

Blog Post

N° 3/2018

E-Identity-Lösungen in Europa

Ein europäischer Vergleich

Andrea Müller

Dr. Andreas Windisch

ASQUARED

asquared Blog Post N° 3/2018

Februar 2018

Copyright © asquared GmbH

Wesentliches Element eines digitalen europäischen Binnenmarktes sind Lösungen für digitale Identitäten. Europa kann dabei von den existierenden Erfahrungen und der Vielfalt der Lösungen in den europäischen Ländern profitieren. Die vorliegende Studie untersucht die europäische e-Identity-Landschaft sowie Erfolgsfaktoren für eine hohe Verbreitung und Akzeptanz. Neben hoher Benutzerfreundlichkeit, die für eine e-Identity-Lösungen als digitaler Service unabdingbar ist, zeichnen sich die klare Fokussierung auf dedizierte Anwendungsfälle und der stringente Ausbau der Anwendungsfälle entlang des Geschäftsmodells als wesentlich für den Erfolg einer Lösung ab.

Einleitung

Die zunehmende Vielfalt und Präsenz von Online-Diensten verstärkt den Bedarf nach online nutzbaren, sicheren und vertrauenswürdigen Identitäten. Vor dem Hintergrund der eIDAS werden zunehmend staatliche bzw. nationale e-Identity-Lösungen sichtbar. So hat nach Deutschland beispielsweise Italien Ende des vergangenen Jahres das EU-weite Peer-Review für das nationale e-Identity-System SPID gestartet. Weitere Länder werden folgen. Darüber hinaus drängen zunehmend privatwirtschaftliche Lösungen in das Sichtfeld einer breiten Öffentlichkeit, die nicht zwingend die Rolle eines nationalen e-Identity-Schemes übernehmen wollen. Europaweit existieren eine ganze Reihe unterschiedlicher Lösungen und Initiativen: Von mehreren Lösungen einzelner Unternehmen, über mehrere Initiativen ganzer Unternehmenssektoren bis hin zu Lösungen in Kooperation mehrerer Unternehmen.

In unserem Post „E-Identity-Initiativen – Der europäische Weg“ haben wir bereits die Relevanz und grundlegende Historie des Themas e-Identity mitsamt den aktuellen regulatorischen Rahmenwerken zusammengefasst. Diesem Post lag bereits die unsererseits durchgeführte Studie zu e-Identity-Lösungen in Europa zu Grunde, deren Ergebnisse der vorliegende Post nun tiefergehend beleuchten soll.

Theorieunterricht: Heute „e-Identity-Vokabular“

Im Themenbereich e-Identity treffen Player aus unterschiedlichen Domänen mit unterschiedlichen Blickwinkeln und Schwerpunkten aufeinander. Das Thema ist relevant für Anbieter technischer Infrastruktur, für staatliche Behörden, Banken, Unternehmen aus dem Bereich industrielle Produktion, eCommerce und Medien. Die Vielfältigkeit der Perspektiven zeigt sich häufig auch in der unterschiedlichen Sprache. Häufig werden Begriffe im Kontext e-Identity unterschiedlich verwendet. Deshalb nachfolgend zum

gemeinsamen Verständnis zunächst eine kurze Definition des sowohl im Rahmen der durchgeführten Studie als auch im vorliegenden Post verwendeten Vokabulars:

e-Identity-Mittel - Ist eine materielle und/oder immaterielle Einheit, die Personenidentifizierungsdaten enthält und zur Authentifizierung bei Online-Diensten verwendet wird (Definition aus eIDAS Artikel 3, Pkt. 2). Ein ID-Mittel kann also beispielsweise ein Personalausweis sein, ebenso wie ein elektrifizierter Dienstaussweis oder gar ein Facebook-Account.

e-Identity-Provider - Sind die Herausgeber der ID-Mittel im Rahmen eines ID-Schemes. Für den deutschen Personalausweis ist der ID-Provider das jeweilige Landeseinwohneramt, beim Facebook-Account ist es Facebook.

e-Identity-Scheme - Ist die Gesamtheit der Regeln und der technischen Standards für die Ausführung von ID-Funktionen unter Verwendung der zugrundeliegenden ID-Systeme. Der elektronische deutsche Personalausweis in Kombination mit der AusweissApp2 ist ein solches e-Identity-Scheme.

e-Identity-System bzw. -Initiative - Ist ein technisches System für die elektronische Identifizierung, in dessen Rahmen natürlichen oder juristischen Personen oder natürlichen Personen, die juristische Personen vertreten, elektronische Identifizierungsmittel ausgestellt werden (Definition aus eIDAS, Artikel 3, Pkt. 4). Facebook ist beispielsweise ein ID-System. Ist das System noch in Entwicklung, sprechen wir von einer e-Identity-Initiative.

