AIRLOCK®
SECURE ACCESS HUB

WHITEPAPER

Die (R)Evolution der digitalen Identität

Den Siegeszug von SSI und eID souverän begleiten und mit hybriden Full-Service-Modellen rechtzeitig die Weichen stellen

airlock.com

Partner: kuppingercole ANALYSTS, PXL VISION

Inhaltsverzeichnis

Management Summary

Das Whitepaper beleuchtet, wie das Konzept der Self-Sovereign Identity (SSI) einen Paradigmenwechsel im Identitätsmanagement auslöst. Die traditionelle Identitätsprüfung wird damit revolutioniert und Unternehmen bieten sich im Zuge der nationalstaatlich forcierten Ausbreitung elektronischer Identitäten (eID) auf Basis von SSI entscheidende Potenziale für das Tagesgeschäft. Gerade im Hinblick auf Compliance, Sicherheit und Anwenderfreundlichkeit legt SSI die Messlatte ein signifikantes Stück höher.

SSI ermöglicht es Nutzer:innen, ihre digitalen Identitäten selbst zu verwalten und zu kontrollieren, wer Zugang zu welchen Informationen erhält. Dieser dezentrale Ansatz reduziert die Abhängigkeit von zentralen Identitätsanbietern und erhöht gleichzeitig die Datensicherheit, da persönliche Informationen nur mit ausdrücklicher Zustimmung der Nutzer:innen weitergegeben werden.

Staatliche Initiativen treiben die Einführung von SSI-Technologien derzeit massiv voran. An den Beispielen der Schweiz und der Europäischen Union wird gezeigt, wie weit die Umsetzung bereits vorangeschritten ist. Auch aus Analystensicht ist SSI ein Thema, das weit oben auf der Agenda stehen sollte.

Unternehmen, die frühzeitig auf SSI setzen, können sich wichtige Wettbewerbsvorteile sichern. Zahlreiche Prozesse wie die Kontoeröffnung oder Vertragsabschlüsse lassen sich effektiv aufgleisen und Konversionsraten steigern. Airlock und PXL Vision bieten dabei professionelle Unterstützung, um den Übergang zur neuen Welt der Identitätsprüfung erfolgreich zu gestalten.

Insgesamt unterstreicht das Whitepaper die Bedeutung von SSI als zukunftsweisende Technologie, die sowohl Chancen als auch Herausforderungen mit sich bringt. Unternehmen, die diese Herausforderungen meistern, können langfristig vom Mehrwert eines sicheren, effizienten und nutzerfreundlichen Identitätsmanagements profitieren.

Dezentralisierte Identität: Potenzial für bahnbrechende Innovationen

Die Dezentrale Identität (DCI) hat sich über mehr als ein Jahrzehnt hinweg entwickelt und steht kurz vor dem Wendepunkt für eine breite Akzeptanz und die Auslösung massiver Innovationen in der Art und Weise, wie Unternehmen und Regierungen mit Kunden, Verbrauchern, Mitarbeitern oder Bürgern interagieren.

Von zentralisierten Identitätssilos zu dezentralen Identitäts-Wallets

DCI, auch als SSI (Self-Sovereign Identity) bezeichnet, ist ein Konzept, das sich grundlegend von etablierten Modellen unterscheidet. Üblicherweise verwalten Organisationen die Identitäten von Einzelpersonen in ihren eigenen Systemen, wodurch Identitätssilos entstehen, und Einzelpersonen gezwungen sind, sich bei vielen verschiedenen Dienstanbietern zu registrieren. Jeder erlebt dies fast täglich bei der Nutzung des Internets. Zwar können einige Identitäten wie die von LinkedIn, Facebook, Google oder Apple wiederverwendet werden, doch sind sie immer noch zentralisiert und nicht allgegenwärtig.

Im Gegensatz dazu belässt DCI die Identität und ihre Attribute bei der Person. Auf der Grundlage von Standards können diese Informationen flexibel mit anderen Parteien ausgetauscht werden. Sogenannte verifiable credentials (VCs, überprüfbare Nachweise) geben beispielsweise Auskunft über den Namen, die E-Mail-Adresse, die Postanschrift, den Arbeitgeber, den Beschäftigungsstatus oder andere Informationen. Das Konzept des DCI ist offen und schränkt nicht ein, was mit VCs bereitgestellt werden könnte. Dies ist von entscheidender Bedeutung, da dies die Verwendung von DCI für jede Art von Anwendungsfall ermöglicht, insbesondere weil auch Dinge, Geräte oder Organisationen ihre dezentralen Identitäten haben könnten (und im Laufe der Zeit haben werden).

DCI baut auf einem Konzept von Issuers (Emittenten) auf, die VCs ausgeben, Holder (Inhabern) – in der Regel Einzelpersonen –, die VCs besitzen, und Verifiern (Überprüfern), die VCs benutzen. Die VCs werden von den Inhabern in so genannten Wallets gespeichert. Im Laufe der Zeit könnte sich der Begriff «Brieftasche» als irreführend erweisen, da wir potenziell viel mehr Informationen in Form von VC in der Brieftasche haben werden als wir heute Karten in unseren Brieftaschen haben. Außerdem werden die Anwendungsfälle viel breiter werden.

Dezentrale Identität: Mehr als nur Verifizierung, Onboarding und Authentifizierung

DCI wird heute häufig als Mittel gesehen, um eine verifizierte Identität auf der Grundlage von menschengestützten oder vollautomatischen IDV-Prozessen (Identity Verification) zur Verfügung zu haben, die wiederverwendbar ist. Das ermöglicht vertrauenswürdige Interaktionen mit anderen Parteien wie Organisationen oder Behörden.

Die VCs liefern dann zusätzliche Daten und können zum Beispiel den Onboarding-Prozess wie die Registrierung auf einer eCommerce-Website vereinfachen. Auf der Grundlage der verifizierten Identität, der sicheren Brieftasche und der Möglichkeit, diese Brieftasche zu öffnen, können Authentifizierungsprozesse vereinfacht werden.

Die Betrachtung nur dieser Aspekte kratzt jedoch nur an der Oberfläche des Potenzials, das DCI bieten. Die Möglichkeiten sind viel grösser. Überprüfbare Nachweise (VCs) können zur Prozessautomatisierung und -optimierung eingesetzt werden. Stellen Sie sich das Onboarding von Externen für ein Projekt vor. Dieser Prozess kann auf der Grundlage des Namens, des Arbeitgebers, des Beschäftigungsstatus und einiger anderer Informationen vollständig automatisiert werden. Oder stellen Sie sich die Beantragung eines Kredits bei einer Bank vor, die auf anderen VCs basiert, von der überprüften Identität bis hin zu den monatlichen Gehaltsabrechnungen, dem Familienstand, dem Nachweis bestehender Immobilien und so weiter. Die kostspieligen AML- (Anti Money Laundering) und KYC-Prozesse (Know Your Customer) in Banken würden massiv sinken, ebenso wie die Kosten für die Genehmigung (oder Ablehnung) von Krediten. Die Optimierung der Prozesskosten ist ein großes Potenzial von DCI.

Aber es gibt noch mehr. Die Zustimmung (digitaler Consent) beim Zugriff auf Websites könnte durch VCs verwaltet werden, die die Verwendung bestimmter Informationen durch bestimmte Parteien für einen bestimmten Zweck und eine begrenzte Zeit erlauben. Menschen könnten Gesundheitsdaten auf kontrollierte Weise als VCs weitergeben. Das Potenzial ist praktisch unbegrenzt und ermöglicht bahnbrechende Innovationen in der digitalen Wirtschaft.

Potenzial für den Durchbruch: Disruptive Innovation für Geschäftsmodelle, ohne die IT zu zerstören

Unternehmen, die das Potenzial von DCI nutzen, gewinnen durch die Bereitstellung neuer, innovativer Dienste, aber auch durch die Optimierung ihrer Prozesse und damit ihrer Kosten. Die kürzlich verabschiedete EU-Regulierung eIDAS 2.0, die unter anderem vorschreibt, dass die Mitgliedsstaaten ihren Bürger bis 2026 ein Wallet für DCI, das EU DI Wallet (EU Decentralized Identity Wallet) bereitstellen müssen und DCI auch als zentrales Element im eGovernment definiert, wird sich nach unserer Einschätzung als Treiber für eine deutlich schnellere Akzeptanz und Umsetzung von DCI-Konzepten erweisen. Diese Wallets sind eine Basis auch für weitergehende Anwendungen von DCI.

Glücklicherweise sind disruptive Innovationen für Geschäftsmodelle und Geschäftsprozesse nicht gleichbedeutend damit, dass bestehende IT-Systeme nicht mehr genutzt werden können. DCI ergänzt das Bestehende. Wenn ein Kunde über DCI registriert wird und Waren kauft, wird dies immer noch durch Datensätze im ERP-System des Unternehmens reflektiert. Wenn ein neuer Mitarbeiter kommt, gibt es vielleicht immer noch einen Eintrag in einem internen Verzeichnis.

Wenn DCI nur an der Schnittstelle zwischen Individuen und Organisationen gerückt wird, um Nutzer zu identifizieren, zu registrieren und zu authentifizieren, kann das Potenzial jedoch nicht voll ausgeschöpft werden. Die Nutzung von VCs zur Entscheidungsfindung, von Zugangsberechtigungen bis zur Prozessautomatisierung, erfordert Änderungen in den Backends. In vielen Fällen wird dies ein evolutionärer Prozess sein.

Angesichts des immensen Potenzials von DCI ist es spätestens jetzt an der Zeit, dass Organisationen dieses Potenzial bewerten und über die Innovationen nachdenken, die es für ihr Geschäft oder die Art und Weise, wie Regierungen ihren Bürgern dienen, bringen kann. Dabei müssen alle Mitarbeiter der Organisation einbezogen werden, nicht nur das Team, das sich mit IAM (Identity und Access Management) und digitalen Identitäten beschäftigt.

