HSLU Hochschule Luzern

Informatik
Information Systems Research Lab

Digitale Identitäten und elektronische Nachweise in der Schweiz 2026

Tim Weingärtner, Niklas Kustor

DIDAS

FH Zentralschweiz

Der vorliegende Bericht wurde
dank der Unterstützung
von DIDAS ermöglicht.

Zitiervorschlag
Weingärtner T., Kustor N. (2026) «Digitale Identitäten und elektronische Nachweise in der Schweiz 2026» Hochschule Luzern, Rotkreuz, Schweiz

Projektleitung
Prof. Dr. Tim Weingärtner

Kontakt für Rückfragen
Hochschule Luzern
Informatik
Prof. Dr. Tim Weingärtner
Suurstoffi 1
6343 Rotkreuz

tim.weingaertner@hslu.ch

Impressum

Hinweis:
Diese Studie wurde von der Hochschule Luzern, Informatik erstellt.
Ziel ist eine unabhängige, neutrale Standortbestimmung zu digitalen Identitäten und verifizierbaren Nachweisen in der Schweiz. Die Studie erhebt Wahrnehmungen und Einschätzungen der Befragten; sie stellt keine Produktbewertung dar und leitet keine kausalen Zusammenhänge ab.

Transparenzhinweis:
Die Befragung wurde über Netzwerke und öffentliche Kanäle verbreitet. Dadurch kann eine Überrepräsentation digital affiner Organisationen nicht ausgeschlossen werden. Die Ergebnisse sind als indikative Standortbestimmung zu verstehen.

Der Mitautor, Tim Weingärtner, ist Vizepräsident des Vereins DIDAS.

Inhaltsverzeichnis

Management Summary

Digitale Identitäten und elektronische Nachweise (z. B. digitale Ausweise, Bescheinigungen oder Berechtigungen) werden in der Schweiz zunehmend als Grundlage für sichere digitale Interaktionen verstanden, sowohl im Kontakt mit Behörden als auch zwischen privaten Organisationen. Durch die Abstimmung über die e-ID wurde das Thema breit in der Öffentlichkeit diskutiert. Die vorliegende Studie zeigt: Das Thema ist in vielen Organisationen angekommen, bleibt aber in der Umsetzung stark von praktischen Fragen geprägt.

Vertrauen spielt eine zentrale Rolle: Wer digitalen Identitäten vertraut, vertraut meist auch der Infrastruktur und umgekehrt. Das passt zur Schweizer Ausgestaltung, bei der der Bund eine Vertrauensinfrastruktur mit Registern betreibt, die keine personenbezogenen Daten einzelner Nachweise enthalten, sondern technische Identifikatoren, Schlüssel und Statusinformationen.

Eine weitere Erkenntnis ist, dass eine Zunahme von Identitätsmissbrauch durch KI (Deepfakes, synthetische Identitäten) wahrgenommen wird. Viele Organisationen werten dies als reales Risiko und sehen digitale Nachweise als Teil der Lösung, sofern sie gut umgesetzt sind.

Diese Studie liefert eine Standortbestimmung bezüglich der Einführung digitaler Identitäten in Schweizer klein- und mittelständischen Unternehmen (KMU) und Behörden. Die wichtigsten Erkenntnisse sind:

Kernaussagen

1. **Umsetzung hängt mit Wissen zusammen**
   93.6 % der KMU-Befragten haben von der neuen e-ID und der Vertrauensinfrastruktur in der Schweiz gehört. Organisationen mit besserem (selbst eingeschätztem) Verständnis befinden sich häufiger in der Planungs- oder Umsetzungsphase.
2. **Früher Reifegrad**
   Identitätslösungen werden heute nur spärlich eingesetzt (20.5 %). Ein substanzieller Anteil der befragten KMU hat sich des Themas noch nicht verbindlich angenommen. Bei staatlichen Behörden (kleine Stichprobe) zeigt sich im Vergleich ein höherer Umsetzungsgrad.
3. **Treiber unterscheiden sich**
   KMU begründen die Verwendung digitaler Identitäten primär mit Effizienzsteigerung. Behörden argumentieren stärker aus einer Sicherheits- und Compliance-Perspektive.
4. **Top-Hürden (KMU)**
   Die grössten Hürden liegen klar auf der operativen und organisatorischen Seite: Integration in bestehende Systeme (47.4 %), mangelndes Wissen/Verständnis (43.6 %), fehlende Geschäftsfälle oder fehlender Bedarf (39.7 %).
5. **Vertrauen wirkt als Hebel**
   Das Vertrauen in den Datenschutz und die Sicherheit digitaler Identitäten sowie in die Vertrauensinfrastruktur des Bundes ist mehrheitlich vorhanden. Es zeigt sich eine klare Kopplung: Wer der Vertrauensinfrastruktur stärker vertraut, bewertet digitale Identitäten tendenziell ebenfalls positiver. Gleichzeitig wird das Risiko KI-generierter Fake-Identitäten als relevant eingeschätzt.
6. **Es besteht Unsicherheit**
   Über die verschiedenen Auswertungen hinweg zeigt sich, dass grosse Unsicherheit besteht. Sei es über den Bedarf, das Verständnis oder die konkreten Umsetzungen.
7. **Zukünftige Pläne bis inkl. 2028**
   Unternehmen verfolgen vor allem einen vorsichtig-pragmatischen Kurs: Beobachten, dann handeln, sowie die Integration der Prüfung digitaler Identitäten sind die wesentlichen Stossrichtungen. Eine aktive Rolle als Herausgebende von digitalen Nachweisen bleibt die Ausnahme.

Digitale Identitäten und elektronische Nachweise in der Schweiz 2026

Management Summary

Empfehlungen für KMU

1. **Mit Verifikation starten**
   Ein pragmatischer Einstieg liegt bei Anwendungen wie dem Onboarding oder der Nachweisprüfung, weil hier der Mehrwert schnell sichtbar ist und sich schrittweise integrieren lässt. Reines Abwarten erhöht das Risiko, den Zug zu verpassen.

2. **Integration als zentrales Thema behandeln**
   Digitale Identitäten scheitern selten an der Idee, sondern an Schnittstellen, Integration in andere Systeme, Rollenlogiken und Betrieb. Deshalb sollte früh eine Zielarchitektur definiert und Integration, Betrieb und Verantwortlichkeiten innerhalb des Unternehmens klar festgelegt werden.

3. **Beim Business Case potenzielle Einsparungen in den Vordergrund stellen**
   Erwartete Effekte sollten realistisch entlang Prozesskosten, Durchlaufzeiten, Medienbrüchen, Betrugs- und Risikoaufwand modelliert werden. Umsatzargumente nur dort nutzen, wo sie belegbar sind.

4. **Kompetenzen gezielt aufbauen**
   Die Ergebnisse zeigen, dass viele Unternehmen ihren Unterstützungsbedarf noch nicht sicher einschätzen können. Sinnvoll ist ein zweistufiges Vorgehen: erst Grundlagen schaffen, dann konkrete Umsetzungsprojekte planen.

5. **Fraud-Risiko als Treiber nutzen**
   Wer Verifikation einführt, sollte Fraud-Szenarien mitdenken. Das erhöht intern und extern die Akzeptanz, weil es das «Warum gerade jetzt?» beantwortet.

Empfehlungen für Behörden

1. **Ökosystem aktiv gestalten und Orientierung schaffen**
   Viele Nicht-Teilnahmen entstehen aus Unwissen oder Zeitmangel. Klare Beteiligungswege, verständliche Erklärungen und einfach zugängliche Informationen wirken deshalb als Hebel.

2. **Standardisierung und Interoperabilität priorisieren und vorleben**
   Behördliche Nachweise sind ein wichtiger Bestandteil vieler Anwendungsfälle. Damit KMU schneller integrieren, sind Verfügbarkeit von Nachweisen und verlässliche technische Schnittstellen entscheidend.

3. **Sicherheit und Compliance operationalisieren**
   Eine starke Sicherheits- und Compliance-Logik sollte in konkrete Leitplanken übersetzt werden: Mindestanforderungen, Prüfroutinen, Betriebskonzepte, transparente Kommunikation.

«Die Überprüfung von Identitäten ist ein zentraler Bestandteil vieler Geschäftsfälle. Bewegen wir uns im digitalen Raum, ist eine sichere, vertrauenswürdige und selbstbestimmte Identitätslösung ein Muss.»

Prof. Dr. Tim Weingärtner, Hochschule Luzern, Mitautor, Dozent, Vizepräsident DIDAS

Digitale Identitäten und elektronische Nachweise in der Schweiz 2026

Management Summary

Hypothesen

Im Vorfeld dieser Studie wurden 11 Hypothesen aufgestellt. Zusammenfassend lassen sich diese mit Hilfe der Antworten wie folgt beurteilen:

Hypothese 1 → bestätigt
Ein als besser eingeschätztes Verständnis digitaler Identitäten geht mit einem fortgeschrittenem Einführungsgrad innerhalb des Unternehmens einher.

Hypothese 2 → keine Aussage
Grössere Unternehmen haben ein besseres Verständnis digitaler Identitäten als kleinere Unternehmen (z. B. weil sie mehr Ressourcen für IT und digitale Transformation bereitstellen können).

Hypothese 3 → bestätigt
Behörden sind bei der Implementierung digitaler Identitäten weiter fortgeschritten als privatwirtschaftliche Unternehmen, da sie durch regulatorische Anforderungen und staatliche Initiativen gefördert werden.

Hypothese 4 → bestätigt
Unter den Befragten KMU-Repräsentant:innen werde technische und organisatorische Faktoren häufiger als primäre Einführungshürden genannt als rechtliche Faktoren.

Hypothese 5 → widerlegt
Unternehmen sehen die grössten Bedenken bei den Implementierungskosten, während Behörden die Benutzbarkeit in Frage stellen.

Hypothese 6 → bestätigt
KMU nennen als Haupttreiber für digitale Identitäten primär Business-Case-Motive im Sinne der Effizienzsteigerung, während Behörden stärker sicherheits- und compliance-getrieben argumentieren.

Hypothese 7 → bestätigt
Unternehmen sehen digitale Identitäten primär als Lösung für Identitätsverifizierung und Zugriff, während datenbezogene Anwendungsfälle deutlich nachrangig sind.

Hypothese 8 → bestätigt
Die Grösse der Unternehmen spielt bei der Beurteilung der wirtschaftlichen Effekte der digitalen Identität keine wesentliche Rolle. Weiterhin erwarten die meisten Unternehmen keinen direkten Effekt digitaler Identitäten auf Umsatz oder Gewinn; die erwarteten Vorteile werden eher als Prozess- und Kostenthema verstanden.

Hypothese 9 → bestätigt
Vertrauen in Datenschutz/Sicherheit digitaler Identitäten ist positiv mit Vertrauen in die Vertrauensinfrastruktur des Bundes gekoppelt.

Hypothese 10 → bestätigt
Unternehmen mit hohem Vertrauen in die digitale Infrastruktur des Bundes haben weniger Bedenken hinsichtlich regulatorischer Unsicherheiten.

Hypothese 11 → keine Aussage
Unternehmen, welche digitale Identitäten nutzen oder deren Nutzung planen, haben eine höhere Sensibilität für das Risiko von Fake-Identitäten als Unternehmen ohne digitale Identitäten.

Interpretationshinweis: «bestätigt» bedeutet eine klare Tendenz in den Daten; «widerlegt» eine klare Tendenz dagegen; «keine Aussage» weist auf widersprüchliche Befunde, kleine Teilstichproben oder fehlende Werte hin.

1 Ausgangslage

Diese Studie untersucht, wie Schweizer KMU und Behörden digitale Identitäten und elektronische Nachweise wahrnehmen, nutzen oder deren Einsatz planen und welche Faktoren eine Akzeptanz fördern oder bremsen. Der Schwerpunkt liegt auf der Verständlichkeit für Laien, nicht auf technischen Implementierungsdetails.

Was ist eine «digitale Identität»?

Eine digitale Identität ist die Möglichkeit, sich online verlässlich als «diese Person» oder «diese Organisation» auszuweisen. Das kann für Logins, Vertragsabschlüsse, Kontoeröffnungen oder Behördenprozesse genutzt werden.
Entscheidend ist nicht nur die Technik, sondern:
Wer stellt die Identität aus? Wer vertraut ihr? Wer haftet?

Was sind «elektronische Nachweise»?

Elektronische Nachweise sind digitale Bescheinigungen, z. B. «volljährig», «wohnhaft in Gemeinde X», «Führerausweis gültig», «Mitarbeiterin von Firma Y». Wichtig ist das Prinzip **«So viel wie nötig, so wenig wie möglich».**
Oft genügt eine Eigenschaft (z. B. «über 18»), ohne dass Name oder Adresse offengelegt werden müssen.

Die Schweiz baut mit dem neuen e-ID-Rahmen eine staatliche Lösung und die dazugehörige Vertrauensinfrastruktur auf. Der Bund stellt dabei nicht nur die e-ID aus, sondern betreibt auch die Infrastruktur, die den sicheren Austausch und die Überprüfung elektronischer Nachweise ermöglicht.[1]

Politisch ist das Thema in der Schweiz eng mit Vertrauen verknüpft, auch im Nachgang zur Abstimmung 2025. Für die aktuelle Rechtsgrundlage gilt das Gesetz zur e-ID[2] und die darauf basierende Verordnung[3].

Durch die geplante Vertrauensinfrastruktur, welche in Form der «Public Beta»[4] bereits in der Entwicklung fortgeschritten ist und aktuell erprobt wird, wird die Basis für einen breiten Einsatz geschaffen. Damit sind nicht nur behördliche Nachweise wie e-ID, Führerausweis oder Wohnsitzbestätigung umsetzbar, sondern es erlaubt auch der Wirtschaft und öffentlichen Organisationen, eigene digitale Nachweise herauszugeben und die Vertrauensinfrastruktur zu nutzen. Der Bund betont explizit, dass die Infrastruktur offen ist für Stellen, die Nachweise ausstellen, besitzen oder überprüfen wollen, und nicht nur für staatliche Behörden.

Der in der Schweiz gewählte Ansatz basiert auf dem Konzept der selbstverwalteten Identität und somit einem dezentralen Identitätsmodell, das es Personen ermöglicht, ihre Identitätsdaten unabhängig von

---

[1] Bund: e-ID Informationsportal (Überblick zur e-ID und Vertrauensinfrastruktur) https://www.eid.admin.ch/ (Schweizer Eidgenossenschaft - e-ID Portal, 2026)

[2] Bundesgesetz über den elektronischen Identitätsnachweis und andere elektronische Nachweise https://www.fedlex.admin.ch/eli/fga/2025/20/de (Schweizer Eidgenossenschaft - Fedlex, 2026)

[3] Vorentwurf e-ID Verordnung https://cms.news.admin.ch/dam/de/der-schweizerische-bundesrat/CcnTR6jR9xtV/vorentw-veid-d.pdf (Schweizer Bundesrat, 2026)

[4] e-ID Public Beta https://www.eid.admin.ch/de/public-beta (Schweizer Eidgenossenschaft - e-ID Public Beta, 2026)

zentralisierten Anbietern zu verwalten und zu verifizieren. Die Nutzer:innen halten ihre Identitätsdaten in einer elektronischen Brieftasche – dem Wallet. In der Schweiz trägt es den Namen swiyu[5].

Das Ökosystem digitaler Identitäten und Nachweise in der Schweiz umfasst eine Vielzahl von Akteuren mit dedizierten Rollen:

- **Bürgerinnen und Bürger:** Sie können digitale Identitäten und Nachweise beziehen, halten und nutzen. Dabei ist explizit definiert, dass dies freiwillig ist und alternative Lösungen bestehen müssen.

- **Unternehmen und KMU:** Sie nutzen die Vertrauensinfrastruktur und digitale Identitäten zur Vereinfachung der Kunden- und Partnerverifizierung. Sie profitieren von einer sicheren, effizienten Identitätsprüfung und damit der Vermeidung von Fehlern. Gleichzeitig müssen Personendaten nicht gespeichert werden, da sie bei Bedarf elektronisch übermittelt werden können. Die e-ID Lösung ermöglicht datensparsame Prozesse und reduziert die Notwendigkeit, z. B. Ausweiskopien zu erfassen. Je nach Anwendungsfall und regulatorischen Pflichten könnten jedoch weiterhin Daten gespeichert werden.

- **Bund, Kantone, Gemeinden und Behörden:** Sie legen die regulatorischen Rahmenbedingungen fest und fördern vertrauenswürdige Identitätslösungen. Gleichzeitig sind sie primäre Aussteller von digitalen Identitäten und Nachweisen.

- **Technologieanbieter:** Sie entwickeln Plattformen und digitale Wallets zur Verwaltung von Identitätsdaten. Der Bund bzw. das Bundesamt für Informatik entwickelt die swiyu Wallet-App und die Vertrauensinfrastruktur.

- **Branchenverbände und Vereine wie DIDAS[6]:** Sie fördern Standardisierung und setzen sich für die Interoperabilität verschiedener Lösungen ein.

1.1 Begriffe und Konzepte

Für die Einordnung dieser Studie ist es hilfreich, drei Ebenen zu trennen:

1. **E-ID – ein staatlich ausgestellter Identitätsnachweis:**
   Die e-ID ist ein vom Staat herausgegebener, rechtlich verankerter Identitätsnachweis und bildet die Grundlage für verlässliche Identitätsprüfungen in digitalen Prozessen.

2. **Vertrauensinfrastruktur swiyu:**
   Die Vertrauensinfrastruktur des Bundes stellt die technische und organisatorische Basis bereit, damit Nachweise ausgestellt, gehalten und geprüft werden können. Dies nicht nur durch Behörden, sondern auch durch private Organisationen innerhalb klarer Spielregeln.

3. **Rechtliche Grundsätze der Nutzung:**
   Der gesetzliche Rahmen zielt darauf ab, digitale Nachweise datensparsam, privacy-by-design und interoperabel nutzbar zu machen, Dies insbesondere dort, wo heute Ausweiskopien, Medienbrüche und redundante Datenspeicherung dominieren.

---

[5] swiyu App und Vertrauensinfrastruktur https://www.eid.admin.ch/de/swiyu-coming-soon-d (Schweizer Eidgenossenschaft - swiyu, 2026)

[6] Verein DIDAS – Digital Identity and Data Sovereignty Association https://www.didas.swiss/ (DIDAS, 2026)

In dieser Studie verwenden wir den Begriff der digitalen Identität in zwei Bedeutungen, die in der Praxis häufig vermischt werden:

Login-Identität (IAM = Identity & Access Management): Eine technische Identität zur Authentifizierung/ Autorisierung (z. B. Login-Konten, SSO, klassische Identity Provider).

Digitale Handlungs- und Nachweisfähigkeit: Ein rechtlich und technisch belastbarer Nachweis (z. B. e-ID und darauf aufbauende verifizierbare Nachweise), der Eigenschaften («Fakten») digital belegen kann.

Wo wir explizit von staatlich verankerten Nachweisen sprechen, verwenden wir «e-ID» bzw. «elektronischer Nachweis». Wo es primär um Zugriff und Authentication geht, sprechen wir von «Login-Lösungen».

Was ist ein digitales «Wallet»?

Ein digitales Wallet ist eine App, in der man e-ID und Nachweise speichern und bei Bedarf vorweisen kann – ähnlich wie eine Brieftasche. Das System ist besonders dann vertrauenswürdig, wenn die Nutzung nicht zentral nachverfolgt werden kann und wenn der Eigentümerin oder dem Eigentümer des Nachweises klar ist, welche Daten wann geteilt werden.

Im Rahmen von selbstverwalteten Identitäten und Nachweisen spricht man oft von einem Vertrauensdreieck. Dies umfasst die drei Rollenträger: **Aussteller – Nutzer – Prüfer**.

Aussteller:in (Issuer) gibt einen Nachweis heraus (z. B. Behörde, Schule, Arbeitgeber).