Relying Party - Ist eine natürliche oder juristische Person, die auf eine elektronische Identifizierung oder einen Vertrauensdienst vertraut. Üblicherweise handelt es sich hier um die Service Provider (z. B. ein Online-Händler), welche auf eine Identifizierung angewiesen sind und das ID-System einbinden.

Methodik der durchgeführten Studie

Im Jahr 2015 beauftragte das holländische Innenministerium PBLQ, ein holländisches auf den Bereich e-Government fokussiertes Beratungsunternehmen damit, eine Studie über die e-Identity-Verfahren in ausgewählten Ländern der EU unter Berücksichtigung der jeweiligen politischen Motivation zur Schaffung der Systeme durchzuführen. Es wurden insgesamt elf europäische Länder untersucht: Belgien, Dänemark, Deutschland, Estland, Frankreich, Großbritannien, Holland, Luxemburg, Österreich, Portugal, Schweden und Spanien. Fokussiert wurde in dieser Studie explizit auf ID-Mittel, die zu einem nationalen ID-Scheme gehören.

Analog zu dieser Studie haben wir ebenfalls einzelne Länder Europas dahingehend untersucht, welche e-Identity-Mittel (hier -Initiativen oder -Systeme) existieren sowie ob es sich dabei um staatliche, privatwirtschaftliche oder partnerschaftlich orientierte Modelle handelt. Der Abgleich der beiden Studien ermöglicht bereits einen interessanten zeitlichen Vergleich. So zeigen die identifizierten Systeme/Initiativen, dass innerhalb der vergangenen zwei Jahre übergreifend vor allem das Engagement privatwirtschaftlicher Initiativen bzw. der Partnerschaften zwischen Privatwirtschaft und Staat deutlich gestiegen ist.

Im Ergebnis dessen haben wir im Rahmen unserer Untersuchung auch ID-Mittel betrachtet, die nicht notwendigerweise zu nationalen ID-Schemes gehören. Darüber hinaus haben wir den geographischen Umfang der Studie ausgedehnt und alle europäischen Länder analysiert. Zusätzlich haben wir den aktuellen Entwicklungen im Bereich e-Identity Services Rechnung getragen und eine Differenzierung hinsichtlich des e-ID-Ansatzes vorgenommen, wie nachfolgend erläutert.

Einordnung in staatliche vs. privatwirtschaftliche Lösungen

Bei der Klassifizierung in staatliche oder privatwirtschaftliche ID-Mittel sind wir grundlegend wie die Kollegen von PBLQ vorgegangen: Wir haben untersucht, wer die Verantwortung für die Erstellung, die Implementierung sowie die Pflege hat und wem die direkte Kontrolle obliegt.

Ein *Staatliches ID-Mittel* ist ein solches, für welches die Regierung des jeweiligen Landes hauptverantwortlich ist für die Erstellung, die Implementierung und die Pflege sowie dieses direkt kontrolliert.

Ein *Privatwirtschaftliches ID-Mittel* ist ein solches, für welches ein oder mehrere privatwirtschaftliche Unternehmen hauptverantwortlich sind für die Erstellung, die Implementierung und die Pflege sowie dieses direkt kontrollieren. Gewährt ein privatwirtschaftliches ID-Mittel Zugriff zu öffentlichen Diensten, dann ist die staatliche Verantwortung für die Kontrolle des ID-Mittels weiterhin gesetzt.

Ein ID-Mittel einer *Öffentlich-privaten Partnerschaft* (engl. Public Private Partnership - PPP) ist ein solches, für welches sowohl die Regierung des jeweiligen Landes als auch ein oder mehrere privatwirtschaftliche Unternehmen hauptverantwortlich sind für die Erstellung, die Implementierung und die Pflege sowie dieses direkt kontrollieren. Auch hier gilt, dass für den Fall der Gewährung des Zugriffs auf öffentliche Dienste mittels des ID-Mittels die staatliche Kontrolle des ID-Mittels weiterhin gesetzt ist.