SSI und eID: Eine neue Ära des Identitätsmanagements

In der heutigen Welt, in der die Digitalisierung immer schneller voranschreitet und personenbezogene Daten zum Handelsobjekt geworden sind, nimmt das Konzept der Self-Sovereign Identity (SSI) als Leuchtturm für Selbstbestimmung und Privatsphäre eine zunehmend wichtigere Rolle ein. Herkömmliche Identitätssysteme, die auf zentraler Verwaltung und aufwendiger Kontrolle von Dritten beruhen, werden angesichts der aktuellen Entwicklungen künftig weiter in den Hintergrund rücken. Die transformative Idee, die hinter SSI und einem modernen Umgang mit elektronischen Identitäten (eID) steckt, bahnt sich immer stärker ihren Weg in die Praxis.

Aber was genau ist SSI und was ist das Revolutionäre daran?

Self-Sovereign Identity aus Anwendersicht

Stellen Sie sich vor, Sie hätten eine digitale Brieftasche (Wallet), in der alle Angaben zu Ihrer Identität sicher aufbewahrt werden: Daten zu Ihrem Alter, Informationen zu Ihrer Ausbildung, Ihr Führerschein, Ihre Zeugnisse, Ihre Bankverbindungen, Ihr Versicherungsschutz, Ihre Konzerttickets und Ihre Mitgliedsausweise – so ähnlich wie ein Stapel virtueller Karten. Mit SSI können Sie diese Karten selbst verwalten und entscheiden, wer auf die gespeicherten Daten zugreifen darf.

Um das dahinterstehende Konstrukt zu verstehen, gilt es zunächst die verschiedenen Rollen zu kennen.

Aussteller digitaler Nachweise (Issuer): hierbei handelt es sich um Unternehmen oder Organisationen, die berechtigt sind, digitale Nachweise auszustellen (zum Beispiel Bildungseinrichtungen, Arbeitgeber, Banken, Sportvereine, Einkaufsseiten oder Behörden)

Nutzer digitaler Nachweise (Holder): damit ist der Besitzer der digitalen Brieftasche gemeint, der die entsprechenden Nachweise der eigenen Identität selbst verwaltet

Verifizierer digitaler Nachweise (Verifier): Verifier sind Akzeptanzstellen, die je nach Anwendungsfall die für die Interaktion benötigten Nachweise vom Holder anfordern (zum Beispiel Online-Shops)

Selbstbestimmung statt Fremdbestimmung

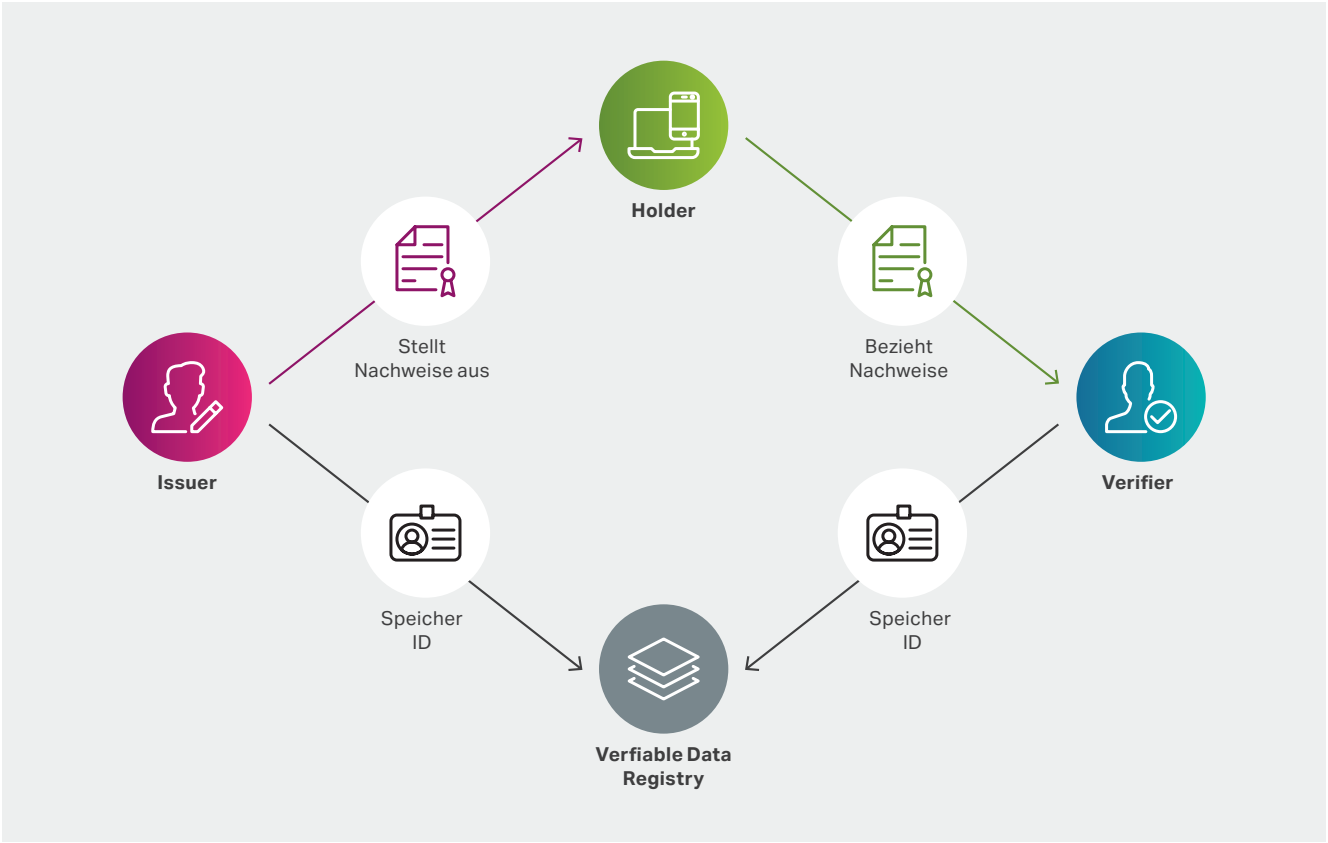
Bisher werden unsere Identitäten in der Regel durch Dritte kontrolliert und nachverfolgt. Diese Identitätsanbieter (Identity Provider oder IdP) – beispielsweise eine Behörde oder ein privater Service Provider wie Google – speichern die jeweiligen Daten mit den entsprechenden Attributen und ordnen diesen Mittel zur Authentisierung zu. Um beim genannten Beispiel zu bleiben: Sobald Sie Funktionen wie «Mit Ihrem Google-Konto anmelden» verwenden, weiss Google, wer Sie sind, und bestätigt Ihre Identität gegenüber dem Dienst, auf den Sie zugreifen möchten. Das ist ziemlich praktisch, da Sie sich nur einmal anmelden müssen, anstatt Ihre Anmeldedaten mehrfach zu verwenden. Aber wie so oft hat die Medaille auch eine Kehrseite. Denn auf diese Weise kann Google nicht zuletzt jeden einzelnen Ihrer Log-

ins im Internet nachverfolgen. Zudem ist für Anwender:innen oftmals nicht transparent, was eigentlich genau gespeichert wird.

Mit SSI ändert sich das. Sie besitzen als Holder Ihre digitale Identität und Sie allein entscheiden, mit wem Sie welche Attribute Ihrer Identität teilen wollen. Dritte haben keine Möglichkeit, Ihre Aktivitäten nachzuverfolgen und zu sehen, wann und wo Sie mit Ihrer Identität digital in Erscheinung treten. Jeder Kontakt, den Sie herstellen, findet nur zwischen Ihnen und dem Dienstanbieter (der als Verifier auftritt) statt, mit dem Sie eine Verbindung herstellen möchten. Verifizierbare Nachweise (Verifiable Credentials, VC) sind Ihre digitalen Karten.

Die Aussteller (Issuer) bestätigen Ihre Daten. Verifiable Credentials werden in Ihrer digitalen Brieftasche (Wallet) gesammelt und nur dort aufbewahrt. Wenn Sie einen Nachweis (beispielsweise hinsichtlich Ihrer Volljährigkeit) erbringen müssen, geben Sie nur die erforderlichen Informationen aus den entsprechenden verifizierbaren Nachweisen preis – ohne weitere persönliche Details zu verraten, die Ihr Gegenüber grundsätzlich nichts angehen («Selektive Offenlegung» oder «Selective Disclosure»). Der Verifier erhält nur die für ihn bestimmten Informationen.

Als Holder verlieren Sie niemals die Kontrolle über die Informationen in Ihrer digitalen Brieftasche. Die Weitergabe von verifizierbaren Nachweisen erfordert Ihre ausdrückliche Zustimmung. Die Vorgaben aus DSGVO und Datenschutzgesetz werden konsequent erfüllt.



Identitätsmangement per SSI

Zuverlässigkeit der ausgetauschten Daten

Sobald Sie als Holder Daten freigeben, die in Ihren verifizierbaren Nachweisen (Verifiable Credentials) enthalten sind und in der digitalen Brieftasche (Wallet) sicher aufbewahrt werden, können Verifier sich darauf verlassen, dass die jeweiligen Issuer (Aussteller) deren Richtigkeit bestätigt haben. Die Empfänger von Informationen aus verifizierbaren Nachweisen prüfen die Integrität der Nachweise und die Vertrauenswürdigkeit der Aussteller. Zu diesem Zweck werden verifizierbare Nachweise mit kryptografischen Signaturen gesichert. Die zeitaufwendige und oftmals manuelle Überprüfung der Richtigkeit von Daten entfällt, da diese durch die Unterschrift des Ausstellers garantiert wird.

Als Anwender:in profitieren Sie von diesem Ansatz in zweifacher Hinsicht. Durch die Freigabe verifizierbarer Nachweise entfällt die manuelle Dateneingabe. Tippfehler und mühsames Ausfüllen von Formularen gehören somit der Vergangenheit an. Zudem steht die Datenintegrität ausser Frage, sobald die verifizierbaren Nachweise von einem vertrauenswürdigen Aussteller zur Verfügung gestellt wurden. Das macht Prozesse sicherer und bequemer.