Nutzer:in (Holder) verwaltet Nachweise (z. B. in einem Wallet) und zeigt diese Nachweise bei Bedarf vor.

Prüfer:in (Verifier) prüft die Echtheit und Gültigkeit, ohne mehr Daten als nötig zu erhalten.

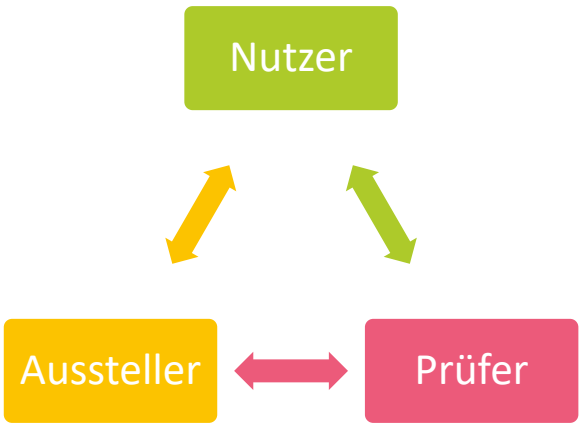

Abbildung 1 – Vertrauensdreieck

Wir kennen dieses Vertrauensdreieck von traditionellen Nachweisen wie etwa der physischen ID. Bei digitalen Nachweisen werden kryptographisch signierte Datenpakte übertragen. Um die Gültigkeit der Aussteller:in und des Nachweises prüfen zu können, braucht es ein elektronisches Register, welches Teil der Vertrauensinfrastruktur swiyu ist. Um Privatsphäre und Datenschutz zu gewährleisten, sind in diesem Register keine Daten über den Nutzer oder die Nutzerin hinterlegt. Auch werden die Aussteller:innen bei der Verifikation durch die Prüfer:innen nicht kontaktiert und erhalten so keine Kenntnis, dass ein Nachweis vorgelegt wurde.

Neben staatlichen Aussteller:innen gewinnt eine zweite Kategorie an Bedeutung: **private Issuer**, die Nachweise wie Mitgliedschaften, Qualifikationen, Unternehmensattribute, Compliance-Bescheinigungen oder Tickets ausstellen. Gerade hier entsteht häufig der praktische Schub für eine Verbreitung, weil Nachweise direkt in Geschäftsprozesse (Onboarding, Beschaffung, Partnerprüfung) hineinwirken.

Digitale Signaturen

Digitale Signaturen weisen die Echtheit und Originalität eines Dokuments oder einer Nachricht kryptografisch nach. Sie dienen der rechts- und beweissicheren Unterschrift von Inhalten und sind damit etwas anderes als digitale Identitäten und personenbezogene Nachweise, die auf Identifikation oder Attributbestätigung zielen.

Organisatorische Identitäten

Organisatorische Identitäten beschreiben, wie eine Organisation digital eindeutig erkennbar ist und wie Vertretungs- und Berechtigungsstrukturen abgebildet werden. Das unterscheidet sich von personenbezogenen Identitäten und Nachweisen, die sich auf natürliche Personen beziehen.

Beide Themen werden in dieser Studie nicht vertieft behandelt, weil die Umfrage bewusst auf personenbezogene Identitäten und Nachweise fokussierte.

1.2 Regulatorischer Rahmen für e-ID und Vertrauensinfrastruktur in der Schweiz

Die digitale Transformation erfordert sichere und vertrauenswürdige Methoden zur Identifizierung und Authentifizierung von Personen und Organisationen im digitalen Raum. Digitale Identitäten und Nachweise spielen dabei eine zentrale Rolle, indem sie die Grundlage für sichere Online-Transaktionen und Interaktionen schaffen, die bezüglich Verlässlichkeit und Praktikabilität vergleichbar sind mit traditionellen, physischen Identifikationsmethoden. Damit wird ein neues Ökosystem an Nachweisen im digitalen Raum geschaffen.

In der Schweiz bildet die elektronische Identität (e-ID) die Basis für digitale Identifikationsprozesse. Der Bund plant, ab diesem Jahr (2026) die e-ID zusammen mit der Vertrauensinfrastruktur und einer Wallet-App zu betreiben. Das Projekt mit dem Namen «swiyu» ermöglicht es Schweizer Bürger:innen und Personen mit Aufenthaltsgenehmigung, ihre Identität online nachzuweisen. Die zugrundeliegende Vertrauensinfrastruktur ermöglicht es auch anderen Behörden und privaten Organisationen, elektronische Nachweise auszustellen. «swiyu» ist hierbei nicht die e-ID selbst, sondern beschreibt die Wallet Applikation plus die Vertrauensinfrastruktur, in der die e-ID als staatlich herausgegebener Nachweis integriert ist.[7]

Die Einführung der staatlich anerkannten e-ID erfordert den Aufbau und Betrieb einer Vertrauensinfrastruktur über alle föderalen Ebenen hinweg, einschliesslich eines staatlichen Wallets sowie

[7] Bund: e-ID Informationsportal https://www.eid.admin.ch/ (Schweizer Eidgenossenschaft - e-ID Portal, 2026)

eines Basis- und Vertrauensregisters. Der Bund betreibt hierbei die Vertrauensinfrastruktur, welche für alle Anwendungsfälle über föderale Ebenen hinweg offen und nutzbar ist.[8] [9]

«Die e-ID und die Vertrauensinfrastruktur des Bundes bilden die Basis für ein digitales Ökosystem verifizierbarer Nachweise in der Schweiz»

Dr. Rolf Rauschenbach, Bundesamt für Justiz, Stellvertretender Leiter Fachbereich e-ID und Informationsbeauftragter e-ID

Die rechtlichen Grundlagen für die e-ID und Vertrauensinfrastruktur in der Schweiz werden durch das Gesetz zur e-ID und entsprechenden Verordnungen geregelt. Eine öffentlich zugängliche Betaversion ist bereits vorhanden, die diese Infrastruktur spiegelt.[10] [11]

In der Schweiz sind bereits verschiedene Identitätslösungen bekannt (z. B. SwissID, SwissPass oder AGOV). Diese Lösungen können im Alltag wertvoll sein, aber sie sind nicht automatisch gleichzusetzen mit einem staatlich ausgestellten, gesetzlich verankerten Identitätsnachweis.

Eine Login-Identität beantwortet primär die Frage «Wer darf sich anmelden?». Die e-ID und verifizierbare Nachweise beantworten zusätzlich die Frage «Welche Aussage kann ich verlässlich prüfen und mit welcher Rechts- und Vertrauensgrundlage?».

1.3 Globale Trends

1.3.1 Einführung digitaler Identitäten in der EU und den USA

Auf globaler Ebene verfolgen sowohl die Europäische Union (EU) als auch die Vereinigten Staaten (USA) Initiativen zur Einführung digitaler Identitäten. Die EU plant die Einführung einer europäischen digitalen Identität, die es Bürger:innen und Unternehmen ermöglicht, sich EU-weit auszuweisen und bestimmte persönliche Informationen nachzuweisen – sowohl online als auch offline für öffentliche oder private Dienstleistungen. Alle Menschen in der EU sollen mit dem Projekt eIDAS 2.0[12] Zugang zu einem persönlichen digitalen Wallet (EUID-Wallet) bekommen und dieses so nutzen können.[13]

Einzelne Länder in der EU betreiben bereits digitale Identitätslösungen, darunter Frankreich mit «France Identité»[14], Österreich mit «ID Austria»[15] oder Polen mit «mDowód»[16]. Diese Lösungen werden mit eIDAS 2.0 abgelöst und sollen eine kompatible, EU-weite digitale Identitätslösung bieten.

In den USA und der EU gibt es Bestrebungen, gemeinsame Ansätze für digitale Identitäten zu entwickeln. Ein gemeinsamer Bericht des Handels- und Technologierats (TTC) der EU und der USA zielt darauf ab,

---

[8] Digitale Verwaltung Schweiz https://www.digitale-verwaltung-schweiz.ch/umsetzungsplan/projekte/behoerdenuebergreifende-digitale-identifikation-etablieren (Digitale Verwaltung Schweiz, 2026)

[9] e-ID Technologie https://www.eid.admin.ch/de/technologie (Schweizer Eidgenossenschaft - e-ID Technologie, 2026)

[10] Strategie zur Digitalen Schweiz https://digital.swiss/de/aktionsplan/massnahme/bundesgesetz-uber-elektronische-identifizierungsdienste (Schweizerische Bundeskanzlei, 2026)

[11] Public Beta https://www.eid.admin.ch/de/public-beta (Schweizer Eidgenossenschaft - e-ID Public Beta, 2026)

[12] eIDAS – elektronische Identifizierung und Vertrauensdienste https://digital-strategy.ec.europa.eu/de/policies/discover-eidas (Europäische Kommission , 2025)

[13] Europäische digitale Identität https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/european-digital-identity_de (Europäische Kommission, 2026)

[14] France Identité https://france-identite.gouv.fr/ (Französische Republik, 2026)

[15] ID Austria https://www.id-austria.gv.at/de/verwenden/eausweise (Bundeskanzleramt, 2026)

[16] mDowód https://info.mobywatel.gov.pl/en/dokumenty/mdowod (Minister of Digital Affairs, 2026)

gemeinsame Definitionen, Vertrauensniveaus und Verweise auf internationale Standards im Bereich der digitalen Identität zu erarbeiten.[17]

Für Schweizer Organisationen ist diese Entwicklung aus zwei Gründen relevant: Erstens können grenzüberschreitende Geschäftsmodelle (z. B. Kundschaft in der EU, Plattformen, regulierte Branchen) mittel- und langfristig mit EUID-Wallet-Interaktionen konfrontiert sein. Zweitens beeinflusst die EU-Standardisierung den internationalen Markt an Identitäts- und Nachweislösungen, etwa über Standards, Sicherheitsanforderungen und Akzeptanzmechanismen.

Gemäss der Europäischen Kommission sollen die Mitgliedstaaten Wallets bis Ende 2026 bereitstellen. Für die Schweiz gelten zwar die EU-Vorgaben nicht direkt, aber es ist strategisch sinnvoll, die Entwicklungen zu beobachten. Dies insbesondere bei Interoperabilitätsanforderungen, anerkannten Nachweisen und der Akzeptanz im Privatsektor.

1.3.2 Bhutan: National Digital Identity (NDI)

Bhutan wird international häufig als Anschauungsbeispiel genannt, wie ein staatlich orchestriertes Wallet-Ökosystem nach dem Prinzip selbstverwalteter Identitäten praktisch umgesetzt werden kann. Mit der National Digital Identity (NDI)[18] existiert eine nationale digitale Identitätsinfrastruktur, die auf eine Wallet-Nutzung und auf digitale Nachweise ausgerichtet ist. In Bhutan ist die NDI nicht nur ein «Login-Projekt», sondern wird als Grundlage für wiederverwendbare Nachweise in digitalen Prozessen positioniert.

Für die Einordnung ist vor allem der Governance-Ansatz relevant: Der «National Digital Identity Act of Bhutan 2023»[19] sieht u. a. die Ausstellung von «verifiable digital credentials» vor und regelt die Onboarding-Prozesse für Aussteller:innen (Issuer) und deren Pflichten. Damit werden Rollen, Verantwortlichkeiten und Verfahren explizit festgelegt: ein Punkt, der in vielen Ländern als Erfolgsfaktor für Vertrauen und Skalierung gilt.

Für die Schweiz ist Bhutan keine Blaupause, denn der Kontext (Grösse, Verwaltungsstruktur, Rechtsraum, Ökosystem) unterscheidet sich deutlich. Als Lernbeispiel ist Bhutan jedoch hilfreich, weil es zeigt, wie klare Governance und Verantwortlichkeiten, eine konsequente Wallet-Orientierung und früh sichtbare Anwendungsfälle zusammenwirken können.

«Bhutan National Digital Identity (NDI) was officially launched in October 2023 by His Royal Highness, the Crown Prince of Bhutan. Gyalsey (Crown Prince) is Bhutan's first digital citizen and today we have onboarded more than 350,000 users in Bhutan. With NDI, we became the first nation in the world to implement self-sovereign identity at the national level. With secured and passwordless access to government and business services, it allows our citizens to control their digital credentials within their fingertips.»

Ms. Audrey Low, President, Gyalpozhing college of information technology, Royal University of Bhutan

---

[17] DRAFT EU-US TTC Digital Identity Mapping Exercise Report https://www.nist.gov/document/eu-us-ttc-wg1 (US-EU Trade and Technology Council, 2026)

[18] Nationale ID in Bhutan https://www.bhutanndi.com/ (Bhutan NDI., 2026)

[19] National Digital Identity Act of Bhutan 2023 https://tech.gov.bt/wp-content/uploads/2024/09/National-Digital-Identity-Act-of-Bhutan-2023.pdf (Parliament of Bhutan, 2026)

2 Struktur der Studie und Umfragemethodik

Die Studie basiert auf einer quantitativen Online-Umfrage, die im November 2025 (Start der Umfrage: 3.11.2025, Ende der Umfrage: 5.12.2025) durchgeführt wurde. Zielgruppe waren Firmenvertreter:innen mit unterschiedlichen Rollen aus Schweizer klein- und mittelständischen Unternehmen, sowie Behördenvertreter:innen, die bei Gemeinden, Kantonen und dem Bund angestellt sind.

Die Teilnehmenden wurden über Branchenverbände, Unternehmensnetzwerke und gezielte Direktanfragen rekrutiert. Die Daten wurden anonymisiert verarbeitet und fallweise nach Branchen, Unternehmensgrösse und Rollen innerhalb des Unternehmens segmentiert.

Die 78 vollständigen Rückmeldungen der Zielgruppe KMU und sechs vollständigen Rückmeldungen der Zielgruppe Behörden wurden entlang der zentralen Dimensionen Verständnis, Einführungsstatus, Hürden, Nutzen, Vertrauen, Risiko- und Zukunftswahrnehmung ausgewertet. Wir möchten an dieser Stelle explizit darauf hinweisen, dass die Stichprobe bei den Behörden statistisch nicht aussagekräftig ist. Trotzdem führen wir die Antworten auf, um ein Stimmungsbild zu zeigen. Wo sinnvoll, haben wir die Antworten beider Kategorien kombiniert.

2.1 Profil der Stichprobe

2.1.1 Branchenverteilung[20]

Die grössten Gruppen sind Wirtschaft, Management, Handel (21.79 %) sowie Industrie, Technik, Informatik (20.51 %). Danach folgt Finanzwesen (14.1 %). Weitere relevante Anteile entfallen auf Bau, Gebäudetechnik, Innenausbau (10.26 %) sowie Öffentliche Verwaltung, Rechtspflege, Sicherheit (6.41 %) und Beratung (6.41 %). Kleinere Anteile: Gesundheit, Sport, Wellness (5.13 %), Bildung, Soziales (3.85 %), Medien, Information, Kommunikation (3.85 %) und Verkehr, Fahrzeuge, Logistik (2.56 %).

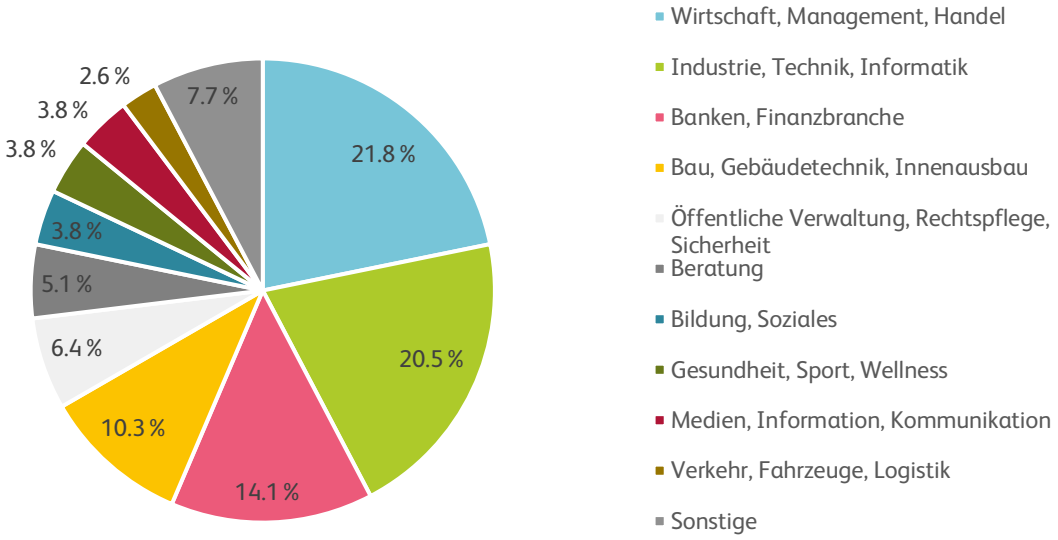

Abbildung 2 – Branchenverteilung der Studienteilnehmenden (n=78)

[20] Hinweis zur Bereinigung: Freitextnennungen aus «Sonstiges» wurden, wenn klar erkennbar, in die jeweilig entsprechende Kategorie (meist Finanzwesen bzw. Beratung) zusammengeführt; vereinzelte übrige Nennungen wurden den naheliegendsten bestehenden Kategorien zugeordnet, wobei 5.13 % als nicht direkt zuordenbar und somit als tatsächlich Sonstige gewertet werden können.

2.1.2 Geografische Verteilung (Hauptsitz)

Die Antworten stammen aus mehreren Kantonen mit klarem Schwerpunkt in Zug (37.2 %), gefolgt von Zürich (20.5 %) und Aargau (14.1 %). Weitere Hauptsitze der Unternehmen liegen in Luzern (7.7 %), wobei wietere kleinere Anteile auf Basel-Stadt (2.6 %) und St. Gallen (2.6 %) entfallen. Weiter sind einzelne Nennungen (je 1.3 %) u. a. in den Kantonen Bern, Fribourg, Nidwalden, Obwalden, Schwyz, Thurgau und Waadt. 6.4 % der Antworten enthalten keine Angabe zum Hauptsitz.

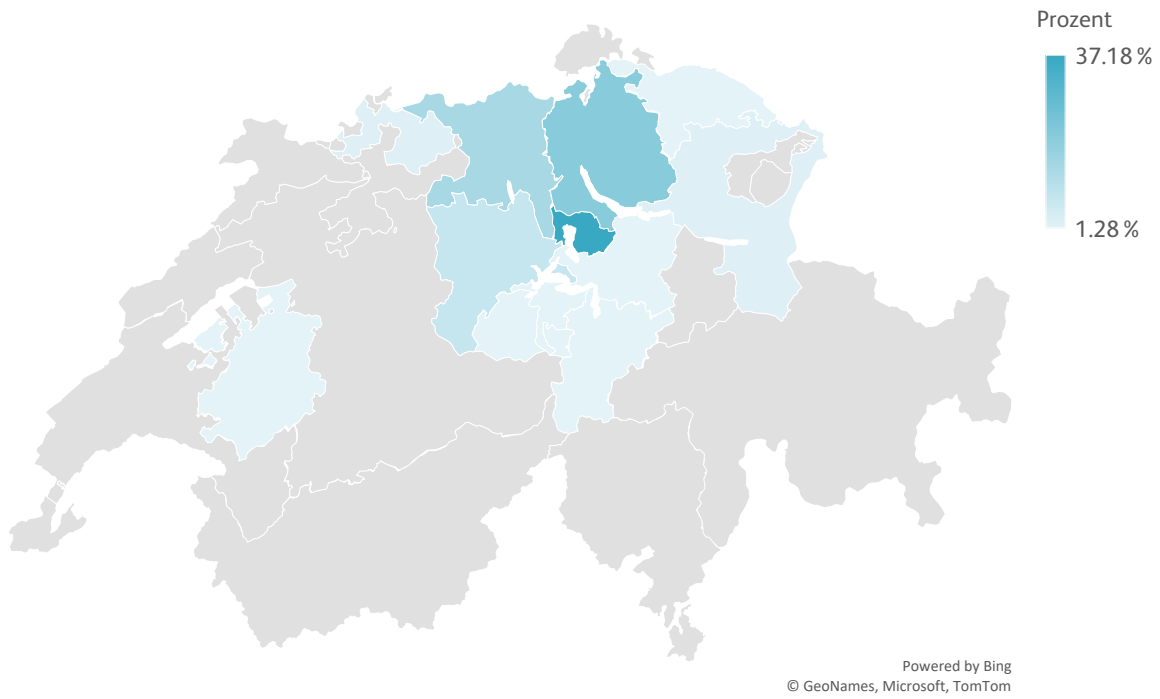

Abbildung 3 – Geografische Verteilung der Studienteilnehmenden (n=73)

«Für KMU ist das grösste Risiko nicht die Veränderung. Es ist, Kunden zu verlieren, weil man zu spät reagiert.»

