiste Suisse PS<br>Partito Socialista Svizzero PS |

**Hochschulen**

| | |
|---|---|
| **BFH** | Berner Fachhochschule, Technik & Informatik, Forschungsgruppe IAM des Instituts IDAS |

| | |
|---|---|
| **HSLU** | Hochschule Luzern, Informatik |
| **ZHAW** | Zürcher Hochschule für Angewandte Wissenschaften, Expert Group «Blockchain Technology in Interorganisational Collaboration» |

**Interessierte Organisationen und Unternehmen / Organisations intéressées et entreprises / Organizzationi interessate e imprese**

| | |
|---|---|
| **asa** | Vereinigung der Strassenverkehrsämter |
| **CloudTrust** | CloudTrust SA |
| **DIDAS** | Digital Identity and Data Sovereignty Association |
| **Post** | Die Schweizerische Post AG |
| **Digitale Gesellschaft** | Digitale Gesellschaft |
| **digitalswitzerland** | digitalswitzerland |
| **DuoKey** | DuoKey SA |
| **economiesuisse** | economiesuisse |
| **esatus** | esatus AG |
| **ZRH** | Flughafen Zürich AG |
| **govtechpodcast** | govtechpodcast.ch |
| **HIN** | Health Info Net AG |
| **eHealth** | IG eHealth |
| **k§rm** | Kompetenzzentrum Records Management AG |
| **KS** | Stiftung für Konsumentenschutz |
| **NEDIK** | Netzwerk digitale Ermittlungsunterstützung Internetkriminalität |
| **Nets** | Nets A/S, Dänemark |
| **OBP** | OpenBankingProject.ch |
| **privatim** | Konferenz der schweizerischen Datenschutzbeauftragten |
| **Procivis** | Procivis AG |
| **SAV** | Schweizerischer Anwaltsverband |
| **SBB** | SBB CFF FSS |
| **SCTO** | Swiss Clinical Trial Organisation |
| **sgv** | Dachorganisation der Schweizer KMU |
| **Sicpa** | Sicpa |
| **SSV** | Schweizerischer Städteverband |
| **Swico** | Wirtschaftsverband der ICT- und Online-Branche |
| **swimag** | swimag GmbH |
| **SB** | Swiss Banking, Schweizerische Bankiervereinigung |
| **SDA** | Swiss Data Alliance |
| **SFTI** | Swiss Fintech Innovations |
| **Swisscom** | Swisscom (Schweiz) AG |

| | |
|---|---|
| **Switch** | Switch |
| **Threema** | Threema |
| **ti&m** | ti&m AG |
| **unimedsuisse** | Universitäre Medizin Schweiz |
| **Vereign** | Vereign AG |

**Verzicht auf Stellungnahme**

– Schweizerischer Arbeitgeberverband (Verweis auf Stellungnahme economiesuisse)
Union patronale suisse
Unione svizzera degli imprenditori