Wichtige Eigenschaften von SSI

Vorteile von SSI im Überblick

Grenzenlose Spielfläche

Die Annahme und Freigabe Ihrer verifizierbaren Nachweise ist nicht nur auf bestimmte Branchen oder Länder beschränkt. Die SSI-Technologie schafft das Fundament, damit Sie Ihre verifizierbaren Nachweise ohne Einschränkungen verwenden können – wann, wo und gegenüber wem Sie wollen. Dies gilt nicht nur für die digitale, sondern auch für die physische Sphäre: Wenn Sie in einem Geschäft Alkohol kaufen, können Sie Ihr Alter nachweisen. Wenn Sie in ein Hotel einchecken, können Sie sich ausweisen, oder Sie können einer Polizistin oder einem Polizisten Ihren Führerschein vorzeigen.

Dabei ist SSI nicht nur für Einzelpersonen geeignet, sondern auch für Organisationen und Gegenstände.

Staatlicher Rückenwind für SSI

Es verwundert kaum, dass das Thema auf nationalstaatlicher Ebene inzwischen massiv vorangetrieben wird. Die Vorteile sprechen schliesslich für sich.

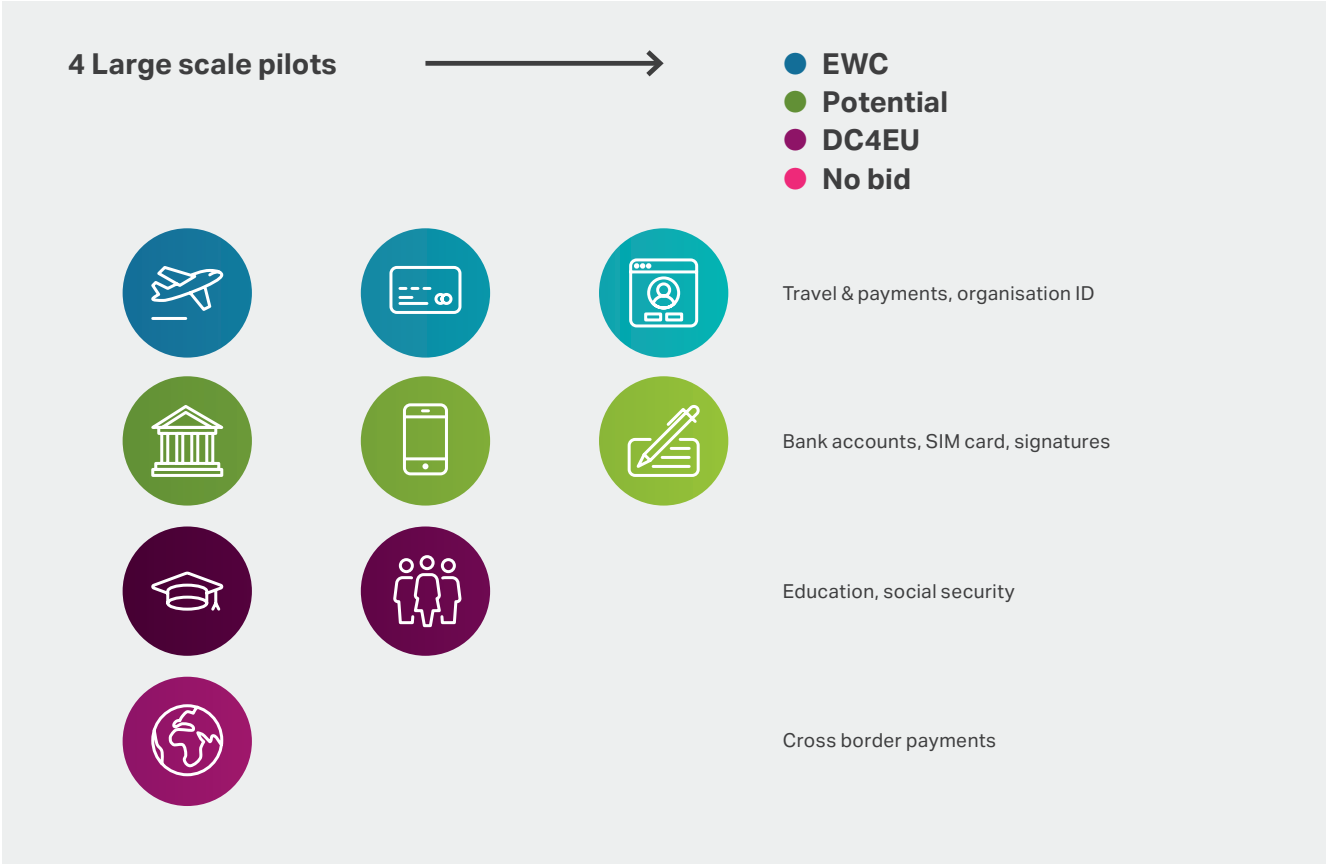
Vor unserer eigenen Haustür laufen Initiativen und Gesetzgebungsverfahren, die die Einführung von SSI-Technologien befeuern, auf Hochtouren. Laut aktuellem Planungshorizont sollen die Vorgaben für einschlägige eID-Konzepte auf Basis von SSI sowohl in den Ländern der Europäischen Union wie auch in der Schweiz bis spätestens 2026 verbindlich Wirkung entfalten. Um dabei Verwirrung von Anfang an vorzubeugen: In einzelnen Ländern weichen die Begrifflichkeiten im Zuge elektronischer Identitätsnachweise voneinander ab. Während in der Schweiz in der Regel von eID gesprochen wird, taucht im internationalen Kontext auch immer wieder das Kürzel PID (Personal Identification Data) auf. Im Whitepaper findet eID synonym Verwendung.

Schweiz: Im zweiten Anlauf auf Erfolgskurs

In der Eidgenossenschaft hat der Nationalrat der Neuvorlage zur Einführung eines elektronischen Identitätsnachweises (eID) am 14. März 2024 mit deutlicher Mehrheit zugestimmt. 2021 war die erste Version am Referendum gescheitert. Die damaligen Kritiker sind mittlerweile vielfach verstummt – insofern ist die Wahrscheinlichkeit, dass es zu einem erneuten Volksentscheid kommt, äusserst gering. Derzeit liegt die Vorlage beim Ständerat und es besteht theoretisch durchaus die Chance, dass das Gesetz noch im Jahr 2024 verabschiedet wird. Im Rahmen der praktischen Vorbereitung hat das Schweizer Bundesamt für Informatik eine technische Infrastruktur bereitgestellt, an der sich nicht zuletzt interessierte Unternehmen ausprobieren dürfen. Die nächste Generation, welche dann auch den künftigen technischen Standards entsprechen soll, ist für Anfang 2025 angekündigt. Das ausgerufene Ziel: Bis spätestens 2026 handlungsfähig sein – auf gesetzlich und technologisch einwandfreier Grundlage.

eIDAS2 und EUDI-Wallet: Auf die Plätze, fertig, los!

Einen entscheidenden Meilenstein verzeichnen derzeit auch die EUID- und SSI-bezogenen Aktivitäten der Europäischen Union. Am 29. Februar 2024 hat das Europäische Parlament in einer finalen Abstimmung die novellierte eIDAS-Verodnung (Version 2.0) angenommen. Mit dem nur noch rein formellen Akt des Durchwinkens beim EU-Ministerrat ist das EUDI-Wallet beschlossene Sache und den EU-Mitgliedsstaaten bleiben 24 Monate Zeit, dem Konzept der digitalen Identität auf nationaler Ebene rechtskonform Leben einzuhauchen. Um die zugrundeliegenden technischen Spezifikationen schon im Vorfeld auf Herz und Nieren prüfen zu können, hat die EU bereits 2023 vier grosse Pilotprojekte (Large Scale Pilots – LSP) auf den Weg gebracht, bei denen private Unternehmen und Behörden aus den EU-Mitgliedsstaaten sowie weiteren Länder Europas in Zusammenarbeit derzeit spezifische Anwendungsfälle entwickeln und pilotieren. Beteiligt sind rund 360 Einrichtungen. Technologische Grundlage ist der von der eIDAS Expert Group vorgelegte Werkzeugkasten, der unter anderem die am 7. März 2024 von der Europäischen Kommission vorgestellte, jüngste Version des «Architecture and Reference Framework (ARF)» umfasst.



In vier Large Scale Pilots der EU wird das Konzept auf Herz und Nieren geprüft.

Vielfältige Einsatzszenarien auf dem Prüfstand

Während beim EWC-Projekt insbesondere Use Cases rund um die EU-übergreifende Nutzung digitaler Reisezertifikate im Fokus stehen, arbeiten die Beteiligten beim Potential-LPC an länderübergreifend funktionierenden Prozessen im Hinblick auf Online-Verwaltung, Bankkontoeröffnung, SIM-Karten-Registrierung, einen digitalen Führerschein, E-Signaturen und medizinische Angelegenheiten wie Verschreibungen. NOBID richtet das Augenmerk auf EUDI-Wallet-basierte Bezahlvorgänge und last but not least hinterfragt DC4EU die Möglichkeiten digitaler Nachweise in den Bereichen Bildung und soziale Sicherheit. Es ist davon auszugehen, dass bis 2026 40 bis 50 verschiedene Anwendungsfälle als schlüsselfertige Lösungen bereitstehen. Von den Vorteilen können in naher Zukunft über 400 Millionen EU-Bürger:innen profitieren. Die EU-übergreifende EUDI-Wallet-Nutzung ist dabei freiwillig. Gleichzeitig nimmt die Europäische Kommission bereits jetzt grosse Online-Plattformen und Suchmaschinen sowie Banken in die Pflicht, EUDI-Wallets zur Nutzerauthentifizierung und -registrierung künftig ebenfalls zu akzeptieren. Somit erhöht sich nicht zuletzt der Druck auf Seiten privater Unternehmen.