Dr. Roman Zoun, Swisscom, Head of FinTech and Digital Wallet

2.1.3 Tätigkeitsgebiete

Am häufigsten sind die befragten Unternehmen schweizweit tätig (44.9 %). Danach folgen regionale bzw. nahe Märkte wie Zentralschweiz (23.1 %) und eigener Kanton (20.5 %) sowie die generelle DACH-Region (19.2 %). Auch International/Welt (17.9 %) und Europa (12.8 %) wurden regelmässig genannt. Die übrigen Teilregionen kamen seltener vor: Nordwestschweiz (10.3 %), Ostschweiz (9 %), Westschweiz und Südschweiz (je 7.7 %). «Sonstiges» spielt keine signifikante Rolle (3.8 %).

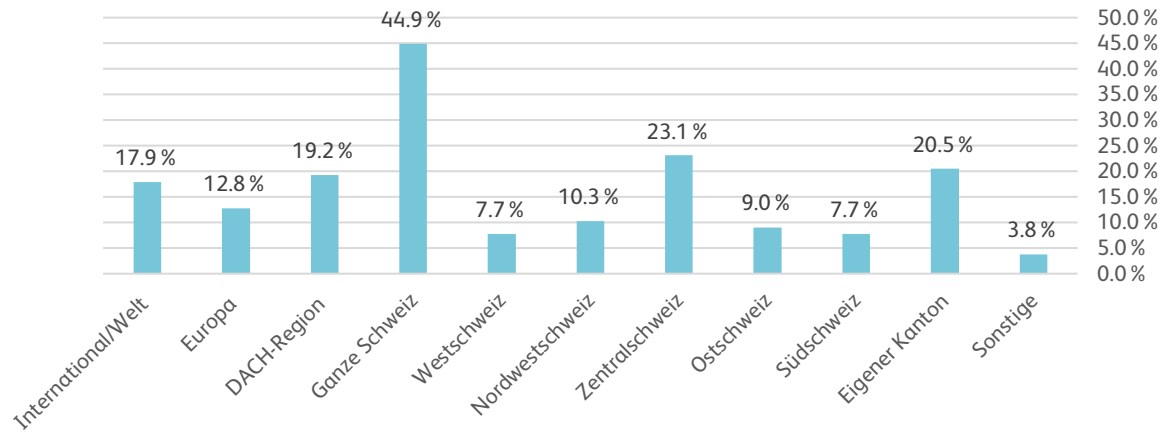

Abbildung 4 – Tätigkeitsgebiete der Studienteilnehmenden (n=78)

2.1.4 Unternehmensgrösse

In den gültigen Angaben haben 43.7 % der Unternehmen einen Umsatz unter CHF 10 Mio., 21.9 % liegen zwischen CHF 10 und unter CHF 50 Mio. und 34.4 % erzielen CHF 50 Mio. oder mehr. In den 78 vollständigen Antworten wurden 32 verwertbare Umsatzangaben gemacht.

Betrachtet man die Unternehmensgrösse nach Mitarbeitenden, so ergibt sich folgendes Bild: Am häufigsten vertreten sind Unternehmen mit 1 bis 9 Mitarbeitenden (23.9 %). Danach folgen 100 bis 249 (19.7 %) und 250 bis 999 (16.9 %). Mittelgrosse Unternehmen machen ebenfalls einen relevanten Anteil aus: 20 bis 99 (12.7 %) sowie 10 bis 19 (11.3 %). Grössere Organisationen sind seltener: 1000 bis 2000 (9.9 %) und über 2000 (5.6 %).

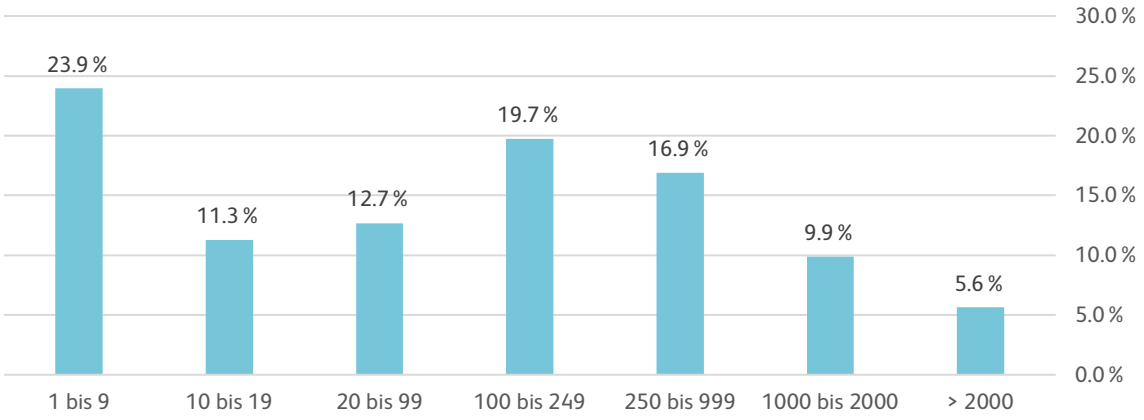

Abbildung 5 – Unternehmensgrössen der Studienteilnehmenden nach Mitarbeitenden (n=71)

2.1.5 Rolle der Befragten im Unternehmen

Nach der Bereinigung der Freitextnennungen in «Sonstiges» zeigt sich ein klarer Schwerpunkt in der Kategorie Management/C-Level (50 %). Die Kategorie Verwaltungsrat umfasst 17.9 %. Business Analyse und Informatik liegen nach Zuordnung der sonstigen Einträge bei 6.4 % und Verkauf bei 7.7 %. Sonstige, nicht direkt zuordenbare Einträge umfassen 11.5 %.

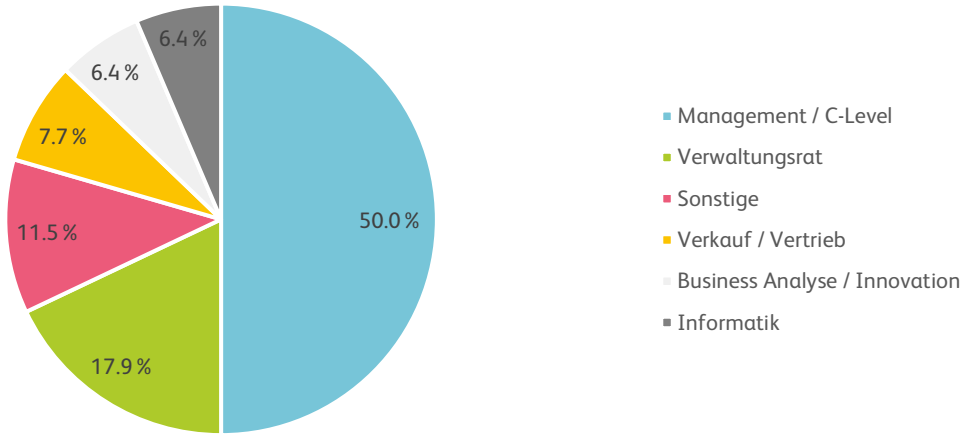

Abbildung 6 – Rolle der Studienteilnehmenden im Unternehmen (n=78)

2.1.6 Bildungsgrad

Fast die Hälfte der Befragten verfügt als höchsten Abschluss über einen Master (47.4 %). Weitere 19.2 % haben einen Bachelor. Weitere 15.4 % geben eine Lehre/Berufsausbildung als höchsten Abschluss an. Ein Doktorat liegt bei 14.1 % vor, während die Matura mit 3.8 % den kleinsten Anteil ausmacht. Insgesamt ist die Stichprobe damit klar akademisch geprägt, was bei der Einordnung der Ergebnisse mitzudenken ist.

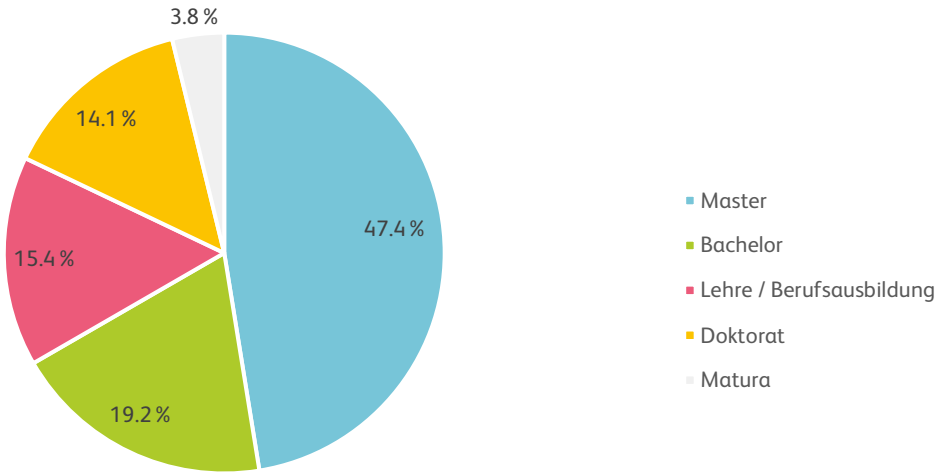

Abbildung 7 – Ausbildung der Studienteilnehmenden (n=78)

2.1.7 Bekanntheit bestehender digitaler Identitätslösungen

Die Umfrage ergab, dass über 90 % der befragten Personen von mindestens einer der etablierten Lösungen gehört haben. Konkret zeigt sich, dass die SwissID und der SwissPass mit jeweils 72 Nennungen (je 92.3 %) am bekanntesten sind. Dahinter folgt ein deutliches Mittelfeld mit MobileID (38.5 %) und AGOV (34.6 %). In einzelnen Branchen eingesetzte Identitätslösungen sind deutlich weniger bekannt. So wird die EduID von 20 Personen genannt (25.6 %), während HealthID mit 12.8 % am wenigsten bekannt ist. Insgesamt zeigt sich eine starke Konzentration auf die zwei etablierten, breit eingesetzten Lösungen, während spezialisiertere oder weniger verbreitete digitale Identitäten deutlich weniger präsent sind. Da Mehrfachnennungen möglich waren, summieren sich die Anteile nicht zu 100 % auf.

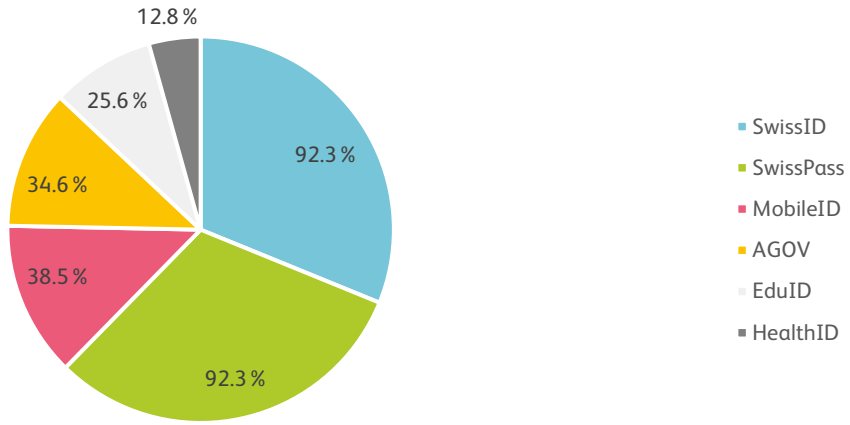

Abbildung 8 – Welche bestehenden digitalen Identitäten kennen Sie? (n=78 – Mehrfachauswahl möglich)

2.1.8 Selbsteinschätzung des Verständnisses digitaler Identitäten

Die Mehrheit der befragten KMU-Vertreter:innen bewertet ihr Verständnis als gut (59 %), also mit Kenntnis der wichtigsten Aspekte und bestehender Auseinandersetzung mit dem Thema. 20.5 % stufen es als sehr gut ein und geben an, digitale Identitäten aktiv zu nutzen und die Konzepte sowie die rechtlichen Grundlagen zu kennen. 18 % verfügen nur über ein geringes Verständnis. Lediglich 2.6 % geben an, praktisch uninformiert zu sein und somit kein Verständnis zu haben. Insgesamt deutet dies auf eine Stichprobe hin, die sich beim Thema digitale Identitäten überwiegend als informiert beurteilt.

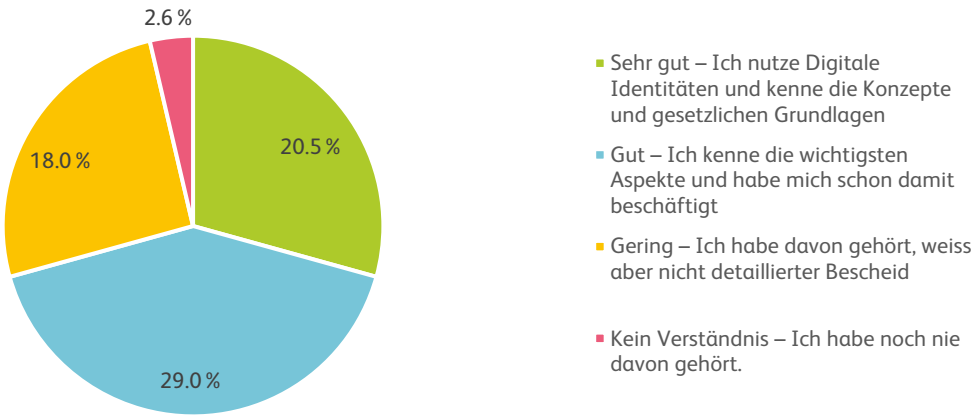

Abbildung 9 – Wie würden Sie Ihr Verständnis von digitalen Identitäten bewerten? (n=78)

An dieser Stelle sei bemerkt, dass eine grundsätzliche Selbsteinschätzung nicht als objektiv vorhandene Kompetenz gelesen werden darf. Ohne weiter darauf eingehen zu wollen, sind hier zwei wesentliche psychologische Aspekte relevant:

- Overconfidence/Dunning-Kruger-Effekt: Personen mit niedrigerem Wissen überschätzen teils ihre Kompetenz. «Gut» kann demnach sehr unterschiedlich gemeint sein und ist nicht zwingend gleichbedeutend mit Umsetzungsfähigkeit oder Priorisierung.
- Social Desirability Bias/soziale Erwünschtheit: In einem Kontext, der stark digital geprägt wirkt, kann es attraktiv sein, das eigene Verständnis höher zu bewerten (gemäss dem Mantra «Ich sollte das können»). Dieser Effekt kann die «Gut/Sehr gut»-Quote grundsätzlich nach oben verzerren.

2.1.9 Bekanntheit der neuen e-ID und Vertrauensinfrastruktur

Die grosse Mehrheit der Befragten hat bereits von der neuen Lösung der e-ID und Vertrauensinfrastruktur gehört (93.6 %). Nur fünf Befragte (6.4 %) geben an, noch nie etwas davon gehört zu haben. Das spricht für eine sehr hohe Grundbekanntheit in der Stichprobe der KMU, wodurch spätere Antworten eher auf einer inhaltlichen Einschätzung als auf fehlender Information beruhen dürften.

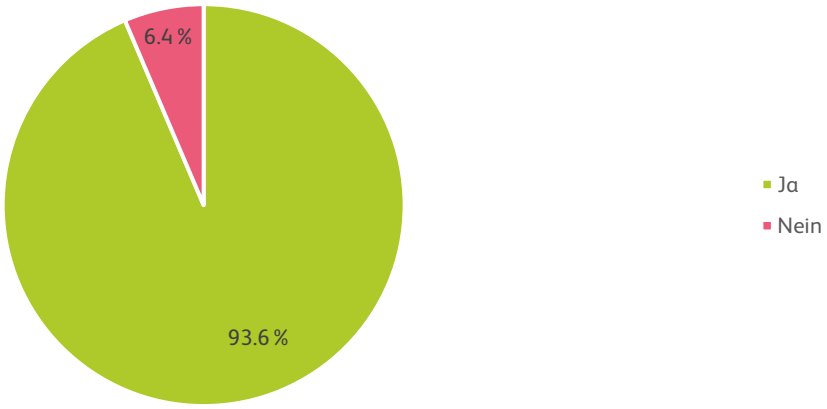

Abbildung 10 – Haben Sie von der neuen Lösung der e-ID und der Vertrauensinfrastruktur in der Schweiz gehört? (n=78)

Von denjenigen, die angaben, von der neuen Lösung der e-ID und der zugrundeliegenden Vertrauensinfrastruktur bereits gehört zu haben, bewerten 57.7 % ihr Wissen als gut, 19.2 % als sehr gut und 16.7 % als ausgezeichnet.

2.1.10 Wahrnehmung des regulatorischen Rahmens

Innerhalb der Einschätzung der Governance und des regulatorischen Rahmens zeigt sich, dass etwa die Hälfte der Befragten den regulatorischen Rahmen als unklar (48.8 %) bewertet. Rund ein Viertel ist noch unschlüssig (26.2 %). Kritischer fällt die Einschätzung bei 14.3 % aus: sie nehmen die aktuelle Situation als verwirrend und einschränkend wahr. Nur eine Minderheit empfindet den Rahmen als klar und unterstützend (10.7 %).

Insgesamt dominiert somit ein Bild von spürbarer Unsicherheit. Hier braucht es zwingende Aufklärungsmassnahmen und Informationskampagnen. Denn genau diese Unsicherheit kann in der Praxis wie eine Bremse wirken: Unternehmen warten länger ab, investieren eher schrittweise (Pilot, Vorbereitung) und versuchen Entscheidungen zu vertagen, bis mehr Klarheit bezüglich Auslegung, Standards und politischer Verbindlichkeit entsteht.

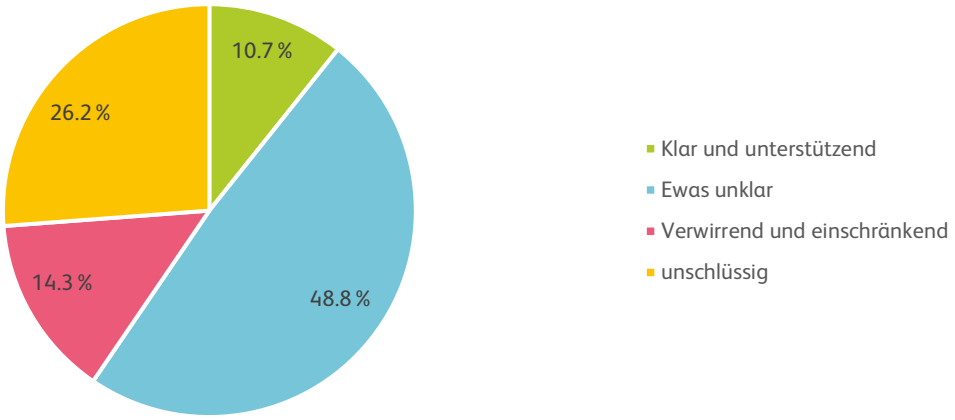

Abbildung 11 – Wie beurteilen Sie den regulatorischen Rahmen für digitale Identitäten in der Schweiz? (n=84 – KMU und Behörden)

2.1.11 Teilnahme an der öffentlichen Diskussion zur e-ID

In der Schweiz besteht durch die direkte Demokratie und Mitwirkungsgefässe wie Vernehmlassungen, Referenden und Anhörungen grundsätzlich ein starker Einbezug der Bevölkerung. Umso mehr überrascht es, dass die Teilnahme an der öffentlichen Diskussion laut den Antworten eher niedrig ist. Die Nicht-Teilnahme wird am häufigsten damit begründet, dass die Möglichkeiten nicht bekannt sind (34.5 %) und weil die Zeit fehlt (34.5 %). Aktive Beteiligung ist deutlich seltener: Konferenzen (10.7 %), Partizipationsmeetings des Bundes (8.3 %) und Mitgliedschaft in Vereinen wie DIDAS, oder Berufsverbänden (11.9 %). Kein Interesse wird selten genannt (6 %), was sehr erfreulich ist.

Bei dieser Frage waren Mehrfachantworten möglich.

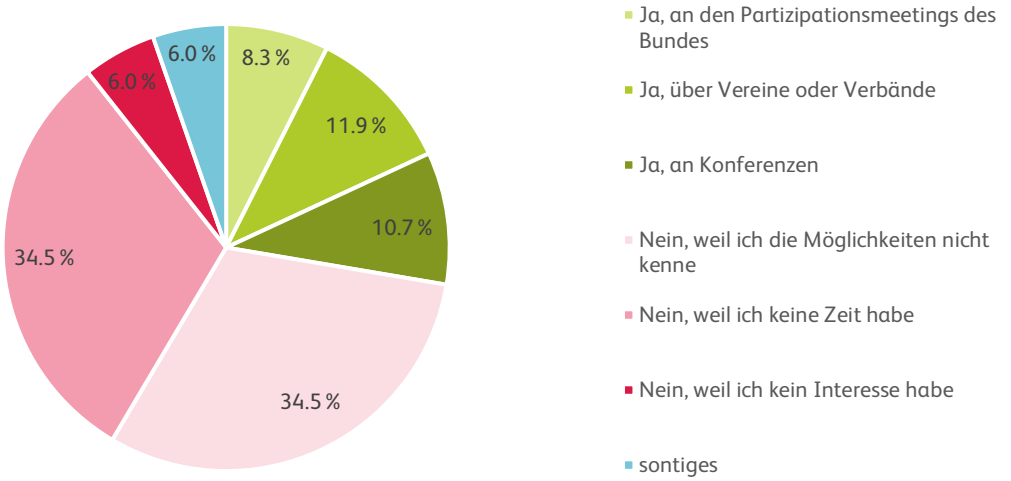

Abbildung 12 – Nehmen Sie an der öffentlichen Diskussion zur Vertrauensinfrastruktur des Bundes in der Schweiz teil? (n=84 – KMU und Behörden – Mehrfachantworten)

2.1.12 Nutzung und Einführung digitaler Identitäten nach Branchen

Die branchenbezogene Auswertung zum Einführungsstand digitaler Identitäten zeigt ein heterogenes Bild. Insgesamt deutet die Verteilung darauf hin, dass das Thema in vielen Organisationen bereits konkret bearbeitet wird (Implementierung oder Planung/Umsetzung), während ein relevanter Anteil weiterhin keine Pläne verfolgt und ein weiterer Teil sich im Modus «in Betracht gezogen» befindet.

Nach Branchen scheinen **Industrie, Technik, Informatik** vergleichsweise weiter zu sein: Hier ist der Anteil aktiver Organisationen höher als in anderen Bereichen. Gleichzeitig bleibt auch dort ein Teil der Firmen ohne Pläne, was auf eine Zweiteilung zwischen Vorreitern und abwartenden Organisationen hindeutet. In **Wirtschaft, Management, Handel** verteilt sich der Stand gleichmässig auf aktiv, prüfen und keine Pläne – ein Muster, das häufig auf einen stark vom Business Case und von externen Anforderungen (Kunden/Partner, Standards) abhängigen Entscheidungsprozess hinweist. Der Bereich **Öffentliche Verwaltung, Rechtspflege, Sicherheit** wirkt eher aktiv, ist aber aufgrund kleiner Fallzahlen mit Vorsicht zu interpretieren. Deutlich zurückhaltender zeigt sich in dieser Stichprobe **Bau/Gebäudetechnik**, wo die Einschätzung «keine Pläne» dominiert.

Einige Branchen haben sehr kleine Fallzahlen. Daher sind die Ergebnisse als indikative Tendenzen zu lesen.

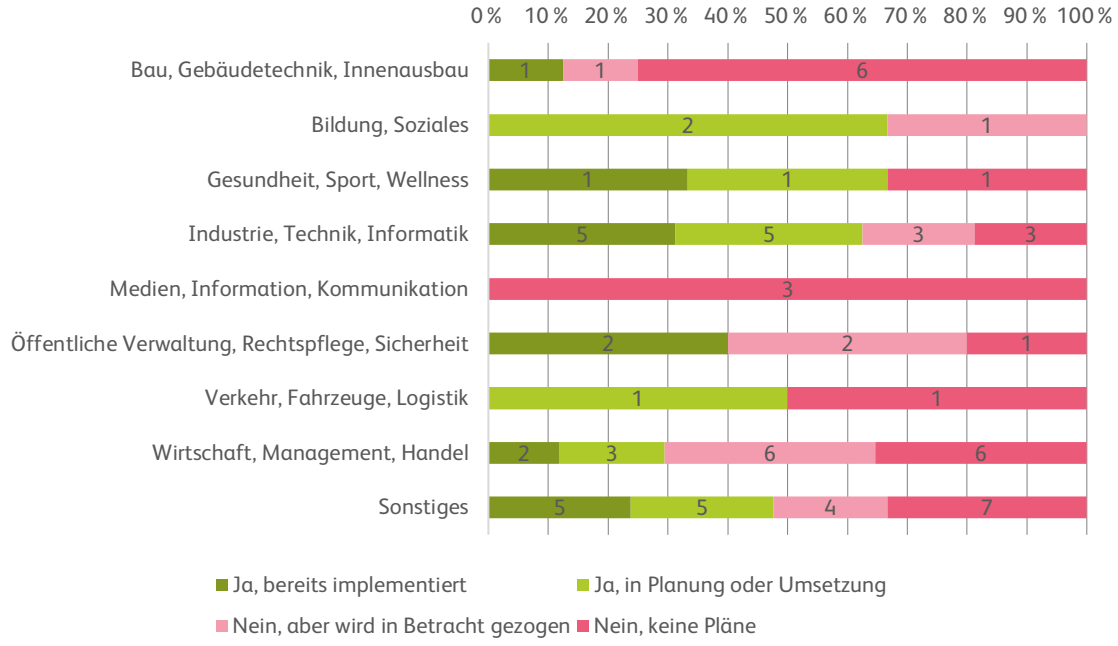

Abbildung 13 – Setzt Ihr Unternehmen derzeit Lösungen zu digitalen Identitäten um oder plant dies zu tun? Kombiniert mit der Branche (n=78)

3 Ergebnisse und Analyse der Umfrage

Die Einführung digitaler Identitäten und verifizierbarer Nachweise in der Schweiz steht an einem entscheidenden Punkt. Die Studie zeigt, dass viele Unternehmen und Behörden bereits erste Schritte in Richtung Digitalisierung unternehmen, jedoch weiterhin Herausforderungen bestehen. In diesem Abschnitt werden die zentralen Ergebnisse der Befragung in Bezug auf das Bewusstsein, Nutzung, wahrgenommene Herausforderungen, potenzielle Vorteile und zukünftige Entwicklungen dargestellt. Ergänzend werden Hypothesen formuliert, die anhand der erhobenen Daten überprüft werden können.

3.1 Bewusstsein und Verständnis digitaler Identitäten

Ein grundlegendes Verständnis digitaler Identitäten ist eine zentrale Vorbedingung und daher essenziell für deren Einführung und Skalierung. Die Ergebnisse der Studie zeigen, dass 20.5 % der Befragten sehr gut informiert sind und 59 % gut informiert. Hingegen schätzen 18 % der Befragten ihr Verständnis als gering ein und 2.6 % geben an, gar kein Verständnis zu besitzen. Damit liegt die Selbsteinschätzung insgesamt eher im positiven Bereich, wobei der Anteil mit geringem oder keinem Verständnis (zusammengerechnet 20.5 %) nicht vernachlässigbar ist und auf anhaltenden Bedarf an Zielgruppenkommunikation und greifbaren Praxisbeispielen hindeutet.

Hypothese 1:

Ein als besser eingeschätztes Verständnis digitaler Identitäten geht mit einem fortgeschrittenem Einführungsgrad (Implementierung oder Planung) innerhalb des Unternehmens einher.

Die Hypothese wurde bestätigt.

Validierung der Hypothese 1

Die Kreuzauswertung zwischen dem selbst eingeschätzten Verständnis digitaler Identitäten und dem Einführungsgrad stützt diese Hypothese klar. In der Gruppe mit sehr gutem Verständnis ist der Anteil der Organisationen, die bereits implementiert haben oder sich in der Planung/Umsetzung befinden, deutlich höher als in den Gruppen mit geringerem Verständnis (6 implementiert, 4 in Planung; n=16). Umgekehrt dominiert bei geringem oder ganz fehlendem Verständnis der Status «keine Pläne» bzw. «wird (nur) in Betracht gezogen».

Der Trend ist jedenfalls deutlich: Organisationen, die digitale Identitäten besser verstehen, befinden sich häufiger in fortgeschritteneren Phasen der Einführung. Gleichzeitig ist zu beachten, dass es sich hier um eine Selbsteinschätzung handelt und die Fallzahlen in einzelnen Verständnisgruppen klein sein können. Der Befund ist daher als Tendenz zu interpretieren, nicht als kausaler Nachweis.

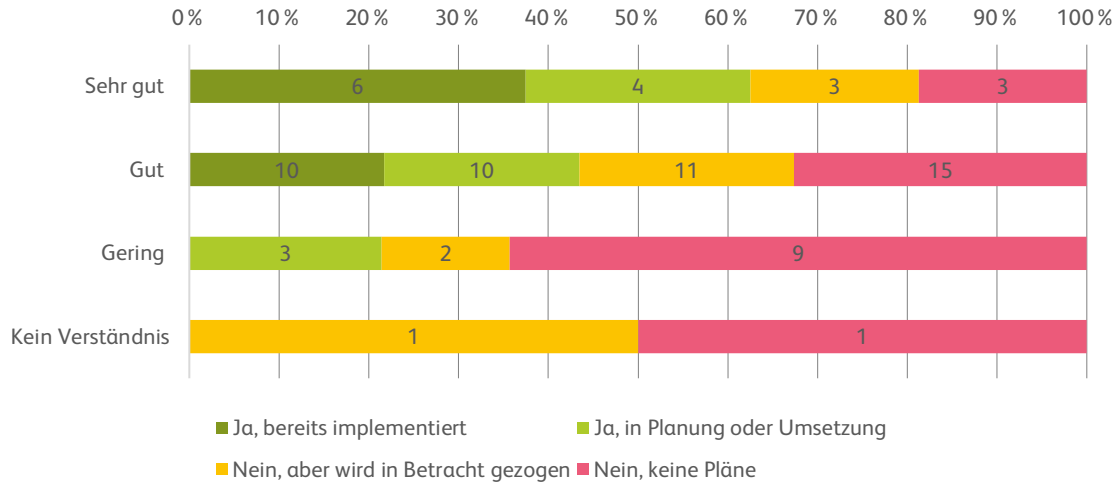

Abbildung 14 – Setzt Ihr Unternehmen derzeit Lösungen zu digitalen Identitäten um oder plant dies zu tun? und Wie würden Sie Ihr Verständnis von digitalen Identitäten bewerten? (n=78)

Hypothese 2:

Grössere Unternehmen haben ein besseres Verständnis digitaler Identitäten als kleinere Unternehmen (z. B. weil sie mehr Ressourcen für IT und digitale Transformation bereitstellen können).

Es kann keine eindeutige Aussage gemacht werden.

Validierung der Hypothese 2

Die Auswertung über die Verteilung des selbst eingeschätzten Verständnisses nach Unternehmensgrösse zeigt kein klares Bild, und zwar über alle Grössenklassen. Auch wenn der aktuelle Stand der digitalen Identitätslösungen im Unternehmen mit betrachtet wird, ändert sich das Bild nicht. Es zeigt sich kein klarer Trend, der die Hypothese stützt.

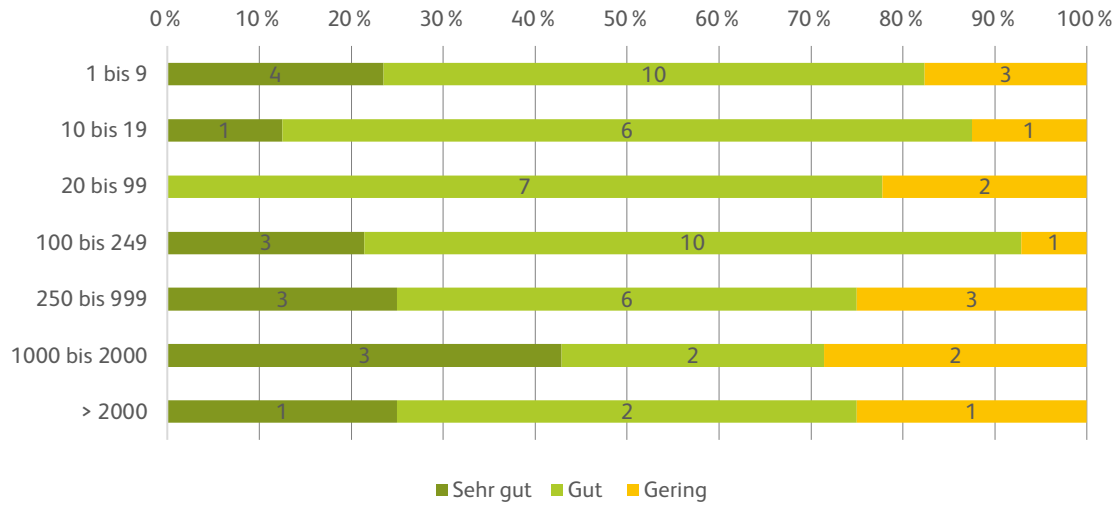

Abbildung 15 – Unternehmensgrösse und Wie würden Sie Ihr Verständnis von digitalen Identitäten bewerten? (n=71)

3.1.1 Aktuelle Einführungsraten

Der Digitalisierungsgrad in der Schweiz variiert grundsätzlich je nach Sektor und Unternehmensgrösse. KMU machen 95 % der Schweizer Wirtschaftslandschaft aus und spielen daher eine entscheidende Rolle bei der digitalen Transformation[21]. Viele KMU konzentrieren sich auf die Digitalisierung interner Prozesse, jedoch steht die Kundschaft und deren Erfahrungen selten im Mittelpunkt. Unternehmen, die sich für den digitalen Wandel entschieden haben, sind der Meinung, dass sich das finanzielle Engagement gelohnt hat.[22]

Im internationalen Vergleich, besonders mit Gesamteuropa, hinkt die Schweiz aber immer noch hinterher. Der eGovernment-Benchmark-Bericht 2024 der Europäischen Kommission zeigt, dass die Schweiz bei der Verfügbarkeit und dem Ausbaustand von elektronischen Dienstleistungen unter dem EU-Durchschnitt liegt. «Während in der EU 88 % der […] Behördendienstleistungen online verfügbar sind, kommt die Schweiz auf eine Online-Quote von 79 %.»[23] [24]

Besonders im Bereich der Transparenz, dem Umgang mit persönlichen Daten sowie bei der Nutzung von Schlüsseltechnologien wie der e-ID besteht Nachholbedarf seitens der Schweiz.

Hypothese 3:

Behörden sind bei der Implementierung digitaler Identitäten weiter fortgeschritten als privatwirtschaftliche Unternehmen, da sie durch regulatorische Anforderungen und staatliche Initiativen gefördert werden.

Die Hypothese wurde bestätigt.

Validierung der Hypothese 3

Unsere Studie zeigt, dass digitale Identitäten aktuell nur in wenigen Unternehmen verwendet werden. Die Auswertung zeigt einen Unterschied zwischen Behörden (n=6) und KMU (n=78) beim Einführungsstand digitaler Identitätslösungen. Bei den Behörden geben 50 % an, bereits implementiert zu haben, weitere 33.3 % befinden sich in Planung oder Umsetzung. Somit sind rund 83 % der Behörden in dieser Stichprobe aktiv.

Bei den KMU ist das Bild deutlich zurückhaltender: 20.5 % sind bereits implementiert und 21.8 % in der Planung/Umsetzung (zusammen sind rund 42 % aktiv). Gleichzeitig geben 21.8 % an, dass das Thema erst in Betracht gezogen wird, und 35.9 % haben «keine Pläne». Insgesamt ist bei KMU also ein grosser Anteil noch in frühen Phasen (Prüfen oder keine Priorität).

Bezogen auf Hypothese 3 stützt die Abbildung die Annahme indikativ: Behörden wirken in dieser Erhebung klar weiter fortgeschritten als privatwirtschaftliche Unternehmen. Das ist konsistent mit der Erwartung, dass staatliche Programme, regulatorische Anforderungen und die Rolle des Staates als Infrastrukturbetreiber eine Nutzung begünstigen.

Wir weisen hier nochmals deutlich auf die geringe Anzahl an Antworten von Behörden hin.

---

[21] Die Digitalisierung der KMU in der Schweiz: ein Schlüsselfaktor https://www.kmu.admin.ch/kmu/de/home/fakten-trends/digitalisierung.html (Schweizer Eidgenossenschaft - KMU Portal, 2026)

[22] PWC Digitalisierung – wo stehen Schweizer KMU? https://www.pwc.ch/de/publications/2016/pwc_digitalisierung_wo_stehen_schweizer_kmu.pdf (PWC, 2025)

[23] Studien der Digitalen Verwaltung CH https://www.digitale-verwaltung-schweiz.ch/publikationen/studien (Digitale Verwaltung Schweiz - Studie, 2026)

[24] eGovernment Benchmark 2024 https://www.digitale-verwaltung-schweiz.ch/publikationen/studien/egovernment-benchmark-2024 (Digitale Verwaltung Schweiz - eGovernment, 2026)

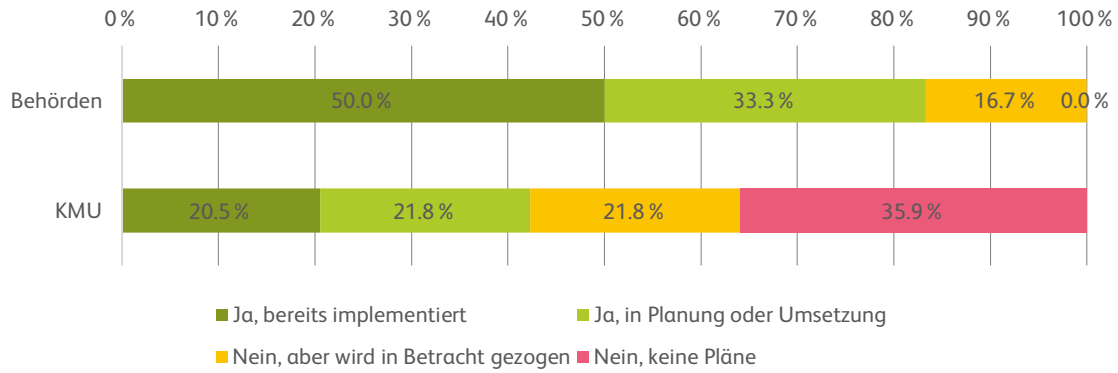

Abbildung 16 – Setzt Ihr Unternehmen oder Ihre Organisation derzeit Lösungen zu digitalen Identitäten um oder plant dies zu tun? (KMU n=78, Behörden n=6)

3.1.2 Herausforderungen bei der Einführung

Trotz der Vorteile digitaler Identitäten bestehen nach wie vor zahlreiche Herausforderungen, die eine flächendeckende Einführung verhindern bzw. verlangsamen.