Schulterschluss zwischen staatlichen Organisationen und Privatwirtschaft

Als offenes System und von seiner Konzeption her ist SSI perfekt geeignet, um unterschiedlichste Ökosysteme zu unterstützen (zum Beispiel Behörden, Gesundheitswesen, Finanzen, Sport und Unterhaltung) – ganz unabhängig von individuellen Ansprüchen hinsichtlich Sicherheit, Vertrauenswürdigkeit und Qualität. Die Vielfalt der Issuer (Aussteller) und Verifier (Akzeptanzstellen) nimmt massgeblich Einfluss auf den Mehrwert in der Anwendung. So kann die Privatwirtschaft von verifizierbaren Nachweisen profitieren, die von

staatlichen Stellen ausgestellt werden (zum Beispiel Führerschein), aber auch staatliche Stellen könnten von verifizierbaren Nachweisen profitieren, die von Unternehmen aus der Privatwirtschaft ausgestellt werden (Steuerbehörden erhalten Gehaltsbescheinigungen oder Kontoauszüge als verifizierbare Nachweise).

Ziel muss es sein, einen nahtlosen Datenaustausch zu schaffen, der vor einzelnen Branchen und Ländergrenzen nicht Halt macht. SSI ermöglicht sichere, grenzüberschreitende Transaktionen, ohne sich dabei auf zentrale Behörden verlassen zu müssen. Rechtliche Hürden werden gerade abgebaut und die europaweite Gesetzgebung bildet eine solide Grundlage für die internationale Zusammenarbeit.

Schlagende Argumente für Unternehmen

Nachdem die Anwendersicht ausführlich beleuchtet wurde und das öffentliche Interesse klar umrissen ist, sollen im Folgenden die grundsätzlichen Treiber und spezifischen Vorteile von SSI für Unternehmen aufgezeigt werden. Schlagworte sind dabei Compliance, Sicherheit und Benutzerfreundlichkeit. An dieser Dreifaltigkeit der Identität kommt über kurz oder lang keine Organisation mehr vorbei.

Dreifaltigkeit der Identität

Compliance

Im Hinblick auf Compliance stehen Unternehmen unter ständiger Beobachtung – und zwar nicht nur von staatlicher Seite. Privatpersonen werden zunehmend sensibler, wenn es um die Verwendung ihrer Daten geht. Sobald zentralisierte Identity Provider Benutzerdaten ohne ausdrückliche Zustimmung der Benutzer:innen erheben und verarbeiten, wird die Privatsphäre des Einzelnen untergraben. Aktuell ist dies ein hervorragendes Geschäftsmodell für einige Unternehmen. Der Erfolg und Mehrwert von Websites wie LinkedIn und Facebook basiert schliesslich nicht zuletzt auf einer solchen Nutzbarmachung privater Daten in Form gezielter Marketingkampagnen. Hier kann SSI ganz neue Klarheit schaffen. Die Verantwortung über die persönlichen Daten liegt in den Händen der Anwender:innen. Gleichzeitig werden versteckte AGB eliminiert und Datenschutzgesetze per Voreinstellung «automatisch» durchgesetzt. Somit ergeben sich nicht zuletzt gleiche Voraussetzungen und Rechtssicherheit für alle.

Sicherheit

Traditionelle Systeme stützen sich auf zentrale Identity Provider (Regierungen oder private Dienstanbieter). Von dieser Zentralisierung geht einerseits der Eindruck einer gewissen Kontrolle und Überwachung der Benutzer:innen aus, andererseits wird ein einziger Punkt geschaffen, an dem es zu Angriffen oder Fehlern kommen kann. Auch hier beschreitet SSI neue Wege. Durch den dezentralisierten Ansatz ist Ausfallsicherheit gewährleistet. Das System bleibt auch dann funktionsfähig, wenn bei einem Issuer oder Verifier eine Störung vorliegt. Alle Daten im System werden verteilt und sind in der digitalen Brieftasche der Eigentümer:innen gespeichert. Dass ein Cyberangriff alle Daten im gesamten System gefährdet, ist nahezu ausgeschlossen, denn hierzu müssten alle digitalen Brieftaschen genau zur gleichen Zeit erfolgreich gehackt werden. Durch die kryptische Signatur der verifizierbaren Nachweise lässt sich jeder Versuch der Datenmanipulation sofort erkennen. Nicht nur die Integrität der Daten ist auf diese Weise sichergestellt. Auch die Authentizität des Unterschreibenden ist jederzeit nachvollziehbar.

Benutzerfreundlichkeit

Convenience ist das Gebot der Stunde und Benutzerfreundlichkeit wird immer mehr zum Zünglein an der Waage – gerade im B2C-Umfeld. Im Zuge der Digitalisierung gibt es viel Konkurrenz und die Qualität des Online-Erlebnisses auf Kundenseite entscheidet am Ende über den Gesamterfolg. Steht diese nicht im Zentrum, läuft man als Unternehmen schnell Gefahr, dass Kund:innen abspringen oder gar nicht erst «aufspringen». Für viele Banken

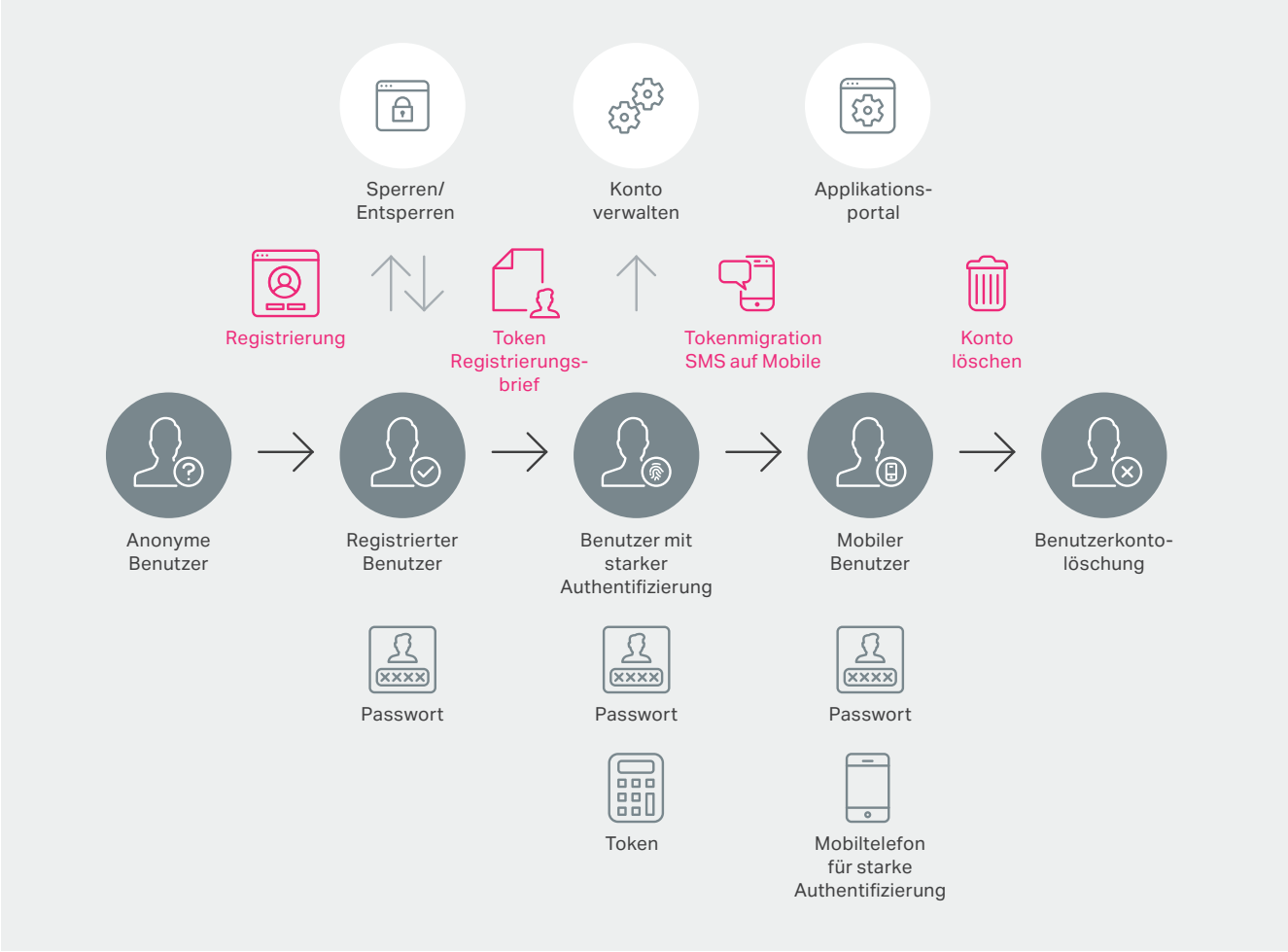
und Versicherungen sowie Online-Händler ist dies bereits der Alltag. Aber auch Behörden und Akteure des Gesundheitswesens erkennen, dass sie sich auf traditionellen Abläufen nicht länger ausruhen können. Der heutige Nutzer erwartet optimale Bedienbarkeit und Prozesse, die einfach und intuitiv verständlich sind. Genau aus diesem Grund gilt es aus Unternehmenssicht speziell diesen Aspekt im Zuge von SSI zu berücksichtigen. Ein auf SSI basierendes Identitätsmanagement ermöglicht eine Customer Journey ohne Medienbrüche. Die Zeiten, in denen ein Kunde erst seinen Ausweis scannen oder eine Unterschrift leisten muss, sind damit passé. Stattdessen kann sich der Anwender mit einem Klick registrieren und muss dabei nur die Daten freigeben, die zwangsläufig erforderlich sind. Selbst komplexe Prozesse wie die Eröffnung eines Bankkontos, bei der es auf Nachweise zu Wohnsitz, Einkommen und vielem weiteren entlang der rechtlichen Vorgaben ankommt, werden mit SSI zum Kinderspiel. Das Gleiche gilt für Vertragsabschlüsse oder eine Altersprüfung, die komplett anonymisiert erfolgen kann. Die Datenhoheit liegt bei den Inhaber:innen der Identität. Sie entscheiden, wer, wann auf welche Daten zugreifen darf.