Hypothese 4:

Unter den Befragten KMU-Repräsentant:innen werde technische und organisatorische Faktoren (Integration, Wissen, Business Case) häufiger als primäre Einführungshürden genannt als rechtliche Faktoren (Regulatorik)

Die Hypothese wurde bestätigt.

Validierung der Hypothese 4

Innerhalb der Auswertung der Studie zeigt sich, dass die Integration in bestehende Systeme am häufigsten als Herausforderung genannt wird bei der Einführung digitaler Identitäten (47.4 %) und damit als zentraler Engpass gesehen wird. Direkt danach folgt mangelndes Wissen/Verständnis (43.6 %) sowie fehlende Geschäftsfälle oder kein Bedarf (39.7 %). Ebenfalls stark vertreten sind Datenschutz- und Sicherheitsbedenken (34.6 %) und das Thema einer fehlenden einheitlichen Lösung (34.6 %). Hohe Implementierungskosten werden von 30.8 % der Befragten genannt, fehlende Infrastruktur von 25.6 %. Deutlich seltener sind regulatorische Bedenken (17.9 %) und eine komplexe Benutzerschnittstelle (15.4 %). «Sonstiges» spielt eine Nebenrolle (9 %). Die Freitextantworten unter «Sonstiges» spiegeln im Kern Themen der Nutzung wider: «Es braucht eine breite Akzeptanz und erfolgreiche Anwendungsfälle, damit die digitale Identität funktioniert», fasst einige Aussagen treffend zusammen. Die übrigen Kommentare nennen fehlende Affinität bzw. Bereitschaft bei der Kundschaft. Hinzu kommt die hohe Sensibilität für Datenschutz und das Narrativ der digitalen Überwachung. Viele warten, bis die offizielle Lösung (swiyu) stabil verfügbar und breit akzeptiert ist. Es zeigt sich also auch in der qualitativen Interpretation, dass Regulatorik eher als Kontextfaktor beschrieben wird, während praktische Umsetzungsthemen den Ausschlag geben.

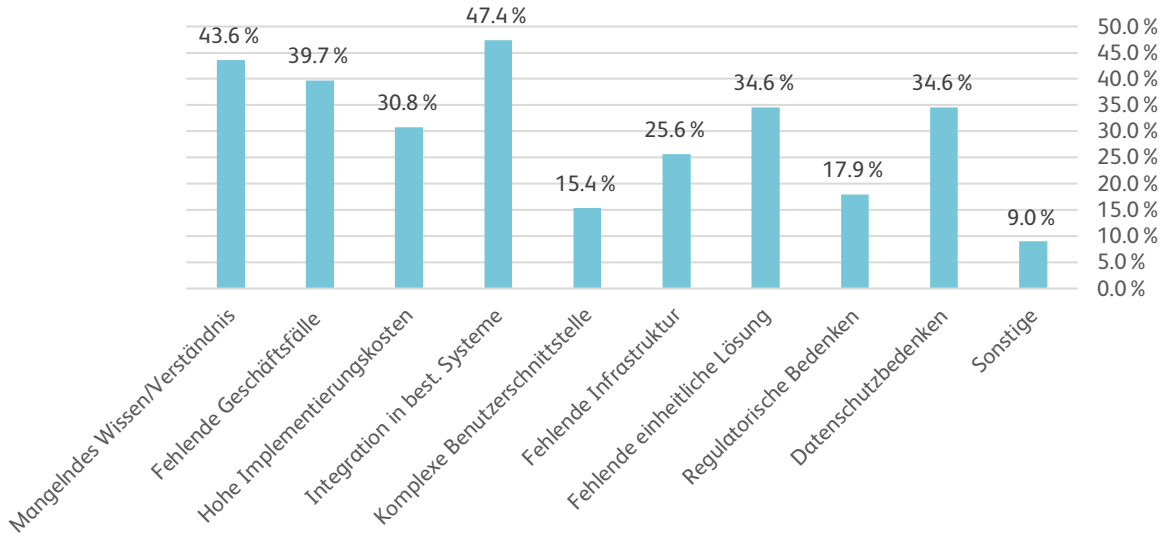

Abbildung 17 – Was sehen Sie als die grössten Herausforderungen bei einer Einführung digitaler Identitäten in Ihrem Unternehmen? (n=78 – Mehrfachauswahl möglich)

Die Verteilung zeichnet also ein typisches Bild für neue, noch nicht etablierte Technologien und Ansätze, die erst Fuss fassen müssen, so wie das bei der Identitäts- und Vertrauenslösung in der Schweiz der Fall ist. Die grössten Hürden sind weniger «Regulation» oder «Benutzerschnittstelle», sondern Technologie und Organisation. Dass Integration auf dem ersten Platz liegt, passt zur Tatsache, dass digitale Identitäten nicht als Einzeltool funktionieren, sondern eine hohe Integration benötigen. Gleichzeitig zeigt der hohe Wert bei mangelndem Wissen und Verständnis, dass in vielen Unternehmen Grundlagen wie etwa Funktionsweise, Verantwortlichkeiten, Nutzen/Mehrwert oder innerbetriebliche Regulatorik noch nicht verankert sind, was wiederum die Entwicklung eines klaren Geschäftsmodells erschwert. Was sich direkt in der dritthäufigsten Hürde widerspeigelt: «fehlende Geschäftsfälle oder kein Bedarf».

Hypothese 5:

Unternehmen sehen die grössten Bedenken bei den Implementierungskosten, während Behörden die Benutzbarkeit in Frage stellen.

Die Hypothese wurde widerlegt.

Validierung der Hypothese 5

Die Vertreter:innen der befragten Behörden nennen die Integration in bestehende Systeme und mangelndes Wissen und Verständnis jeweils mit 66.7 % als grösste Bedenken. Danach folgen hohe Implementierungskosten und fehlende Infrastruktur (je 33.3 %). Seltener sind fehlende Geschäftsfälle/kein Bedarf, regulatorische Bedenken, komplexe Benutzerschnittstelle und eine fehlende einheitliche Lösung (je 16.7 %).

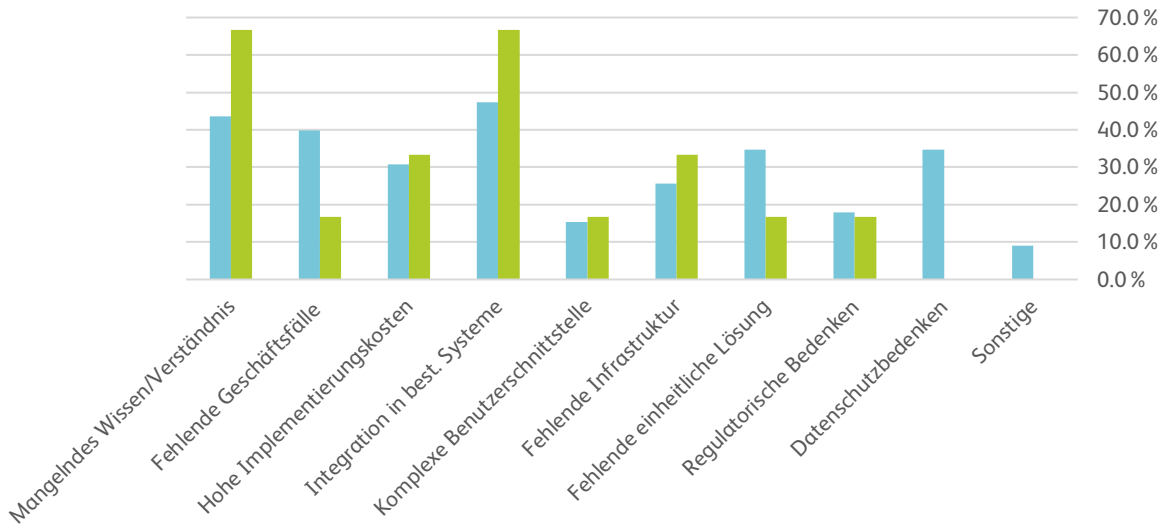

Abbildung 18 – Vergleich der Herausforderungen zwischen KMU (blau) und Behörden (grün) (n=78 KMU, n=6 Behörden – Mehrfachauswahl möglich)

Im Vergleich zur KMU-Auswertung zur äquivalenten Frage (siehe Hypothese 4) zeigt sich, dass Integration für beide Gruppen der zentrale Engpass ist. Auch Wissens- und Verständnislücken sind grosse Herausforderungen. Bei KMU sind fehlende Geschäftsfälle und fehlender Bedarf ein grosser Block, während dies bei Behörden kaum relevant ist. Besonders auffällig: Datenschutz und Sicherheit sind bei KMU relevant, während dies bei Behörden in dieser kleinen Stichprobe gar nicht genannt wird. Das kann bedeuten, dass Behörden diese Aspekte eher als gegebenen Standard ansehen oder sie im Zusammenhang mit anderen Punkten (Regulatorik, Integration, Governance) schon mitdenken. Wegen der geringen Stichprobenanzahl sollte man dies aber als Tendenz lesen und nicht als eindeutigen Beleg.

Die Hypothese hält somit der Datenlage nicht stand: In beiden Gruppen stehen andere Hürden im Vordergrund und weder sind Kosten bei Unternehmen die zentralen Bedenken noch ist es die Benutzbarkeit bei Behörden.

3.1.3 Wahrgenommene Vorteile digitaler Identitäten

Trotz bestehender Herausforderungen sehen viele Unternehmen und Behörden deutliche Vorteile in der Einführung digitaler Identitäten.

Hypothese 6:

KMU nennen als Haupttreiber für digitale Identitäten primär Business-Case-Motive im Sinne der Effizienzsteigerung, während Behörden stärker sicherheits- und compliance-getrieben argumentieren.

Die Hypothese wurde bestätigt.

Validierung der Hypothese 6

Als häufigster Einführungsgrund (84 %) wird von den befragten KMU-Vertreter:innen Effizienzsteigerung genannt. Danach folgt verbesserte Sicherheit (72 %). Reduktion von Betrug liegt im Mittelfeld (48 %).

Kostensenkung und regulatorische/gesetzliche Vorgaben werden gleich häufig genannt (44 %). Am seltensten wird Einhaltung von Vorschriften genannt (30 %).

Als Hauptgründe für die Einführung bei Behörden werden am häufigsten verbesserte Sicherheit und Einhaltung von Vorschriften genannt (je 66.7 %). Danach folgen Effizienzsteigerung sowie regulatorische/gesetzliche Vorgaben (je 50 %). Reduktion von Betrug wird von zwei Befragten genannt (33.3 %). Kostensenkung und Sonstiges spielen eine Nebenrolle (16.7 %).

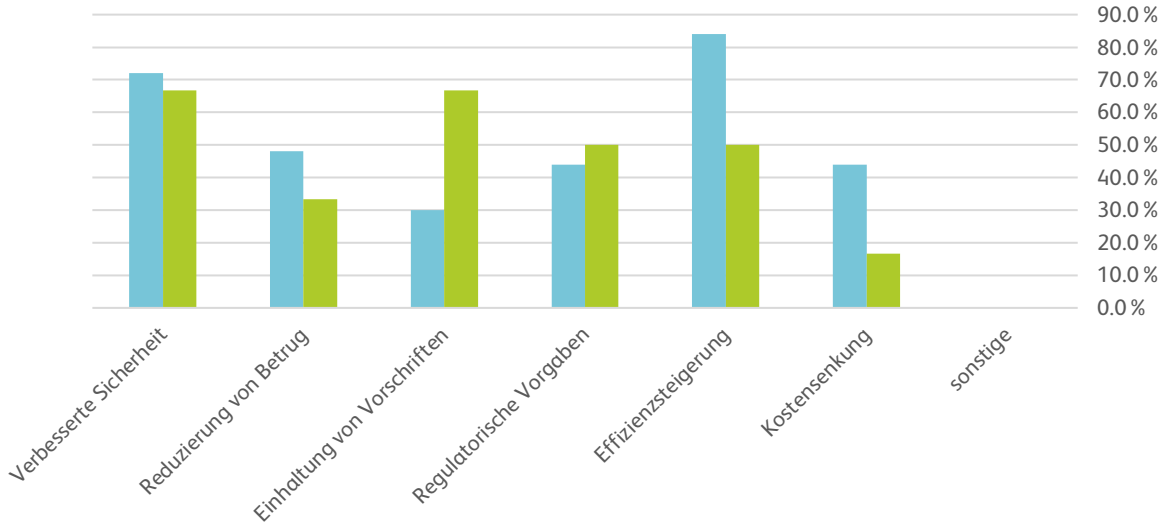

Abbildung 19 – Vergleich der Hauptgründe für die Einführung von digitalen Identitäten zwischen KMU (blau) und Behörden (grün) (n=50 KMU, n=6 Behörden – Mehrfachauswahl möglich)

Die Verteilung zeigt somit, dass digitale Identitäten in der Praxis bei den Unternehmen primär als Thema der Operationalisierung verstanden werden. Effizienzgewinne stehen klar vor reinen Compliance-Motiven. Sicherheit bleibt aber ein sehr starker Treiber, was gut zu klassischen Identitätsprozessen (Zugriffe, Verifizierung) passt. Für Behörden wird die Einführung digitaler Identitäten primär unter Sicherheits- und Compliance-Gesichtspunkte betrachtet. Effizienz ist wichtig, aber eher als unterstützender Nutzen. Reine Kostenargumente sind deutlich weniger relevant, was gut zur Logik des öffentlichen Sektors passt.

Zusammenfassend kann also geschlossen werden, dass die Hypothese korrekt ist und durch die Auswertung gestützt wird.

Hypothese 7:

Unternehmen sehen digitale Identitäten primär als Lösung für Identitätsverifizierung und Zugriff, während datenbezogene Anwendungsfälle (Verwaltung von Kunden-, Mitarbeitenden-, Partnerdaten) deutlich nachrangig sind.

Die Hypothese wurde bestätigt.

Validierung der Hypothese 7

Am häufigsten werden digitale Identitäten im Kontext der Identitätsverifizierung gesehen (84 %). Danach folgen datenbezogene Anwendungsfälle: Verwaltung von Kundendaten (42 %) und Verwaltung von

Mitarbeitendendaten (34 %). Am seltensten wird die Verwaltung von Lieferanten-/Partnerdaten genannt (26 %).

Da Mehrfachnennungen möglich waren, summieren sich die Prozente nicht zu 100 % auf.

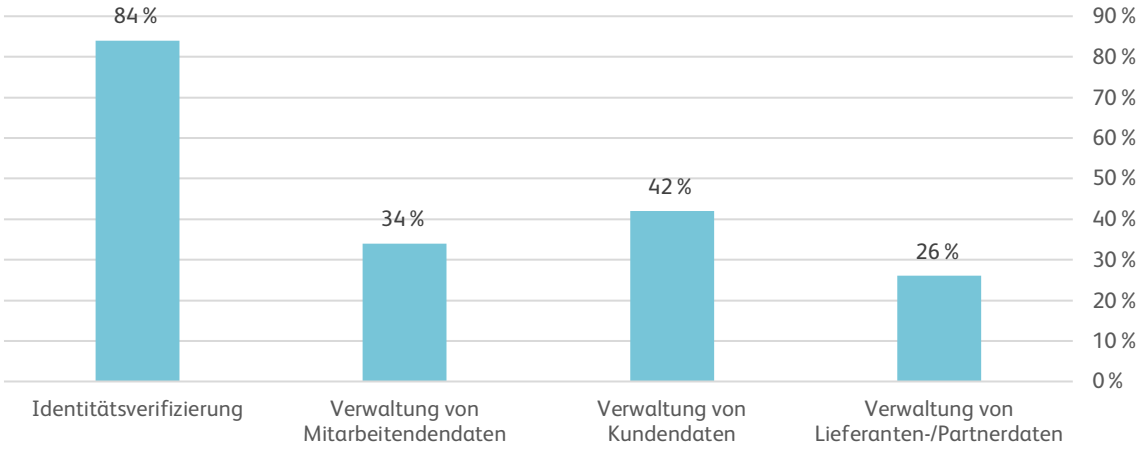

Abbildung 20 – In welchen Bereichen Ihres Unternehmens werden digitale Identitäten genutzt oder könnte genutzt werden? (n=50 – Mehrfachauswahl möglich)

Die Verteilung zeigt eine klare Priorität: Digitale Identitäten werden primär als Vertrauens- und Zugangsthema verstanden (Identitätsprüfung als Basisfunktion). Die Verwaltung von Daten (sowohl von Kundinnen und Kunden, als auch von Mitarbeitenden) sind relevant, aber deutlich nachgelagert. Dies vermutlich, weil sie stärker von bestehenden Systemen abgedeckt werden und der Mehrwert weniger unmittelbar greifbar ist.

Daher hält die Hypothese: Identitätsverifizierung ist die mit Abstand meistgenannte Anwendung, während die drei Datenverwaltungsfälle (insbesondere Partner- und Lieferantendaten) deutlich darunter liegen,

Hypothese 8:

Die Grösse der Unternehmen spielt bei der Beurteilung der wirtschaftlichen Effekte der digitalen Identität keine wesentliche Rolle. Weiterhin erwarten die meisten Unternehmen keinen direkten Effekt digitaler Identitäten auf Umsatz oder Gewinn; die erwarteten Vorteile werden eher als Prozess- und Kostenthema verstanden.

Die Hypothese wurde bestätigt.

Validierung der Hypothese 8

Die vorliegende Hypothese konnte durch die Analyse bestätigt werden, da in nahezu allen Grössenklassen «kein Effekt» die häufigste oder eine der dominierenden Antworten ist – «mehr Umsatz» bleibt selten. Die Freitextantworten unter «Sonstiges» stützen zusätzlich, dass der Business Case primär über Effizienz und (mittelfristige) Kostensenkung gedacht wird, und nicht über direkte Umsatzsteigerung.

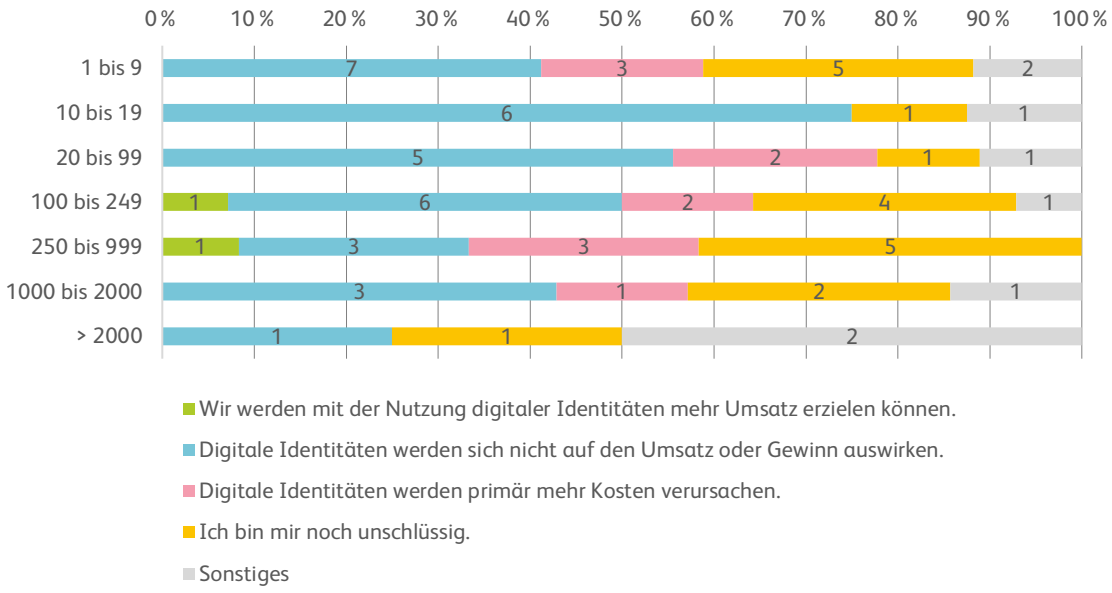

Abbildung 21 – Wie beurteilen Sie einen möglichen wirtschaftlichen Effekt für Ihre Organisation? Kombiniert mit der Unternehmensgrösse (n=71)

Ein klarer Trend ist nicht sichtbar. Was fast über alle Grössenklassen hinweg auffällt: Es wird kein spürbarer Effekt auf Umsatz und Gewinn vermutet. Mehr Umsatz erwarten sehr wenige Personen. Die grösste wirtschaftliche Unsicherheit liegt im Segment 250 bis 999 Mitarbeitende (höchster «unsicher»-Anteil). Bei sehr grossen Unternehmen ist wegen der kleinen Fallzahlen (n=4) keine zuverlässige Aussage möglich.