Mit Veränderungen mitwachsen

Moderne Lösungen zum Identitätsmanagement berücksichtigen bereits heute eine Vielzahl von Möglichkeiten, um das Zusammenspiel von Compliance, Sicherheit und Benutzerfreundlichkeit so gut wie möglich abzubilden. So unterstützen beim Onboarding beispielsweise einfache Wizards und Self Services, die Anwender:innen nach ihren Wünschen durch den Registrierungsprozess führen. Entscheidend ist, Eintrittsbarrieren konsequent abzubauen – von Anfang bis Ende. Durch Single-Sign-On über alle Applikationen können Kund:innen verschiedene Dienste nutzen, ohne ständig nach ihren Zugangsdaten gefragt zu werden. Selbstverständlich erfolgt die Nutzung mit dem Gerät ihrer Wahl (Mobiltelefon, Tablet, Desktop-Computer). Die Integration der angeschlossenen Applikationen funktioniert aus Sicht der Benutzer:innen völlig transparent. Die Auswahl der Authentisierungsmittel gestaltet sich im Idealfall absolut flexibel und entlang der risikobasierten Authentisierung wird immer nur so viel Authentisierung durchgeführt, wie notwendig ist.

Relevante Funktionen eines IAM-Systems decken, wie in der Grafik gezeigt, den gesamten Lebenszyklus von Identitäten ab – und nicht nur die Kernfunktion der Authentifizierung von Anwender:innen.

- Benutzerauthentifizierung mit mehreren Faktoren
- Adaptive/Riskobasierte Authentisierung
- Single Sign-On
- Autorisierung und Zugriffskontrolle
- Identity Federation
- User-Provisionierung und Selbst-Registrierung
- Selbstbedienungsfunktionen (Passwort zurücksetzen, Konto entsperren, Profil verwalten)
- Audit- und Compliance-Informationen



Customer Lifecycle – vom Social Login über das Onboarding bis hin zur Löschung eines Benutzerkontos

Integration von eID in Verifikationssysteme steigert Konversionsraten

Wer bereits heute die Weichen stellt, um neben den bereits bestehenden Verifikationsmethoden künftig auch die elektronischen Identitäten (eID) verschiedener Länder auf Basis von SSI berücksichtigen zu können, sichert das Fundament des Geschäftserfolgs durch reibungslose Prozesse. Flexibilität ist das entscheidende Kriterium. Die Konversionsrate – also der Prozentsatz der erfolgreich verifizierten Identitäten – steht und fällt mit der Benutzerfreundlichkeit. Hierbei ist gleichzeitig darauf zu achten, dass die Verifizierung fehlerfrei erfolgt. Denn eine extrem hohe Konversionsrate ist manchmal auch ein Hinweis darauf, dass Verifikationskriterien zu locker sind und somit das Risiko besteht, dass Personen fälschlicherweise verifiziert werden.

Eine moderne Identity-Verification-Lösung wie PXL Ident bietet folgende Funktionen:

- ▶ Dokumenten-Verifizierung (von Ausweisdokumenten wie Personalausweisen, Führerscheinen etc.)
- ▶ Lebendigkeitserkennung (Liveness Detection), um sicherzustellen, dass es sich um eine echte Person und kein Foto oder Video handelt
- ▶ Face Verification, um zu prüfen, ob die Person vor der Kamera auch die Person am Ausweis ist
- ▶ OCR-Extraktion der Daten am Ausweis

Optional können dann auch noch folgende Funktionen angewendet werden:

- ▶ Auslesen der biometrischen Daten aus dem NFC-Chip
- ▶ Datenabgleich mit Online-Datenbanken für Adresscheck oder Sanktionslisten

Mit einer SSI-basierten eID lassen sich Sicherheit und Benutzerfreundlichkeit konsequent in Einklang bringen.

Die Customer Journey könnte dann beispielsweise wie folgt aussehen:

1. Endkunde startet den Onboarding-Prozess über das Airlock-System des Unternehmens

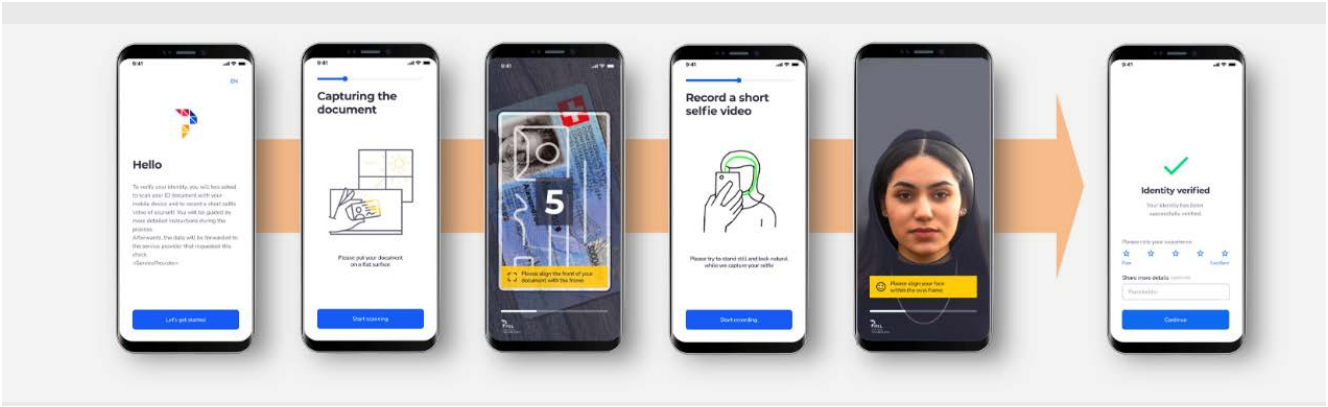
2. Weiterleitung zum Verifikationsprozess (vom Laptop/PC via QR-Code oder per Smartphone über einen direkten Link)

3. Auswahl des Identitätsdokuments: «Haben Sie eine staatliche eID?»

   a. Wenn ja, kann sich der Kunde direkt über seine staatliche eID verifizieren. Dazu scannt er einen QR-Code und kann in seiner digitalen Brieftasche die gewünschten Attribute entsprechend freigeben.

   b. Besitzt der Kunde keine staatliche eID, kann er die Frage verneinen und eine alternative Identifizierungsmethode wählen, zum Beispiel AutoIdent. Hier bekommt er konventionelle Ausweisdokumente zur Auswahl, mit denen er sich verifizieren kann – so wie man es heute schon kennt: per Scan des physischen Identitätsnachweises plus anschliessendem Selfie-Video zum biometrischen Gesichtsabgleich und zur Lebenderkennung. Ergänzend kann der Prozess auch um einen NFC-Scan erweitert werden. Dadurch

lässt sich beispielsweise der biometrische Chip eines Reisepasses mittels NFC über das Mobiltelefon auslesen. Dies gewährleistet ein besonders hohes Sicherheitsniveau, wie es beispielsweise im Finanzbereich erforderlich ist.



4. Übermittlung der Verifikationsdaten des Kunden in Echtzeit an das onboardende Unternehmen.

Massgeschneiderte Lösungen für spezifische Anwendungen

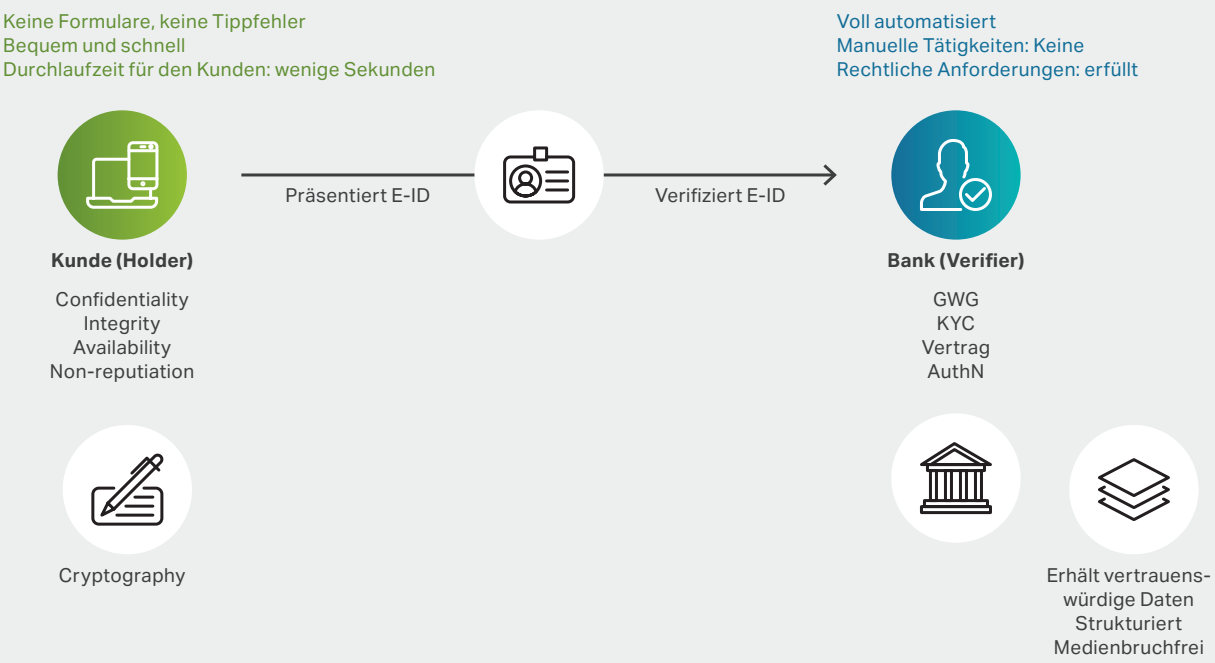
Im Zusammenhang mit der Identitätsprüfung ist es wichtig zu erkennen, dass es keine universelle Lösung gibt, die für alle Anwendungsfälle geeignet ist. Jeder Anwendungsfall erfordert je nach Industrie einen individuellen Ansatz, um den spezifischen Anforderungen gerecht zu werden. Bei der Einführung von SSI werden nicht alle Anwender:innen sofort in der Lage sein, eine eID zu besitzen oder zu benutzen. Umso entscheidender ist es, sich bereits heute damit auseinanderzusetzen, wie sich im Rahmen konkreter Szenarien die Identitätsprüfung der alten und neuen Welt zusammenführen lässt und welchen Mehrwert SSI hierbei verspricht. Technologieanbieter und Unternehmen müssen flexible und benutzerfreundliche Lösungen zur Identitätsprüfung anbieten, die sowohl eID als auch herkömmliche Identitätsdokumente berücksichtigen. Nur so kann sichergestellt werden, dass die Identitätsprüfung effizient, sicher und für alle Beteiligten zugänglich bleibt.