Die Freitextantworten unter «Sonstiges» lassen sich in drei inhaltliche Pakete bündeln, welche darüber hinaus gut zum Gesamtbild passen: Viele Unternehmen sehen den Vorteil digitaler Identitäten primär bei Effizienz und langfristiger Kostensenkung und weniger als Umsatztreiber.

1. Effizienz und Prozessoptimierung
   Mehrere Antworten zielen direkt auf bessere Abläufe innerhalb der Unternehmen ab: Prozesse optimieren, mehr Effizienz, Zeit- und Kostenersparnis. Das ist im Kontext digitaler Identitäten logisch, da der unmittelbare Nutzen von digitalen Identitätssystemen oft nicht Umsatz ist, sondern weniger manuelle Prüfung, weniger Medienbrüche, schnelleres Onboarding und sauberere Zugriffsprozesse.

2. Kostenlogik
   Ein Teil der Personen formuliert explizit eine Kostenkurve: «Höhere Kosten zu Beginn … aber mittel- bis langfristig geringere Betriebskosten» sowie die Reduktion von operationellen Aufwänden und Kosten. Es geht nicht zwingend um dauerhaft höhere Kosten, sondern um Einmalkosten (Setup, Integration, Change) mit langfristig erwarteter Entlastung im Betrieb.

3. Keine Relevanz bzw. kein Effekt
   Aussagen wie «kein Bedarf» oder «kein (wirtschaftlicher) Effekt» legen nahe, dass die Anwendungsfälle im Unternehmen fehlen.

3.1.4 Vertrauen in Technologie und Infrastruktur des Bundes

Ein entscheidender Faktor für die Einführung digitaler Identitäten ist das Vertrauen in die zugrunde liegende Technologie und die Vertrauensinfrastruktur des Bundes selbst. Das Thema Vertrauen ist in der Schweiz besonders sensibel. In den Medien und der Öffentlichkeit wurde das Thema e-ID politisch bereits mehrfach

intensiv diskutiert und letztlich mit der Volksabstimmung vom 28.09.2025 angenommen – wenn auch knapp.[25]

Das für die Vertrauensinfrastruktur zuständige Team von BJ (Bundesamt für Justiz) und BIT (Bundesamt für Informatik) pflegten von Anfang an eine sehr offene und transparente Kommunikationskultur. Generell ist der Bund beim swiyu-Ökosystem sichtbar auf Transparenz und Partizipation ausgerichtet (Public Beta, offene technische Dokumentation und Community-Strukturen).[26]

Trotzdem wurden einige Aspekte kritisiert. Dabei handelt es sich vor allem um die Angst vor einer Überidentifikation und dem Missbrauch von Identitätsdaten trotz entsprechendem Datenschutzgesetz.

Die zwei Ebenen von Vertrauen

Institutionelles Vertrauen (Governance Trust): Transparenz, Zuständigkeiten, Aufsicht, nachvollziehbare Entscheidprozesse.

Digitales Vertrauen (Technical Trust): Die Fähigkeit, Aussagen aus Nachweisen maschinenlesbar und kryptografisch zu prüfen – also nicht «Vertrauen in eine Organisation», sondern verifizierbare Fakten durch autorisierte Aussteller.

Beide Ebenen sind Fundament: Institutionelles Vertrauen schafft Legitimität und Akzeptanz, technische Verifizierbarkeit schafft Skalierbarkeit in Prozessen

In der Befragung zeigt sich beim Thema Datenschutz und Sicherheit digitaler Identitäten eine mehrheitlich positive, aber nicht vorbehaltlose Haltung. 19 % geben an, sehr hohes Vertrauen zu haben, während 45.2 % ihr Vertrauen immerhin noch als hoch mit Verbesserungsbedarf einstufen. Weitere 23.8 % liegen im mittleren und 11.9 % im niedrigen Bereich («gering» oder «sehr gering»).

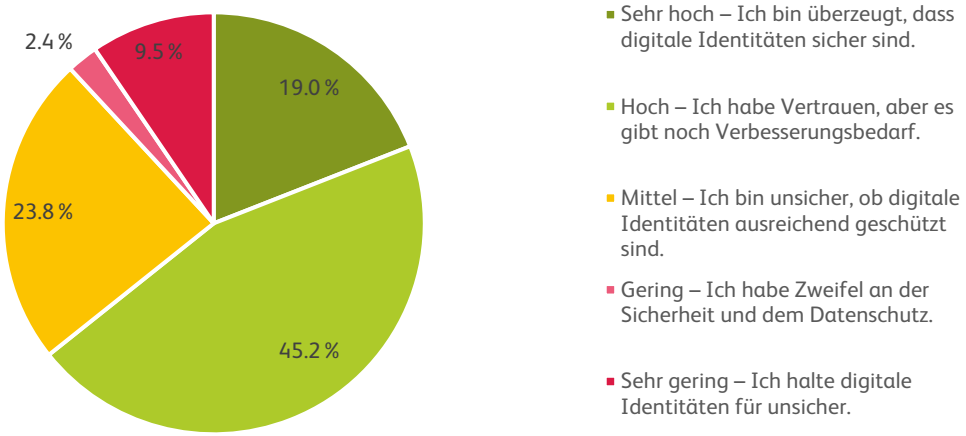

Abbildung 22 – Wie hoch ist Ihr Vertrauen in den Datschenschutz und in die Sicherheit digitaler Identitäten? (n=84 – KMU und Behörden)

[25] Detaillierte Ergebnisse, Abstimmung vom 28.9.2025 https://abstimmungen.admin.ch/details/2025-09-28?proposalId=6790 (Bundesamt für Statistik, 2025)

[26] swiyu Trust Infrastructure Community auf Github https://github.com/swiyu-admin-ch/community (Schweizer Eidgenossenschaft - Github, 2026)

Insgesamt überwiegt innerhalb der Studien ein grundsätzliches, aber kein blindes Vertrauen: Viele akzeptieren digitale Identitäten grundsätzlich, erwarten jedoch eine saubere Umsetzung, transparente Sicherheitsmechanismen und klare Verantwortlichkeiten seitens des Bundes. Gleichzeitig ist der Anteil mit mittlerem oder geringem Vertrauen (rund ein Drittel) ein Hinweis darauf, dass Sicherheits- und Datenschutzkommunikation sowie nachvollziehbare Schutzmassnahmen entscheidend bleiben für breite Akzeptanz und Skalierung.

Bezüglich Vertrauen in die Infrastruktur des Bundes ist das Bild ähnlich. Am häufigsten wird die Infrastruktur als hoch vertrauenswürdig, aber mit Optimierungspotenzial eingeschätzt (36.9 %). Ein weiterer grosser Teil betrachtet die Infrastruktur als noch nicht ausgereift (28.6 %) und sehr hohes Vertrauen geben 20.2 % der Befragten an. Eine skeptischere Einschätzung ist seltener: sehr geringes Vertrauen geben 8.3 % der Befragten an und geringes Vertrauen deren 6 %.

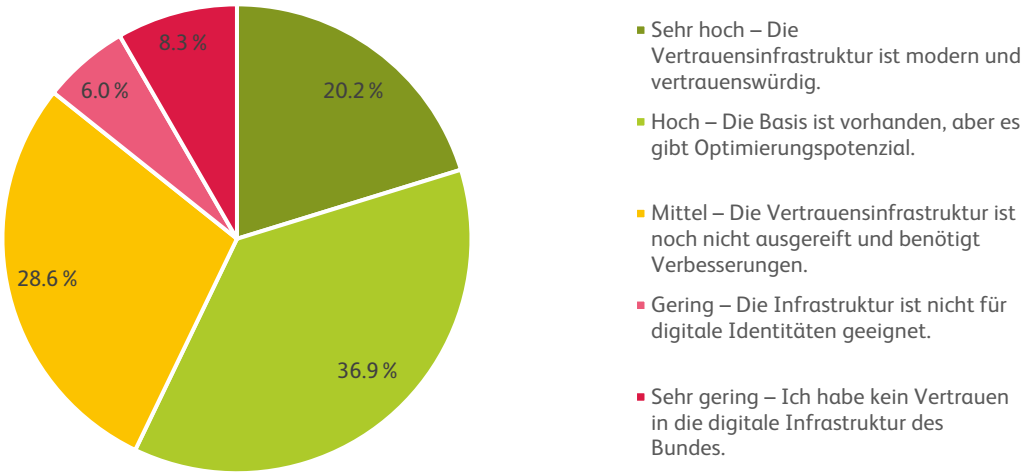

Abbildung 23 – Wie hoch ist Ihr Vertrauen in die Vertrauensinfrastruktur des Bundes? (n=84 – KMU und Behörden)

Insgesamt überwiegt hinsichtlich der gestellten Vertrauensinfrastruktur eine vorsichtig positive Haltung. Viele sehen eine tragfähige Basis, aber erwarten noch Verbesserungen bezüglich Reifegrad, Stabilität und bei Umsetzung und Governance. Gleichzeitig zeigt der relevante Anteil mit mittlerem Vertrauen, dass das Vertrauen nicht nur von der Idee der Infrastruktur abhängt, sondern stark von einer nachvollziehbaren Ausgestaltung, von Transparenz und einem reibungslosen Betrieb sowie einer transparenten begleitenden Kommunikation des Bundes.

Hypothese 9:

Vertrauen in Datenschutz/Sicherheit digitaler Identitäten ist positiv mit Vertrauen in die Vertrauensinfrastruktur des Bundes gekoppelt.

Die Hypothese wurde bestätigt.

Validierung der Hypothese 9

Fasst man beide Einschätzungen als Kreuzdarstellung zusammen, so ist (wie in der untenstehenden Grafik dargestellt) eine ziemlich deutliche Kopplung zu erkennen. Wer Datenschutz und Sicherheit digitaler Identitäten als hoch einschätzt, vertraut meistens auch der Vertrauensinfrastruktur des Bundes und umgekehrt. Das Vertrauen in digitale Identitäten scheint stark davon abzuhängen, als wie glaubwürdig und reif die staatliche Vertrauensinfrastruktur wahrgenommen wird. Dieser Zusammenhang ist logisch nachvollziehbar.

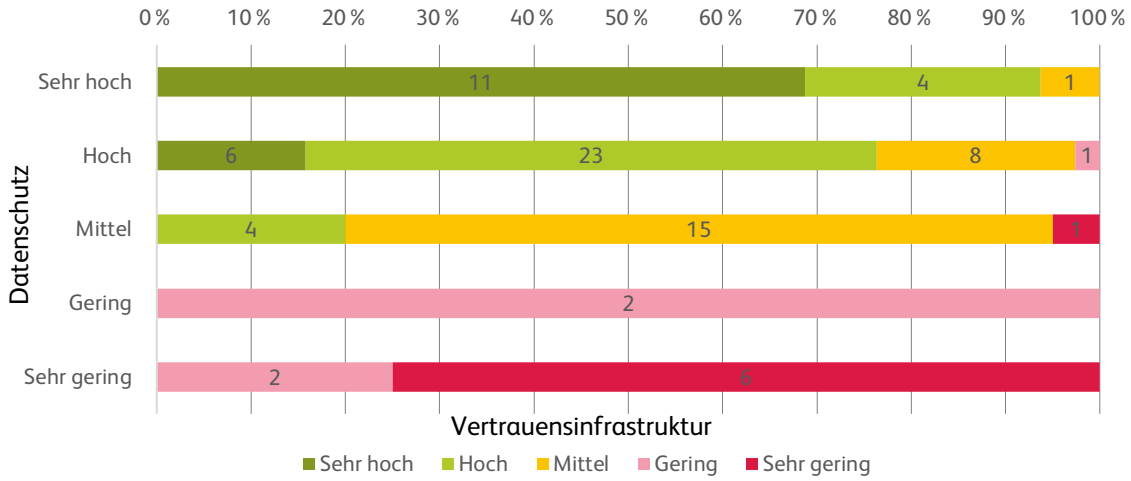

Abbildung 24 – Kreuzdarstellung: Wie hoch ist Ihr Vertrauen in den Datenschutz und die Sicherheit digitaler Identitäten? und Wie hoch ist Ihr Vertrauen in die Vertrauensinfrastruktur des Bundes? (n=84 – KMU und Behörden)

Hypothese 10:

Unternehmen mit hohem Vertrauen in die digitale Infrastruktur des Bundes haben weniger Bedenken hinsichtlich regulatorischer Unsicherheiten.

Die Hypothese wurde bestätigt.

Validierung der Hypothese 10

Die Auswertung stützt die Hypothese. Mit steigendem Vertrauen in die Vertrauensinfrastruktur sinkt tendenziell der Anteil jener, die regulatorische Bedenken angeben. Bei sehr hohem Vertrauen äussert nur eine sehr kleine Minderheit regulatorische Unsicherheiten, bei hohem und mittlerem Vertrauen bleibt der «Bedenken»-Anteil ebenfalls relativ niedrig. Am deutlichsten kippt das Bild bei sehr geringem Vertrauen, wo sich die Antworten etwa die Waage halten.

Die unteren Vertrauenskategorien haben kleine Fallzahlen, und «gering» wirkt weniger eindeutig als «sehr gering». Trotzdem zeigt die Gesamttendenz klar in Richtung mehr Vertrauen – weniger regulatorische Unsicherheit.

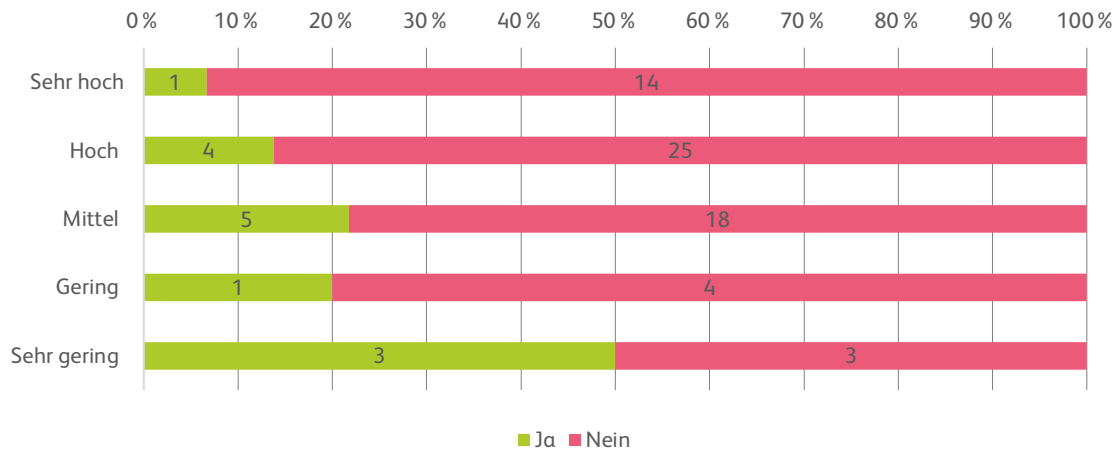

Abbildung 25 – Kreuzdarstellung: Wie hoch ist Ihr Vertrauen in die Vertrauensinfrastruktur des Bundes? und Was sehen Sie als die grössten Herausforderungen bei einer Einführung digitaler Identitäten in Ihrem Unternehmen? Antwort: Regulatorische Bedenken (n=78)

3.1.5 Wahrnehmung von Fake-Identitäten und KI-generiertem Identitätsbetrug

Ein wachsendes Problem ist der Missbrauch von Künstlicher Intelligenz (KI) zur Erstellung gefälschter Identitäten. Dazu gehören Deep-Fakes und Voice Clones, welche bei herkömmlichen digitalen Identifikationsverfahren potenziell nicht aufgegriffen werden. Aufgrund fehlender sicherer Identitätsnachweise hat sich im digitalen Raum die Identitätsprüfung über Videoverfahren, Sprachnachrichten oder über Bilder in Abgleich mit Identitätsdokumenten (z. B. Reisepass), E-Mail und generell über Zweitgeräte (z. B. via SMS oder Authenticator Apps) durchgesetzt. Das ging zwar lange gut, aber heute können KI-Tools zur Imitation von Stimmen oder zur Erstellung von qualitativ hochwertigen Fake-Bildern/Videos genutzt werden. Auch das «Kapern» von E-Mail-Konten und Mobilfunknummern, z. B. über Phishing[27], ist grundsätzlich möglich und verbreitet sich weiter stark. Digitale Nachweise können hier helfen und solchen Trenderscheinungen entgegenwirken.

Die Befragten stufen KI-gestützte Fälschungen mehrheitlich als relevantes Risiko ein: 36.9 % sehen ein mittleres Risiko, weitere 28.6 % ein hohes Risiko und 20.2 % sogar ein sehr hohes Risiko. Demgegenüber halten 11.9 % das Risiko für gering. Gar kein Risiko sehen nur 2.4 % der Befragten.

[27] Unter Phishing versteht man die Nutzung von gefälschten, imitierten Nachrichten oder E-Mails, um Benutzer:innen zum falschen Login und damit zur Weitergabe ihrer Passwörter zu bewegen.

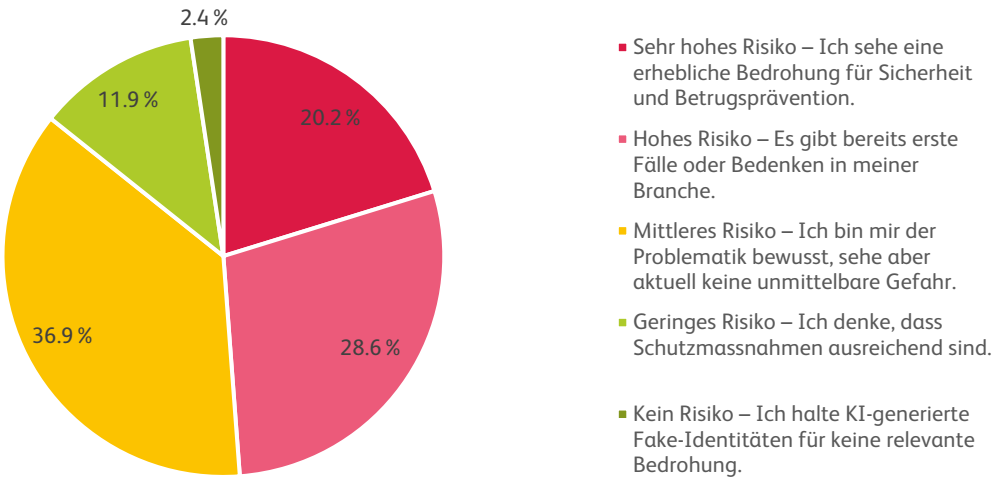

Abbildung 26 – Inwieweit sehen Sie KI-generierte Fake-Identitäten (Deepfake-Identitäten, synthetische Identitäten) als Risiko für Ihr Unternehmen? (n=84 – KMU und Behörden)

Insgesamt wird das Risiko klar ernst genommen: Rund 86 % identifizieren ein mindestens «mittleres Risiko» und fast die Hälfte (49 %) sogar eine «hohes» oder «sehr hohes». Das spricht dafür, dass Deepfakes und synthetische Identitäten in vielen Unternehmen nicht nur als theoretische, sondern als reale Bedrohung wahrgenommen werden, die Massnahmen erfordert im Rahmen von Betrugsprävention, Identitätsprüfung und der generellen Sicherheit. Gleichzeitig zeigt der Anteil «mittleres Risiko», dass zwar Bewusstsein vorhanden ist, aber (noch) kein akuter Handlungsdruck empfunden wird. Dies, weil oft konkrete Vorfälle fehlen oder bestehende Gegenmassnahmen als ausreichend wahrgenommen werden.

Passend hierzu erwartet eine Mehrheit (63.8 %), dass digitale Identitäten bei der Verhinderung von Fake-Identitäten helfen können.

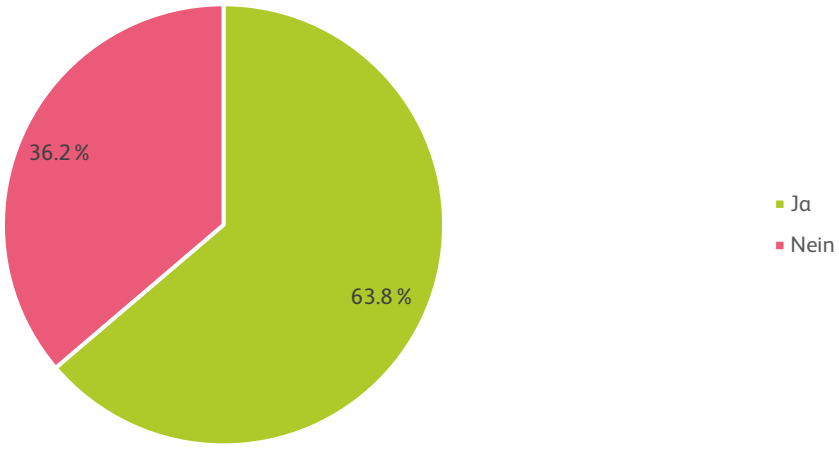

Abbildung 27 – Helfen digitale Identitäten Ihrer Meinung nach bei der Verhinderung von Fake Identitäten? (n=69)

Hypothese 11:

Unternehmen, welche digitale Identitäten nutzen oder deren Nutzung planen, haben eine höhere Sensibilität für das Risiko von Fake-Identitäten als Unternehmen ohne digitale Identitäten.

Es kann keine eindeutige Aussage gemacht werden.

Validierung der Hypothese 11

Die untenstehende Grafik zeigt keinen Zusammenhang zwischen Einführungsreife und Risikowahrnehmung bei KI-generierten Fake-Identitäten. Generell wird das Risiko als hoch bis sehr hoch eingestuft.

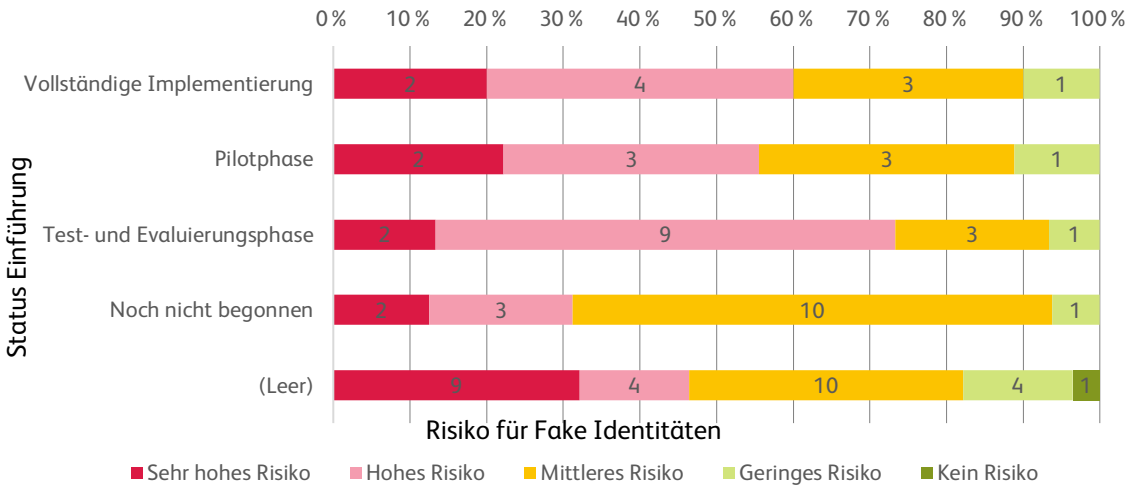

Abbildung 28 – Kreuzdarstellung: Inwieweit sehen Sie KI-generierte Fake-Identitäten (Deepfake-Identitäten, synthetische Identitäten) als Risiko für Ihre Organisation? und In welchem Status befindet sich die Einführung von digitalen Identitäten in Ihrem Unternehmen? (n=78)

3.1.6 Zukünftige Pläne und Trends

Dies ist die erste Durchführung dieser Studie. Deshalb war es für uns besonders wichtig nachzufragen, wie Unternehmen und Behörden die Zukunft von digitalen Nachweisen in der Schweiz beurteilen.

Für die Perspektive bis und mit 2028 zeigt die Umfrage einen vorsichtig-pragmatischen Kurs: 50.6 % möchten aktiv werden und die Prüfung von digitalen Identitäten in ihre Systeme einbauen, erste Pilotprojekte starten oder aktiv digitale Identitäten ausstellen. 27.7 % werden den Markt beobachten und 21.7 % werden vorerst nicht aktiv.

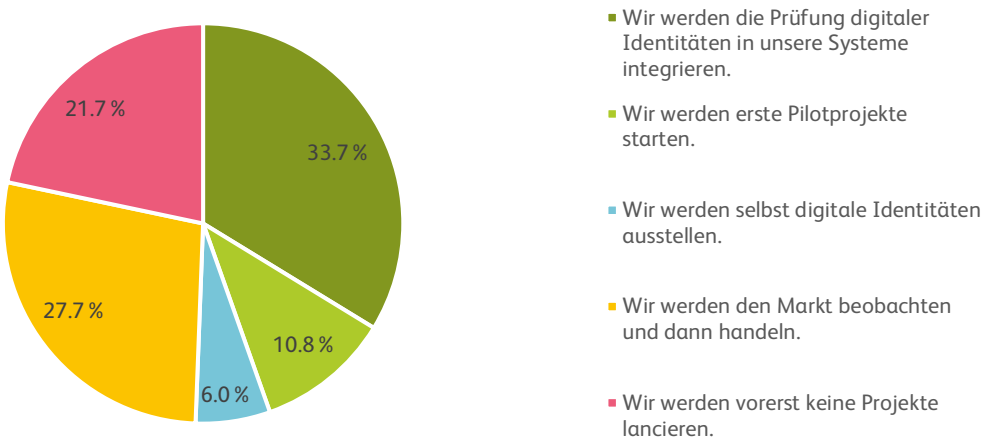

Abbildung 29 – Wie sehen Sie die Entwicklung von digitalen Identitäten in Ihrem Unternehmen in den nächsten 3 Jahren (bis inkl. 2028)? (n=83 – KMU und Behörden)

Viele Befragte sind zwar grundsätzlich bereit (Integration oder Beobachtung), aber ein substanzieller Anteil bleibt auf dem Kurs «beobachten». Das spricht für ein Umfeld, in dem Unternehmen den Nutzen sehen, aber weiter auf Reife, Standards und klare Rahmenbedingungen warten, bevor sie stärker investieren. Dies deckt sich mit anderen Antworten innerhalb dieser Studie. Aktiv «vorne mitspielen» (d. h. selbst ausstellen) ist vorerst noch die Ausnahme. Wie oben erwähnt, passt das gut zu einer frühen Marktphase, in der die meisten eher Nutzende und Integratoren als Issuer sein wollen.

Die eben angeführte Auswertung zeigt, dass viele Organisationen, im engeren Sinne Unternehmen, bis 2028 eher vorsichtig agieren und häufig noch auf Reife, Standards und klare Rahmenbedingungen warten. Daraus ergibt sich unmittelbar die Anschlussfrage: Verfügen Unternehmen überhaupt über die dafür nötigen Kompetenzen und Ressourcen oder braucht es zusätzliche Unterstützung? Genau darauf zielt das nächste Diagramm zum Schulungs- und Unterstützungsbedarf ab.

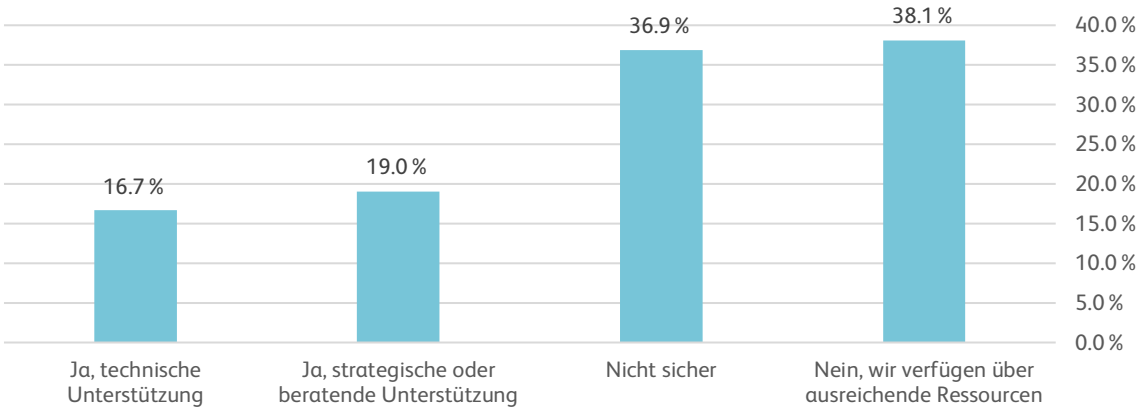

Abbildung 30 – Benötigt Ihr Unternehmen (zusätzliche) Schulungen oder Unterstützung zur Implementierung von digitalen Identitäten? (n=84 – KMU und Behörden – Mehrfachauswahl möglich)

Am häufigsten sind zwei Haltungen: «Nicht sicher» (36.9 %) und «Nein, wir verfügen über ausreichende Ressourcen» (38.1 %). Gleichzeitig wünschen sich 16.7 % der Unternehmen technische Unterstützung und 19 % strategische bzw. beratende Unterstützung. Dass sich diese beiden «Ja»-Optionen grundsätzlich überschneiden können liegt nahe, da in der Realität einige der Befragten während der Anfangsphase sowohl technische als auch beratende Unterstützung benötigen.

Das Bild zeigt also allgemein weniger «wir brauchen sicher nichts», sondern weisst eher auf Unklarheit plus Reifegrad-Fragen hin. Viele Unternehmen sind noch nicht weit genug, um den eigenen Bedarf sauber einschätzen zu können, während ein relevanter Teil bereits konkrete Hilfe erwartet. Das passt gut zu den zuvor genannten Haupthürden wie Wissenslücken und Integration in bestehende Systeme.

4 Geschäftsfälle für Digitale Identitäten in KMU und Behörden

Digitale Identitäten und verifizierbare Nachweise bieten eine Vielzahl von Anwendungsmöglichkeiten für kleine und mittlere Unternehmen sowie für öffentliche Verwaltungen. Sie ermöglichen eine sichere, effiziente und automatisierte Identitätsprüfung, reduzieren Betrugsrisiken und vereinfachen Compliance-Anforderungen. Die folgenden Use Cases zeigen praxisnahe Anwendungsfälle für beide Sektoren, die jedoch nicht ein direkter Teil der Studie waren.

Anhand von je fünf Geschäftsfällen möchten wir aufzeigen, wie konkrete Lösungen aussehen können und was dabei zu erwarten ist.

4.1 Geschäftsfälle für KMU

4.1.1 Kunden-Onboarding und KYC

Bei einem Schweizer Finanzdienstleister eröffnet eine Kundin online ein Konto. Dazu gehört eine KYC («Know your customer»)-Prüfung. Statt Video-Ident bestätigt die Kundin im swiyu Wallet ihre e-ID. Beim Onboarding scannt sie im Browser einen QR-Code, sieht in swiyu, welche Daten angefragt werden (z. B. Name, Geburtsdatum) und gibt diese frei. Die Firma verifiziert dann die kryptografische Signatur und prüft den Aussteller im Basis-Register.

Vorteile gegenüber heute:

- Weniger Abbrüche (kein Video-Call, kein Upload der Ausweiskopie)
- Schnellere Freigabe, weniger manuelle Prüfungskosten
- Geringeres Datenschutzrisiko (keine ID-Scans im System, nur verifizierte Attribute)

4.1.2 Altersnachweis im Online-Shop

Ein KMU verkauft online Produkte mit Altersgrenze. Beim Checkout erscheint «Altersnachweis nötig». Der Kunde scannt den QR-Code mit dem swiyu Wallet, die wiederum gegenüber dem Shop nur bestätigt, dass der Kunde «über 18» ist, also ohne das Geburtsdatum zu übermitteln. So ist eine sichere, aber datensparsame Überprüfung möglich.

Vorteile gegenüber heute:

- Kein Upload von Ausweisfotos (weniger Daten, geringeres Missbrauchsrisiko)
- Weniger Betrug, keine Fake-IDs
- Schneller Checkout und damit eine höhere Conversion für den Shop

4.1.3 Digitale Mitarbeitenden-Nachweise

Ein KMU stellt einer neuen Mitarbeiterin ein «Mitarbeitender der Firma X»-Zertifikat aus (z. B. Rolle: Servicetechnikerin). Die Mitarbeiterin bestätigt bei einem Partner (z. B. Rechenzentrum oder Industrieanlage) über das swiyu Wallet ihren Rollen-Nachweis. Der Partner verifiziert Signatur und Gültigkeit und kann auch prüfen, ob das Zertifikat widerrufen wurde.

Vorteile gegenüber heute:

- Keine physischen Badges, keine E-Mail-Bestätigungen, weniger Social Engineering
- Rollenwechsel und Austritt kann schneller wirksam werden
- Besser auditierbar (wer hatte wann welche Rolle)

4.1.4 Nachweisprüfung statt Dokumentkopien sammeln

Ein HR-Dienstleister braucht für eine Entscheidung nur «Wohnsitz im Kanton ZH» oder «Name stimmt mit Vertrag überein». Anstelle einer Wohnsitzbestätigung als PDF oder Scan bittet er um einen verifizierbaren Nachweis. Der Kunde teilt den Nachweis über das swiyu Wallet und der KMU-Verifier speichert nur das Prüfergebnis, nicht die Ausweiskopie.

Vorteile gegenüber heute:

- Deutlich weniger sensible Daten im KMU-System (geringeres Datenschutz-Risiko)
- Weniger Fälschungen (kryptografische Signatur statt «PDF sieht echt aus»)
- Widerruf statt ständigem Überprüfen und schnellere Prozesse ohne Medienbruch

4.1.5 Qualifikationen

Ein Spitaldienstleister beauftragt externe Pflegefachpersonen. Die Fachperson teilt aus dem swiyu Wallet ein Qualifikations-Zertifikat (z. B. anerkannte Ausbildung, Berufsrolle, ggf. Gültigkeit) direkt im Bewerbungsportal per QR-Code Workflow. Der Dienstleister prüft Signatur und Herausgeber. Er akzeptiert die Bewerbung ohne manuelle Dokumentprüfung.

Vorteile gegenüber heute:

- Keine eingescannten Diplome und damit weniger Fälschungen
- Schnellere Besetzung, weniger Hin-und-her
- Bei Rezertifizierung oder Entzug kann ein aktueller Status nachgewiesen werden

4.2 Geschäftsfälle für Behörden

4.2.1 Behörden-Login (AGOV)

Eine Bürgerin will online ihre Steuererklärung beim Kanton einreichen. Auf dem Portal wählt sie «Login mit AGOV», bekommt einen QR-Code, scannt ihn mit der AGOV access App und ist ohne Passwort eingeloggt.

Hierzu ist keine e-ID nötig. Die e-ID im swiyu Wallet kann jedoch als besonders sicherer Zugang zu AGOV verwendet werden, also als Login-Faktor für AGOV. In der Public Beta wird das auch praktisch gezeigt: «AGOV-Integration – Sich mit der Beta-ID via AGOV bei der fiktiven Behörde Alphaoffice einloggen».[28] AGOV bleibt weiterhin als Login-Methode bestehen.

Vorteile gegenüber heute:

- Kein Passwort und kein Passwort-Reset. Damit weniger Supportaufwand, geringeres Phishing-Risiko
- Einheitlicher Login über verschiedene Behördenebenen (Bund/Kanton/Gemeinde)
- Schnellerer Zugang, weniger Abbrüche bei E-Services

4.2.2 Wohnsitzbestätigung als digitaler Nachweis

Eine Person zieht um und braucht für eine Versicherung die Wohnsitzbestätigung. Sie bestellt diese im Gemeinde-Portal. Statt Papier bekommt sie den Nachweis direkt im swiyu Wallet ausgestellt und kann ihn mit der Versicherung digital teilen. Dieser kann die Bestätigung digital prüfen.

Vorteile gegenüber heute:

- Keine Schalterzeit, kein Papier, kein Scan per E-Mail
- Weniger Fälschungen: Nachweis ist kryptografisch verifizierbar

---

[28] Public Beta https://www.eid.admin.ch/de/public-beta (Schweizer Eidgenossenschaft - e-ID Public Beta, 2026)

– Datensparsamkeit: Versicherung kann nur die nötigen Attribute prüfen (z. B. «Wohnsitz Gemeinde X») statt Dokumentkopien zu sammeln

4.2.3 Betreibungsregisterauszug digital verifizierbar

Für den Mietvertrag einer Wohnung verlangt die Verwaltung einen Betreibungsregisterauszug. Die betreffende Person bestellt ihn online. Der Auszug wird als Zertifikat (Verifiable Credential) an das swiyu Wallet zugestellt und diese teilt es direkt mit der Verwaltung.

Vorteile gegenüber heute:

– Kein Papierauszug, kein Scan, keine Medienbrüche
– Weniger Manipulation (verifizierbar), weniger manuelle Prüfschritte
– Ein Nachweis kann bei Bedarf mit mehreren Stellen geteilt werden, ohne jedes Mal erneut den Papierweg nutzen zu müssen

4.2.4 Strafregisterauszug

Eine Person bewirbt sich für eine Stelle mit Vertrauensanforderungen, zum Beispiel bei einer Bank. Sie beantragt online ihren Strafregisterauszug. Heute wird dieser typischerweise als digital signiertes PDF ausgestellt, das online überprüft werden kann.

Zielbild: Der Auszug oder ein statusbasierter Nachweis kann zusätzlich als verifizierbarer Nachweis ins swiyu Wallet ausgegeben und direkt mit dem Arbeitgeber geteilt werden.

Vorteile gegenüber heute:

– Weniger PDF-Handling und weniger manuelle Validierung
– Effektiver gegen Fälschungen (standardisierte kryptografische Verifikation)
– Datensparsame Option möglich (z. B. «Nachweis vorhanden» statt vollständiger Dokumentinhalt)

4.2.5 Führerausweis als digitaler Nachweis

Bei einer Fahrzeugmiete oder im Carsharing muss der Führerausweis schnell geprüft werden. Statt einer Kopie des Führerausweises teilt die Nutzerin aus dem swiyu Wallet einen Nachweis «gültiger Führerausweis (Kategorie B)», der automatisch vom Anbieter verifiziert wird. Hinweis: Der Lernfahrausweis ist bereits produktiv im swiyu Wallet verfügbar.