Praxiseinsatz von SSI

Bankwesen

Gerade im Bankwesen verspricht die Einbindung der eID auf Basis von SSI klare Vorteile – nicht nur im Hinblick auf das Vermeiden von Eingabefehlern und ein schnelles Onboarding von Kund:innen. Anstelle vieler, bisher manueller Tätigkeiten treten automatisierte Prozesse – inklusive der Erfüllung von rechtlichen Vorgaben (z. B. des im Geldwäschegesetz (GWG) geforderten "Know your customer"-Prinzips) bei verlässlicher Identifizierung. Der Kunde muss nicht länger in der Filiale vor Ort erscheinen oder sich durch aufwendige Video- oder Online-Identifizierungsverfahren quälen: Die digitale Brieftasche mit den erforderlichen verifizierbaren Nachweisen genügt, was nicht zuletzt auch die Abläufe aufseiten der Bank enorm verschlankt.

Onboarding Prozess mit EUDI/E-ID



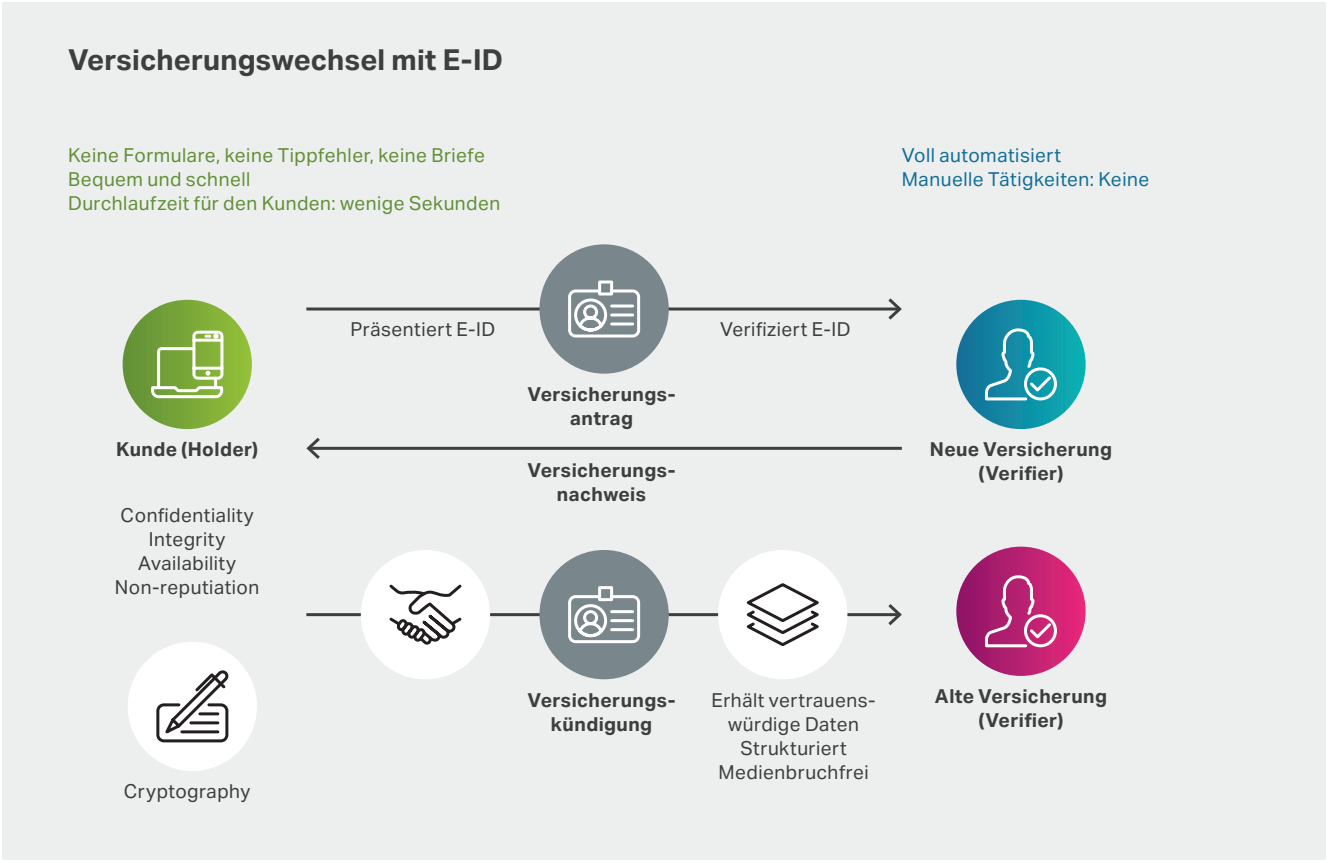
Krankenversicherung Schweiz

Ein Beispiel aus der Schweiz zeigt, wie SSI sich eignet, um Prozesse, die in der physischen Welt umständlich und mühsam sind, zu vereinfachen und so die User Experience bei den Endkunden zu verbessern und die Kosten bei den Anbietern zu senken.

Jede in der Schweiz wohnhafte Person muss zwingend eine Krankenversicherung haben. Beim Wechsel der Versicherung muss darum der Kunde zuerst eine neue Versicherung abschliessen und dann diesen Vertrag der alten Versicherung vorweisen, um die alte Versicherung zu kündigen.

Dieser Prozess ist für den Kunden sehr aufwendig, weil einzelne Schritte teilweise noch auf dem Postweg erledigt werden müssen.

Im folgenden Beispiel wird veranschaulicht, wie der Kunde mit seiner eID die neue Versicherung abschliessen kann (Identifikation und digitale Signatur) und sofort die Versicherungsdeckung als Nachweis von der neuen Versicherung erhält. Diesen Nachweis kann er zusammen mit der eID im zweiten Schritt dazu verwenden, die alte Versicherung zu kündigen.



Versicherungswechsel mit eID (Schweiz) (grafisch neu aufbereitet)

Weitere Szenarien

Die Spielfläche für SSI ist nahezu unbegrenzt. So wird beispielsweise auch die Automiete dank SSI zum Kinderspiel, wenn das Kopieren von Identitätskarte und Führerschein entfällt. Womöglich können Mieter:innen sogar direkt einsteigen und losfahren, weil das smarte Auto den Fahrzeugschlüssel als verifizierbaren Nachweis in der digitalen Brieftasche findet und prüft. Ein weiteres Anwendungsszenario ist der Bewerbungsprozess: Digital zertifizierte Dokumente wie Zeugnisse oder Diplome können im Handumdrehen übermittelt werden – und potenzielle Arbeitgeber:innen prüfen die Echtheit der Unterlagen automatisiert. Ähnlich gestaltet sich der Altersnachweis, beispielsweise um einen Jugend- oder Seniorenrabatt in Anspruch nehmen zu können. Mit SSI besteht im Zuge dessen keine Notwendigkeit mehr, einem Verkehrsbetrieb oder einem Museum das exakte Geburtsdatum offenzulegen. Gerade angesichts der Tatsache, dass in der Regel alle Personen eines Landes durch den vollständigen Namen und das Geburtsdatum eindeutig identifiziert sind, wird klar, wie innovativ die neuen Möglichkeiten daherkommen. Denn insbesondere die Bearbeitung des

Geburtsdatums ist aus Sicht des Datenschutzes derzeit noch kritisch. Im E-Commerce profitieren Händler dank SSI von einer sofortigen Bonitätsprüfung und einem schnellen Bezahlprozess. Und zwar mit einem Nachweis, der direkt mit der Bank der Käufer:innen verknüpft ist. Sichergehen können auch Käufer:innen, dass sie beim richtigen Online-Shop einkaufen und kein Geld verlieren – durch Überprüfung der digitalen Händler-Nachweise.

Sommerferien mit Self-Sovereign Identities

Es sind Sommerferien in einer Zukunft, in der sich SSI bereits flächendeckend durchgesetzt hat. Schon im Frühling freut sich Paul auf den Urlaub, denn er plant, eine spanische Insel zu erkunden. Dafür braucht er ein Auto. Im Internet findet er schnell eine Autovermietung mit tollen Angeboten und legt sein Wunschauto in den Warenkorb. Jetzt muss er den Mietvertrag abschliessen.

Der Vermieter will Pauls Führerschein und Versicherungsnachweis sehen. Der Vermieter identifiziert sich selbst, und Paul erhält die Details des Vermieters für seine digitale Brieftasche – Name, Mitgliedschaft im spanischen Tourismusnetzwerk, bestätigte Telefonnummer, Webseite und E-Mail-Adresse. Paul kennt diese Art des bestätigten Nachweises und weiss, dass seine digitale Brieftasche diese Einträge nur dann grün markiert, wenn sie auch vertrauenswürdig sind.

Paul teilt per Knopfdruck seinen Führerschein und Versicherungsnachweis – letzteres birgt gleich mehrfachen Mehrwert, denn seine eigene Autoversicherung macht beim neuen «Bring Your Own Insurance»-Programm mit. So kann er im Urlaub seine eigene Versicherung nutzen und auf teure Angebote der Autovermieter verzichten.

Paul entscheidet sich für Vorauskasse und erhält eine virtuelle Zahlungsaufforderung in seine digitale Brieftasche, die er direkt darüber begleicht. Der Vermieter hat sein Geld erhalten und bietet Paul an, den Mietvertrag und den virtuellen Autoschlüssel in seine digitale Brieftasche zu senden. Paul akzeptiert und seine digitale Brieftasche speichert die neuen Daten.

Kurze Zeit später ist es endlich so weit und Paul landet auf der Baleareninsel. Er hat sein Gepäck erhalten und geht Richtung Ausgang, als sein Handy ihn informiert, dass sein Autoschlüssel aktiviert wurde. Aufgrund der Geolocation am Flughafen erhält Paul die Position seines Mietwagens und sein Navigationssystem bietet an, ihn zum Auto zu führen. Er geht an den langen Schlangen vor den Schaltern der Autovermietungen vorbei und denkt sich, dass es wohl noch einige Zeit dauern wird, bis die neuen Möglichkeiten bei allen angekommen sind. Sobald er das Auto erreicht hat, benutzt er seinen virtuellen Schlüssel, um dieses zu öffnen. Das Auto prüft noch einmal seinen Führerschein. Nach ein paar Sekunden ist der Wagen bereit. Die Ferien können beginnen.

An diesem Beispiel wird das von SSI-ausgehende Potential mehr als deutlich. In der neuen Welt sind Nachweise aus verschiedenen Ökosystemen, sowohl von Behörden als auch aus der Privatwirtschaft, Teil der User Journey. Die digitale Brieftasche dient als zentrale Drehscheibe für Authentifizierung, Vertragsabschlüsse und den Austausch von Nachweisen. Sie überprüft alle von Issuern und Verifiern vorgelegten Informationen und zeigt dem Holder an, ob diese vertrauenswürdig sind. Darüber hinaus lassen sich Convenience-Funktionen realisieren, wie Geolocation-spezifische Hinweise. Neue, vorher undenkbare Geschäftsmodelle – wie «Bring Your Own Insurance» – werden möglich. Auch IoT-Geräte wie ein Auto, das sich nur mit gültigem Ausweis fahren lässt, sind integrierbar. Und der besondere Gamechanger: Alle Funktionen können international Anwendung finden.

Prio 1: Nicht den Anschluss verpassen

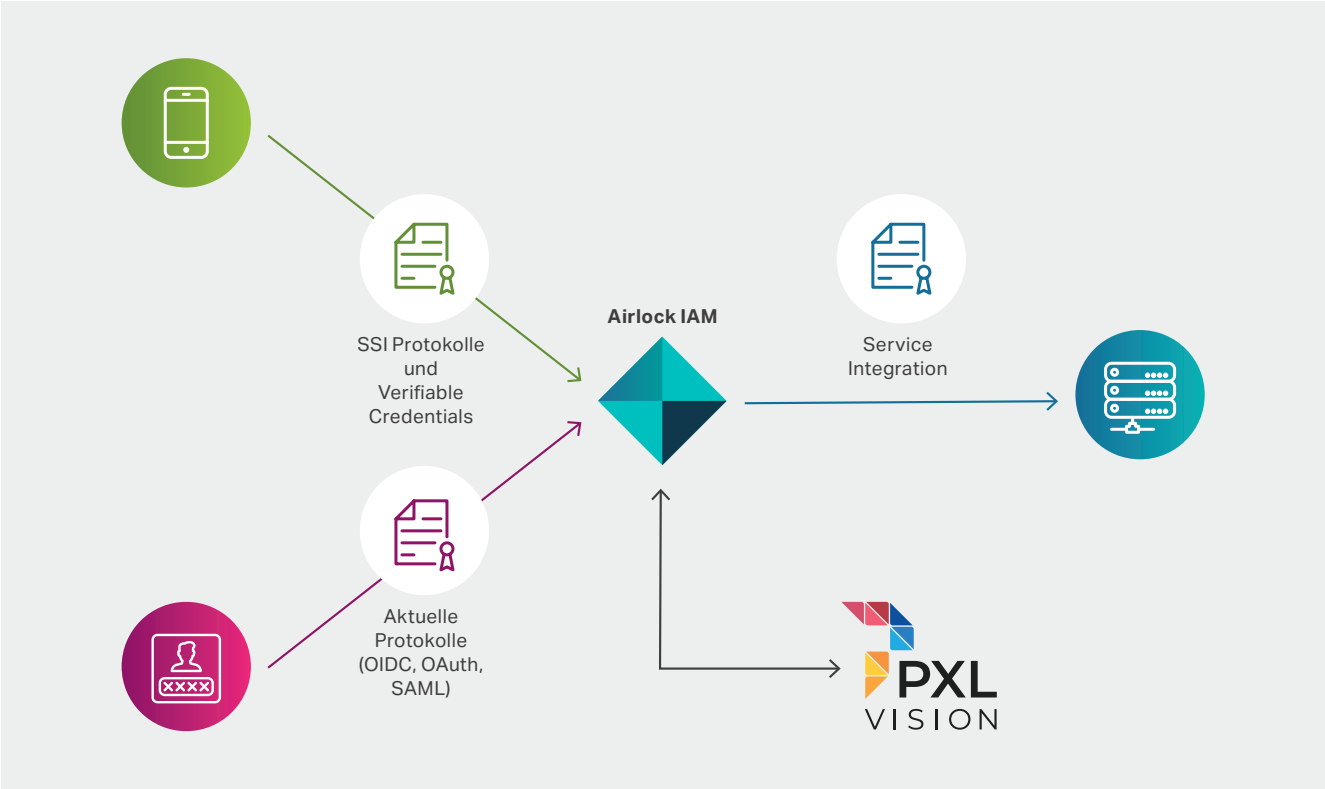
Die vorangegangenen Ausführungen haben die zahlreichen Vorteile, die eID und SSI für Privatpersonen, staatliche Institutionen und Unternehmen bereithalten, stichhaltig aufgezeigt. Zudem wurde deutlich, dass an der Überführung entsprechender Anwendungsfälle aus der Theorie in die Praxis auf internationaler Ebene bereits mit Hochdruck gearbeitet wird. Entsprechend gilt es für Unternehmen, diese Entwicklungen souverän zu begleiten und bereits jetzt eigene Use Cases zu entwickeln. Wer diese rechtzeitig auf den Weg bringen kann, sichert sich von Anfang an die damit einhergehende Nasenlänge Vorsprung im Markt – und zwar in vielerlei Hinsicht:

- **Steigerung des Kundenvertrauens**
- **Compliance (DSGVO und Co.)**
- **Security**
- **Benutzerfreundlichkeit**
- **Automatisierung**
- **Kosteneinsparung durch einfache Prozesse in den eigenen Reihen**

Moderne Ansätze zur Identitätsprüfung, wie sie Airlock und PXL Vision bieten, liefern das Fundament, mit dem sich der Weg in die neue Welt konsequent beschreiten lässt. Der Dreiklang aus Compliance, Sicherheit und Benutzerfreundlichkeit wird nachhaltig bedient.

Auf lange Sicht kann es nicht zielführend sein, SSI in jede Applikation einzeln zu integrieren, schliesslich gehen gerade vom Zusammenspiel der jeweiligen Prozesse entscheidende Synergien aus. Durch ein vorgelagertes Identitätsmanagementsystem, das sowohl die alte als auch die neue Welt unterstützt und jederzeit in der Lage ist, sich flexibel an neue Anforderungen anzupassen, lässt sich die Transformation in Richtung Zukunft massgeblich beschleunigen. Auf diese Weise halten sich Unternehmen alle Türen offen und können jederzeit ohne Verzögerung auf sich verändernde Rahmenbedingungen reagieren.

In einem Ideation Workshop können Unternehmen herausfinden, welche konkreten Chancen sich für das eigene Tagesgeschäft ergeben. Aber auch die Risiken, die drohen, wenn man nicht rechtzeitig anfängt, lassen sich im Zuge eines solchen Workshops gezielt veranschaulichen. Entlang der Darstellung konkreter Beispiele geht es vor allem darum, neue Ideen zu entwickeln, mit denen der Erfolg der individuellen Geschäftsmodelle auf Unternehmensseite vor dem Hintergrund des SSI-Siegeszugs künftig weiter gesteigert werden kann. Auf Wunsch gehen die Expert:innen von Airlock und PXL Vision darüber hinaus gerne auf geeignete Umsetzungsoptionen ein, mit denen sich schon heute die Brücke zwischen klassischer Identitätsprüfung und SSI-basierten Prozessen schlagen lässt.



Ein vorgelagertes Identitätsmanagementsystem sorgt für reibungslose Prozesse, die mit neuen Anforderungen mitwachsen.

Glossar

Abkürzung	Begriff	Erklährung
eID	elektronische Identität (eID)	eIDs sind digitale Nachweise, mit denen man sich mit verschiedensten Attributen online ausweisen kann . Sie enthalten Schlüsselattribute wie einen eindeutigen Identifikator (z. B. eine Nummer oder einen Code), persönliche Informationen (z. B. Ihren Namen und Ihr Geburtsdatum) und Sicherheitsmerkmale (z. B. kryptografische Signaturen), um die Integrität des Ausweises zu schützen. eIDs werden verwendet, um persönliche Informationen nachzuweisen, sicher auf Online-Dienste zuzugreifen, Dokumente zu unterzeichnen und Transaktionen durchzuführen. In der Schweiz wird der Begriff E-ID verwendet. In der EU wird der Begriff PID verwendet.
IdP	Identitätsanbieter, Identity Provider (IdP)	Ein Dienst oder eine Organisation, die Ihre digitale Identität verwaltet und verifiziert. Wenn Sie sich bei einer Website oder App anmelden, bestätigt der Identitätsanbieter (Identity Provider oder kurz IdP), wer Sie sind, indem er Ihre Anmeldedaten wie Benutzername und Passwort überprüft. Ausserdem gibt er bestimmte Attribute wie Ihren Namen oder Ihre E-Mail-Adresse an die Website oder App weiter, sodass Sie auf Dienste zugreifen können, ohne sich separat anmelden oder Ihre Daten mehrfach eingeben zu müssen.
	Aussteller / Issuer (SSI)	Eine Einrichtung oder Organisation, die überprüfbare Nachweise (Verifiable Credentials oder kurz VC) für Einzelpersonen erstellt und bereitstellt. Durch die Bereitstellung überprüfbarer Nachweise bestätigt der Aussteller, dass der Inhalt korrekt ist. Weitere Informationen über den Empfänger von VCs finden Sie unter Inhaber. Weitere Informationen über den Inhalt von VCs finden Sie unter prüfbare Nachweise. Weitere Informationen über die Verwendung von VCs finden Sie unter Prüfer.
	Inhaber / Holder	Eine Person, die überprüfbare Nachweise besitzt und kontrolliert. Als Inhaber bewahren Sie diese verifizierbaren Nachweise in einer sicheren digitalen Brieftasche auf und können wählen, wann und mit wem Sie sie teilen möchten, wodurch Sie die Kontrolle über Ihre persönlichen Daten erhalten. Weitere Informationen über die Ausgabe von VCs finden Sie unter Aussteller. Weitere Informationen über den Inhalt von VCs finden Sie unter verifizierbare Nachweise. Weitere Informationen über die Verwendung von VCs finden Sie unter Überprüfer.
SSI	Self-Sovereign Identity Decentralized Identity (Dezentralisierte Identität)	Ein digitales Identitätsmodell, bei dem Sie Ihre persönlichen Daten vollständig besitzen und kontrollieren. Anstatt sich bei der Verwaltung Ihrer Identität auf eine zentrale Behörde (Identitätsanbieter) zu verlassen, speichern und verwalten Sie Ihre digitalen Nachweise (wie Ausweise, Zertifikate oder andere persönliche Daten) in einer sicheren digitalen Brieftasche. Sie entscheiden, wann und an wen Sie Ihre Daten weitergeben, wodurch Sie mehr Privatsphäre und Kontrolle über Ihre Identität erhalten. In den USA wird der Begriff «Decentralized Idenity» verwendet, in Europa der Begriff «Self-Sovereign Identity».
VC	Überprüfbare Nachweise (SSI) / Verifiable Credentials / VC	Digitale Versionen von Dokumenten oder Bescheinigungen, die etwas über Sie beweisen, z. B. Ihren Ausweis, Führerschein, Bildungsabschluss, Mitgliedschaft oder Versicherungsschutz. Diese Ausweise sind sicher und können leicht von anderen überprüft werden, was bedeutet, dass die darin enthaltenen Informationen vertrauenswürdig sind. Überprüfbare Ausweise werden in der digitalen Brieftasche des Inhabers gespeichert und können von diesem bei Bedarf weitergegeben werden.