Vorteile gegenüber heute:

– Keine Ausweiskopie oder Foto und damit geringeres Datenschutzrisiko beim Anbieter
– Schnellere, automatisierbare Prüfung (weniger Betrug, weniger manuelle Checks)
– Aktualität: Status und Gültigkeit kann zuverlässiger geprüft werden als bei alten Kopien

5 Fazit und Ausblick

5.1 Zusammenfassung der wichtigsten Punkte

Diese erste Durchführung unserer Studie liefert ein insgesamt konsistentes Bild: Digitale Identitäten sind in Schweizer KMU und Behörden als Thema angekommen, aber der Schritt von «wir haben davon gehört» zu «wir haben es verstanden», respektive «konkret umgesetzt» hängt weniger vom Interesse am Thema als von den praktischen Bedingungen ab. Methodisch ist hierbei wichtig zu wiederholen, dass die Ergebnisse auf einer quantitativen Online-Umfrage mit 78 vollständigen KMU-Rückmeldungen und sechs vollständigen Behörden-Rückmeldungen basieren. Aussagen zu Behörden sind somit mit einer gewissen Vorsicht zu lesen, weil jede Segmentierung die Stichprobe weiter ausdünnt.

Die fünf wichtigsten Kernaussagen sind:

1. Die Diskussion ist stark von Vertrauen und Governance geprägt. In der Schweiz ist digitale Identität nicht nur ein Technologieprojekt, sondern auch ein gesellschaftliches Vertrauensprojekt, welches durch entsprechende Kommunikation der zuständigen Gremien nachhaltig gefördert werden kann. Das zeigt sich nicht nur innerhalb der Studie, sondern bereits in der Einordnung der politischen Sensibilität und der Bedeutung von Transparenz und Partizipation rund um das swiyu-Ökosystem.

   Das Vertrauen in Datenschutz und Sicherheit sowie in die Vertrauensinfrastruktur ist mehrheitlich vorhanden, aber klar mit Bedingungen verknüpft. Viele akzeptieren das Grundprinzip, erwarten jedoch eine saubere technische Umsetzung, nachvollziehbare Schutzmechanismen und klare Verantwortlichkeiten.

2. Akzeptanz und Nutzung hängen an der (sinnvollen) Integration, nicht am Konzept. Über die Auswertungen der Studienergebnisse hinweg taucht ein wiederkehrender Aspekt auf: Digitale Identitäten werden nicht als isoliertes Tool eingeführt, sondern müssen in gewachsene Systemlandschaften passen und den Unternehmensmehrwert sinnvoll unterstützen. Das erklärt, warum «Integration in bestehende Systeme» und «Wissen/Verständnis» als zentrale Hürden angesehen werden und warum selbst grundsätzlich positiv eingestellte Unternehmen oft zögern, bevor Standards, Architektur und Verantwortlichkeiten geklärt sind.

3. Unternehmen denken wirtschaftlich vor allem in Effizienz- und Kosten-Logiken und weniger in Umsatzlogiken. Wirtschaftliche Effekte werden in Form von Prozessoptimierung, weniger Medienbrüche und Effizienzsteigerung im Betrieb erwartet. Anfängliche Setup-Kosten werden in Kauf genommen, denn mittel- bis langfristig soll sich weniger operative Reibung und mehr Sicherheit ergeben.

4. Risikowahrnehmung steigt mit dem Reifegrad. Unternehmen, die bereits pilotieren, testen oder implementieren, sind sensibler für Risiken einer digitalen Identitätslösung. Dies zeigt sich durch die Einschätzungen bezüglich KI-generierten Identitätsbetrug. Das ist kein Widerspruch, sondern ein typisches Muster: Wer näher an realen Prozessen ist, denkt schneller in Bedrohungsmodellen und wie diese entschärft werden können.

5. Der Blick nach vorne ist pragmatisch. Bis und mit 2028 dominiert bei den Unternehmen ein Kurs aus «beobachten und dann handeln» und «Prüfung in eigene Systeme integrieren». Aktive Herausgeber-Rollen bleiben die Ausnahme. Behörden wirken im Vergleich fokussierter und stärker auf Integration ausgerichtet.

Strategische Einordnung: Der in der Studie sichtbar gewordene Kurs «beobachten, dann handeln» ist zwar kurzfristig nachvollziehbar, aber strategisch selten optimal. Digitale Identitäten und Nachweise entfalten ihren Wert nicht primär als Einzelprodukt («die e-ID»), sondern als **Infrastruktur mit Netzwerkeffekten**. Je

früher Organisationen verifizieren, integrieren und erste Nachweise in Prozesse überführen, desto schneller entstehen Routine, Standards, Partnerfähigkeit und Lernkurven in Architektur, Betrieb und Governance.

Wer zu lange abwartet, spart kurzfristig Aufwand, zahlt aber mittelfristig häufig höhere Integrationskosten, weil interne Fähigkeiten, Referenzprozesse und Ökosystem-Anschlüsse später und unter Zeitdruck aufgebaut werden müssen.

Aus diesen Erkenntnissen ergeben sich weiterführende Fragestellungen, die für eine potenzielle nächste Durchführung besonders wertvoll sein könnten:

- Was genau blockiert die Integration?
- Wie entsteht Vertrauen operationell? Nicht als abstrakte Zustimmung zur e-ID, sondern als messbare Akzeptanz in konkreten Prozessen wie dem Onboarding, Zugriffskontrollen oder Nachweisprüfungen.

5.2 Zukünftige Trends

Welche potenziellen Trends sehen wir in der Zukunft?

1. Die e-ID wandelt sich vom «Buzzword» zu einem festen Bestandteil der Unternehmensinfrastruktur. Das heisst für Unternehmen, dass digitale Identitäten und Nachweise ein Teil bestehender Prozesse werden und Geschäftsfälle unterstützen.

2. Der erste grosse Skalierungsschub kommt über Verifikation, nicht über Ausstellung. Entsprechend das Bild aus der Umfrage: Organisationen sehen sich kurzfristig primär als Verifier und Integratoren.

   Das ist auch global ein realistischer Pfad. Verifikation lässt sich oft inkrementell in bestehende Flows einbauen (Login, Onboarding, Berechtigungen, Nachweisprüfung). Herausgabe von Zertifikaten ist dagegen «governance-intensiv»: Datenqualität, Haftung, Prozesse, Registeranbindung, Lifecycle-Management. Für viele KMU ist das zwar mittelfristig möglich, aber nicht geeignet als Startpunkt.

3. Deepfakes und synthetische Identitäten werden zum Beschleuniger für die Verbreitung der e-ID. Steigende Betrugsqualität macht stärkere, kryptografisch verifizierbare Nachweise notwendig. Die Daten der Studie bekräftigen diesen Mechanismus. Mit wachsender Einführungsreife steigt die Sensibilität für Fake-Identitäten.

4. Vertrauen bleibt der kritische Engpass, nicht die Technik, denn Misstrauen ist menschlich. Auch wenn die Vertrauensinfrastruktur als «mehrheitlich vertrauenswürdig» eingeschätzt wird, zeigt der relevante Anteil an mittlerem oder geringem Vertrauen, dass für eine breite Akzeptanz Aufklärung und Transparenz wichtig sind.

5. Verifizierbare Daten werden «AI-ready» und digitale Signaturen werden anschlussfähig. Mit zunehmender Automatisierung (inkl. KI-gestützter Prozessketten) steigt der Bedarf an Daten, deren Ursprung, Aktualität und Berechtigung prüfbar ist. Verifizierbare Nachweise und digitale Signaturen können hier als Infrastruktur dienen: weniger manuelle Kontrollen, klarere Evidenzketten, bessere Auditierbarkeit und weniger Angriffsfläche durch synthetische Identitäten.

«Der Trend verschiebt sich von reiner Identifikation hin zu datensparsamen, verifizierbaren Nachweisen, die gezielt eingesetzt werden können. Organisationen wollen nicht «noch ein Account», sondern automatisierbare Vertrauensbausteine für Onboarding, Compliance und Betrugsprävention. Gleichzeitig wächst der Bedarf, Inhalte und Unternehmensidentitäten auf Authentizität zu prüfen.»

Daniel Säuberli, Präsident DIDAS

5.3 Ansatzpunkte zur Förderung der praktischen Einführung

Die Ergebnisse der Studie zeigen, dass der Schritt von einer grundsätzlichen Auseinandersetzung mit digitalen Identitäten hin zur Umsetzung weniger von einer generellen Zustimmung als von praktischen Rahmenbedingungen abhängt – insbesondere von Fragen der Integration, der Zuständigkeiten/Governance sowie von nachvollziehbaren Nutzen- und Risikoabwägungen. Vor diesem Hintergrund kann es sinnvoll sein, ergänzend zu klassischen Projekt- oder Austauschformaten unterstützende Strukturen zu betrachten, die Organisationen beim Übergang von Orientierung zu konkreten Schritten begleiten. Die nachfolgenden Punkte sind als mögliche Anforderungen an solche Formate zu verstehen.

Erstens wird ein Bedarf an **Orientierungshilfen** sichtbar, die Vergleichbarkeit schaffen, ohne Vorgaben zu machen. Viele Organisationen bewerten digitale Identitäten grundsätzlich positiv, knüpfen dies jedoch an Bedingungen wie transparente Verantwortlichkeiten und nachvollziehbare Schutzmechanismen. Unterstützende Formate könnten daher helfen, zentrale Begriffe, Rollen und Entscheidungsfragen einheitlich zu erläutern und die Einordnung parallel laufender Initiativen zu erleichtern. Dies kann eine Grundlage für informierte Entscheidungen schaffen.

Zweitens kann es hilfreich sein, **Bedarf und Nutzenannahmen** systematischer zu strukturieren. Die Daten legen nahe, dass Organisationen wirtschaftliche Effekte eher in Effizienz- und Kostenlogiken als in Umsatzpotenzialen sehen und dass unklare Nutzenargumente bzw. fehlendes Verständnis die Umsetzung bremsen können. Formate, die Use Cases präzisieren, Nutzen und Aufwand transparent machen und Unterschiede zwischen Branchen/Grössenklassen sichtbar machen, könnten die Priorisierung erleichtern.

Drittens sprechen die Befunde dafür, dass der Übergang vom Konzept zur Umsetzung häufig an **Integrations- und Umsetzungsfragen** hängt. Besonders genannt werden die Einbettung in bestehende Systemlandschaften sowie Fragen der Governance und Zuständigkeit. Unterstützungsangebote könnten hier ansetzen, indem sie praxisnahe Orientierung zu Integrationsmustern, Rollenmodellen und typischen Stolpersteinen geben (z. B. in Form von Referenzprozessen, Checklisten oder Erfahrungsberichten), ohne operative Projektverantwortung zu übernehmen.

Viertens ist es für eine stärkere Verbreitung vorteilhaft, **Anschlussfähigkeit und Skalierung** früh mitzudenken. Die Studie zeigt, dass viele Organisationen zunächst beobachten oder einzelne Funktionen integrieren möchten, während aktive Herausgeberrollen die Ausnahme bleiben. In dieser Situation können Hinweise auf Interoperabilität, Schnittstellenanforderungen und Mindeststandards helfen, dass frühe Pilotierungen später leichter übertragbar werden.

Fünftens und letztens ist für die Akzeptanz solcher Unterstützungsformate zentral, dass sie als **neutral und transparent** wahrgenommen werden. Da Vertrauen und Governance in der Schweizer Diskussion eine wichtige Rolle spielen, sollte jede vermittelnde Struktur klar machen, welche Interessen vertreten werden, wie Entscheidungen zustande kommen und wie Rückmeldungen aus der Praxis einbezogen werden.

Zusammenfassend legen die Ergebnisse nahe, dass weniger ein einzelnes Instrument als vielmehr **ein Bündel an pragmatischen Unterstützungsformaten** hilfreich sein kann, um die Transferlücke zwischen Wissen, Entscheidung und Umsetzung zu verkleinern. Entscheidend ist dabei, Orientierung und Umsetzungsnähe zu verbinden, ohne normative Vorgaben zu erzwingen oder Erwartungen an schnelle, flächendeckende Einführung zu wecken.

5.4 Schlussbemerkungen

Die neue e-ID mit Vertrauensinfrastruktur ist für Schweizer KMU kein blosses «Nice-to-have», sondern ein Baustein der digitalen Transformation mit konkreter Wirkung: weniger Medienbrüche, sauberere Zugriffs- und Nachweisprozesse, höhere Betrugsresistenz und langfristig effizientere Abläufe. Gleichzeitig zeigt die Studie klar, dass sich der Nutzen nicht automatisch einstellt; Nutzen entsteht dort, wo Organisationen Identität als Querschnittsthema ernst nehmen – von Architektur über Prozesse zu Datenhaltung, Governance und Change.

Gerade deshalb wäre eine regelmässige Durchführung dieser Studie sinnvoll. Sie kann als Frühwarnsystem agieren: Welche Hürden bleiben konstant, welche verschieben sich, wo entstehen echte Skalierungseffekte und welche Branchen kippen von «abwarten» zu «umsetzen»? Die diesjährige Basis liefert dafür einen Ausgangspunkt. Die nächsten Erhebungen können zeigen, ob swiyu und das Ökosystem nicht nur technisch reifen, sondern ob das Vertrauen, die Use Cases und die Integrationsfähigkeit in der Breite auch tatsächlich mitwachsen.

Verzeichnisse

Abbildungsverzeichnis

Literaturverzeichnis

Bhutan NDI. (Februar 2026). Von Bhutan NDI: https://www.bhutanndi.com/ abgerufen

Bundesamt für Statistik. (Dezember 2025). *Detaillierte Ergebnisse, Abstimmung vom 28. September 2025*. Von Eidgenössische Volksabstimmungen: https://abstimmungen.admin.ch/details/2025-09-28?proposalId=6790 abgerufen

Bundeskanzleramt. (Februar 2026). *ID Austria*. Von https://www.id-austria.gv.at/de/verwenden/eausweise abgerufen

DIDAS. (Januar 2026). Von Digital Identity and Data Sovereignty Association: https://www.didas.swiss/ abgerufen

Digitale Verwaltung Schweiz – eGovernment. (Februar 2026). *eGovernment Benchmark 2024*. Von https://www.digitale-verwaltung-schweiz.ch/publikationen/studien/egovernment-benchmark-2024 abgerufen

Digitale Verwaltung Schweiz – Studie. (Februar 2026). Von Studien (Monitoring): https://www.digitale-verwaltung-schweiz.ch/publikationen/studien abgerufen

Digitale Verwaltung Schweiz. (Februar 2026). *E-ID und Vertrauensinfrastruktur schweizweit einführen*. Von https://www.digitale-verwaltung-schweiz.ch/umsetzungsplan/projekte/behoerdenuebergreifende-digitale-identifikation-etablieren abgerufen

Europäische Kommission. (2025). *eIDAS - elektronische Identifizierung und Vertrauensdienste*. Von https://digital-strategy.ec.europa.eu/de/policies/discover-eidas abgerufen

Europäische Kommission. (Januar 2026). *Europäische digitale Identität*. Von https://commission.europa.eu/topics/digital-economy-and-society/european-digital-identity_de abgerufen

Französische Republik. (Februar 2026). *Französische Identität*. Von https://france-identite.gouv.fr/ abgerufen

Minister of Digital Affairs. (February 2026). *mDowód*. Von https://info.mobywatel.gov.pl/en/dokumenty/mdowod abgerufen

Parliament of Bhutan. (Januar 2026). Von National Digital Identity Act of Bhutan 2023: https://tech.gov.bt/wp-content/uploads/2024/09/National-Digital-Identity-Act-of-Bhutan-2023.pdf abgerufen

PWC. (Dezember 2025). *Digitalisierung – wo stehen Schweizer KMU?* Von https://www.pwc.ch/de/publications/2016/pwc_digitalisierung_wo_stehen_schweizer_kmu.pdf abgerufen

Schweizer Bundesrat. (Januar 2026). *Verordnung zum Bundesgesetz über den elektronischen Identitätsnachweis und andere elektronische Nachweise*. Von

https://cms.news.admin.ch/dam/de/der-schweizerische-bundesrat/CcnTR6jR9xtV/vorentw-veid-d.pdf abgerufen

Schweizer Eidgenossenschaft – e-ID Portal. (Februar 2026). *Die e-ID funktioniert wie eine digitale Identitätskarte*. Von Elektronische Identität und Vertrauensinfrastruktur: https://www.eid.admin.ch/de abgerufen

Schweizer Eidgenossenschaft – e-ID Public Beta. (Februar 2026). *Public Beta*. Von Elektronische Identität und Vertrauensinfrastruktur: https://www.eid.admin.ch/de/public-beta abgerufen

Schweizer Eidgenossenschaft – e-ID Technologie. (Februar 2026). *Technologie*. Von Elektronische Identität und Vertrauensinfrastruktur: https://www.eid.admin.ch/de/technologie abgerufen

Schweizer Eidgenossenschaft – Fedlex. (Februar 2026). *Bundesgesetz über den elektronischen Identitätsnachweis und andere elektronische Nachweise*. Von Fedlex Die Publikationsplattform des Bundesrechts: https://www.fedlex.admin.ch/eli/fga/2025/20/de abgerufen

Schweizer Eidgenossenschaft – Github. (Januar 2026). *Welcome to the swiyu Trust Infrastructure Community*. Von https://github.com/swiyu-admin-ch/community abgerufen

Schweizer Eidgenossenschaft – KMU Portal. (Januar 2026). *Die Digitalisierung der KMU in der Schweiz: ein Schlüsselfaktor*. Von KMU-Portal für kleine und mittlere Unternehmen: https://www.kmu.admin.ch/kmu/de/home/fakten-trends/digitalisierung.html abgerufen

Schweizer Eidgenossenschaft – swiyu. (Januar 2026). *swiyu*. Von Elektronische Identität und Vertrauensinfrastruktur: https://www.eid.admin.ch/de/swiyu-coming-soon-d abgerufen

Schweizerische Bundeskanzlei. (Januar 2026). *Elektronische Identität und Vertrauensinfrastruktur*. Von Strategie Digitale Schweiz: https://digital.swiss/de/aktionsplan/massnahme/bundesgesetz-uber-elektronische-identifizierungsdienste abgerufen

US-EU Trade and Technology Council. (Januar 2026). *DRAFT EU-US TTC Digital Identity Mapping Exercise Report*. Von https://www.nist.gov/document/eu-us-ttc-wg1 abgerufen

Autoren

Prof. Dr. Tim Weingärtner

Dozent

tim.weingaertner
@hslu.ch

Prof. Dr. Tim Weingärtner ist seit 2015 Dozent am Departement Informatik der Hochschule Luzern, Schweiz. Er beschäftigt sich in der Lehre und Forschung mit der Blockchain-Technologie, Smart Contracts und digitalen Identitäten.

Prof. Weingärtner ist Vizepräsident des Vereins DIDAS und Präsident des Vereins DEC Association. Daneben unterstützt er als Vertreter im Smart-up Programm die Förderung junger Start-ups aus der Hochschule Luzern.

Vor seiner Tätigkeit an der Hochschule arbeitete Prof. Weingärtner über 15 Jahre in der Schweizer Finanzindustrie. Er studierte Informatik und promovierte an der Universität Karlsruhe (KIT) in Deutschland im Bereich der medizinischen Robotik.

Link zum Personalprofil

Niklas Kustor

Master Student

niklas.kustor
@hslu.ch

Niklas Kustor, BSc (WU) ist seit September 2024 im Studiengang Master of Science in Wirtschafts-informatik an der FH Technikum Wien und absolviert parallel dazu den Master of Science in IT, Digitalization and Sustainability an der Hochschule Luzern. Beide Programme laufen bis Juni 2026. Die vorliegende Studie bildet zugleich eine inhaltliche und methodische Grundlage für seine Masterarbeit.

LinkedIn Profil

Hochschule Luzern – Informatik
Campus Zug-Rotkreuz
Suurstoffi 1
CH 6343 Rotkreuz