Abkürzung	Begriff	Erklährung
	Prüfer / Verifier	Eine Person oder Organisation, die den Inhaber auffordert, Informationen über seine Identität weiterzugeben. Die Prüfstelle benötigt diese Informationen, um eine Art von Geschäftsdienst zu erbringen, und kann mithilfe von überprüfbaren Nachweisen die vom Inhaber bereitgestellten Informationen erhalten und ihnen vertrauen, ohne den ursprünglichen Aussteller kontaktieren zu müssen.
	(digitale) Brieftasche	Eine digitale App, in der Regel auf einem Smartphone, in der der Inhaber überprüfbare Ausweise wie IDs, Zertifikate oder Mitgliedschaften speichert und verwaltet. Genau wie eine physische Brieftasche Karten enthält, bewahrt eine digitale Brieftasche Anmeldeinformationen sicher auf. Mit der Brieftasche kann der Inhaber entscheiden, wann und mit wem er überprüfbare Nachweise teilt.
PID	Persönliche Identifikationsdaten Personal Identification Data	Siehe eID Der Begriff PID wird in der EU verwendet. Der Begriff E-ID wird in der Schweiz verwendet.
EUDI	European Digital Identity	Ein sicheres digitales Identitätssystem, das von der Europäischen Union entwickelt wurde. Es ermöglicht EU-Bürger:innen und -Unternehmen, ihre Identität online nachzuweisen und auf Dienstleistungen in der gesamten EU zuzugreifen, z. B. auf Behördendienste, Bankgeschäfte und mehr. Die EUDI basiert auf der eIDAS 2.0-Verordnung und wird auf der Grundlage von SSI implementiert.
eIDAS 2.0		eIDAS 2.0 ist eine Überarbeitung der ursprünglichen eIDAS-Verordnung, die offiziell als Europäischer Rahmen für die digitale Identität bekannt ist. eIDAS 2.0 führt eine Europäische Geldbörse für digitale Identitäten ein, die es den EU-Bürgern ermöglicht, ihre digitalen Ausweise und Nachweise sicher zu speichern und zu verwalten. Ziel ist es, Online-Interaktionen bequemer und vertrauenswürdiger zu gestalten, indem ein nahtloser Zugang zu öffentlichen und privaten Diensten in der gesamten EU ermöglicht wird, während der Einzelne mehr Kontrolle über seine persönlichen Daten erhält.
	Selektive Offenlegung Selective Disclosure	Eine Funktion zur Verbesserung der Privatsphäre, die es Benutzer:innen ermöglicht, nur bestimmte Attribute eines überprüfbaren Ausweises und nicht den gesamten Ausweis weiterzugeben. Zum Beispiel, wenn ein Dienst nur den Namen wissen muss, ohne Geburtsdatum oder der Sozialversicherungsnummer preiszugeben. So haben Sie mehr Kontrolle über Ihre Daten und können Ihre Privatsphäre besser schützen.
GWG	Geldwäschereigesetz	Ein Gesetz, das Kriminelle daran hindern soll, illegal erworbenes Geld als rechtmässiges Einkommen zu tarnen. Es legt Regeln und Anforderungen für Finanzinstitute und Unternehmen fest, um verdächtige Aktivitäten, wie grosse oder ungewöhnliche Transaktionen, zu erkennen und zu melden. Das Gesetz hilft den Behörden, den Fluss von schmutzigem Geld durch das Finanzsystem aufzuspüren und zu stoppen, um die Wirtschaft und die Gesellschaft vor den Auswirkungen krimineller Aktivitäten zu schützen. Ein besonders wichtiger Teil dieses Gesetzes verpflichtet die Finanzinstitute, die Identität des Inhabers eines Bankkontos korrekt festzustellen.

Autoren

Elmar Reif

CPO PXL Vision

Elmar Reif ist Chief Product Officer (CPO) bei PXL Vision, einem führenden Schweizer Unternehmen im Bereich der digitalen Identitätsverifikation. Mit seiner umfassenden Erfahrung im Produktmanagement und seiner Leidenschaft für innovative Technologien ist er für die Produktstrategie und -entwicklung des Unternehmens verantwortlich. Vor seiner Tätigkeit bei PXL Vision sammelte Elmar Reif umfangreiche Erfahrungen in verschiedenen Positionen im Technologie- und Bankensektor und entwickelt nun bei PXL Vision nutzerzentrierte Lösungen, die die Art und Weise, wie digitale Identitäten verifiziert werden, revolutionieren.

Martin Kuppinger

Founder and Principal Analyst KuppingerCole

Martin Kuppinger ist Gründer und Principal Analyst bei KuppingerCole, einem führenden Analystenhaus für identitätsorientierte Informationssicherheit, sowohl in klassischen als auch in Cloud-Umgebungen. Vor KuppingerCole hat Martin Kuppinger mehr als 50 Bücher zum Thema IT geschrieben und ist als vielgelesener Kolumnist und Autor von Fachartikeln und Rezensionen in einigen der renommiertesten IT-Magazine in Deutschland, Österreich und der Schweiz bekannt. Darüber hinaus ist er ein etablierter Redner und Moderator bei Seminaren und Kongressen. Sein Interesse an Identity Management reicht bis in die 80er Jahre zurück, als er auch umfangreiche Erfahrungen in der Entwicklung von Softwarearchitekturen sammelte. Im Laufe der Jahre kamen verschiedene andere Forschungsgebiete hinzu, darunter Virtualisierung, Cloud Computing und allgemeine IT-Sicherheit. Da er Wirtschaftswissenschaften studiert hat, verbindet er fundierte IT-Kenntnisse mit einer ausgeprägten Geschäftsperspektive.

Michael Doujak

Senior Product Manager Airlock, eine Security Innovation der Ergon Informatik AG

Michael Doujak hat nach seinem Studium an der ETH Zürich verschiedene Stationen durchlaufen. Seit 20 Jahren hat er verschiedene Projekte und Lösungen im Bereich von Identity Management geplant und umgesetzt. Besonders herauszustreichen ist der Aufbau von SwissSign als Herausgeber von qualifizierten Zertifikaten in der Schweiz, der Aufbau der Patientendossier Plattform «MonDossierMedical », der Aufbau der EPD-Infrastruktur und der Zuweiser Plattform Lösung der Schweizerischen Post. Er beschäftigt sich seit mehreren Jahren mit dem Thema Self-Sovereign Identities und engagiert sich in verschiedenen Gremien, um das Thema voranzubringen. Er ist ein profunder Kenner der Materie, von der tiefen Technik bis in die geschäftlichen Anwendungsfälle hinauf. Michael Doujak ist heute als Product Manager für Airlock bei Ergon Informatik tätig.

Über Airlock – Security Innovation by Ergon Informatik AG
Der Airlock Secure Access Hub vereint die wichtigen IT-Sicherheitsthemen der Filterung und Authentisierung zu einem gut abgestimmten Gesamtpaket, das Massstäbe in Sachen Bedienbarkeit und Services setzt. Der Secure Access Hub deckt alle wichtigen Funktionen der modernen IT-Sicherheit in diesem Bereich ab: von einer durch Fachjournalisten ausgezeichneten Web Application Firewall (WAF), über ein Customer Identitäts- und Zugriffsmanagement (cIAM), dem Schweizer Banken vertrauen, hin zu einer API-Sicherheit, die neueste Anforderungen stemmt. Die IT-Sicherheitslösung Airlock schützt mehr als 20 Millionen aktive, digitale Identitäten und 30.000 Back-Ends von über 550 Kunden auf der ganzen Welt. Weitere Informationen unter www.airlock.com. Airlock ist eine Security Innovation des Schweizer Softwareunternehmens Ergon Informatik AG.

Die 1984 gegründete Ergon Informatik AG ist führend in der Herstellung von individuellen Softwarelösungen und Softwareprodukten. Die Basis für den Erfolg sind 300 hochqualifizierte IT-Spezialisten, die dank herausragendem Fachwissen neue Technologietrends schnell antizipieren und mit innovativen Lösungen entscheidende Wettbewerbsvorteile sicherstellen. Ergon Informatik realisiert hauptsächlich Grossprojekte im Bereich B2B.

Ergon Informatik AG
Merkurstrasse 43
CH-8032 Zürich
+41 44 268 89 00
info@airlock.com

www.airlock.com

ergon