Funktionsumfang bzw. Wertschöpfung

Bei der Analyse der einzelnen ID-Mittel haben wir untersucht, welche Funktionalitäten jeweils unterstützt werden, da diese direkte Auswirkungen auf die potentiellen Einsatzgebiete hat. So existieren ID-Mittel, die maßgeblich auf die Übergabe personenbezogener Daten im Sinne einer Identifizierung abzielen, aber auch solche, die zusätzlich eine Authentifizierung ermöglichen, um als Universalschlüssel für verschiedenste Dienste zu fungieren. Andere bieten die Möglichkeit des spezifischen Datenmanagements oder aber auch des Signierens elektronischer Dokumente unter Nutzung einer qualifizierten digitalen Signatur (QES).

Nachfolgend sind die untersuchten Funktionsblöcke beschrieben. Erfüllte eines der untersuchten ID-Mittel diese Anforderungen, so haben wir diesen Funktionsblock zum Funktionsumfang des ID-Mittels aufgenommen.

I - Identifikation – Ist die Bereitstellung und Übergabe aller anwendungsbezogenen erforderlichen Merkmale einer Entität, hier natürlichen Person (z. B. Name, Anschrift, E-Mail-Adresse) an die Relying Party. Dabei kann zum einen der übergebene Datensatz je nach Relying Party und Anwendungsfall unterschiedlich umfangreich sein, zum anderen können dabei unterschiedliche Vertrauenslevels Anwendung finden. Es können ebenso Metadaten für nachfolgende Authentifizierungen übertragen werden.

A - Authentifikation – Ist das (häufig einer initialen Identifikation nachstehende) Erkennen einer natürlichen Person, üblicherweise handelt es sich um den Login bei einer Relying Party. Das ID-Mittel stellt dabei eine technische Lösung bereit, mit deren Hilfe sich der User authentifiziert, wodurch dieser in Folge von der Relying Party für einen bestimmten Dienst legitimiert wird. Aus diesem Grund zählen wir hierzu auch Verifikations-Use Cases, bei denen die Relying Party Daten zur Verifikation an den e-identity-Provider übermittelt. Abhängig vom Anwendungsfall kann es sich um eine einfache (Ein-Faktor-) oder auch eine Zwei-Faktor-Authentifikation handeln.

D - Datenübergabe – Einige Anbieter bieten die Möglichkeit, nach Zustimmung des Users personenbezogene Daten an die Relying Party zu übergeben, die über die zur Identifikation genutzten Daten hinausgehen. Hierbei kann es sich beispielsweise auch um Kontext-bezogene Informationen handeln.

T - Daten-Tracking – Auch das Verwerten expliziter und impliziter Transaktionsdaten des Benutzers steht im Vordergrund einiger Anbieter. So kann es sich beispielsweise um Lösungen zur digitalen Einholung von Tracking-Opt-Ins handeln, die im Zusammenhang mit der Nutzung des ID-Mittels angeboten werden.

S - QES – Neben der digitalen Identifikation ist die rechtssichere digitale Willenserklärung ein wesentliches Element zur Schaffung eines digitalen Vertrauensraums. Einige e-ID-Systeme integrieren die Möglichkeit, digitale Dokumente zu signieren. In diesem Fall kommt eine qualifizierte digitale Signatur zum Einsatz.

Überblick über die europäische e-Identity-Landschaft

Für die Übersicht der e-Identity-Landschaft sind in Summe 30 Länder betrachtet worden: Die 28 Länder der Europäischen Union sowie Norwegen und die Schweiz. Bei unseren Recherchen konnten wir 94 e-Identity-Lösungen identifizieren, welche wir genauer analysiert haben.

Wie bereits in unserem vorherigen Beitrag „E-Identity-Initiativen – Der europäische Weg“ beschrieben, lagen die ersten Schritte auf dem Weg zur Schaffung digital nutzbarer Identitäten bereits vor vielen Jahren in der Digitalisierung amtlicher Identitätsmittel. So ist es nicht verwunderlich, dass ein Großteil der identifizierten e-Identity-Lösungen eben diesen Ursprung haben: Unsere Übersicht enthält in Summe 46 staatliche Initiativen bzw. Lösungen, die überwiegend auf den jeweils staatlich ausgegebenen Identifikationsmitteln basieren; in der Regel handelt es sich dabei um die nationalen digitalen Personalausweise. Einige dieser Lösungen enthalten jedoch auch die Möglichkeit, Identifikationen oder Verifikationen für weniger sicherheits-relevante Anwendungsfälle ohne Personalausweis durchzuführen. Dem stehen in Summe 43 privatwirtschaftliche Initiativen bzw. Lösungen gegenüber, welche teilweise für höherwertige Identifizierungen die staatlichen Identifizierungsmittel ebenso integrieren. Insgesamt konnten 5 öffentlich-private Partnerschaften identifiziert werden, bei denen staatliche und privatwirtschaftliche Parteien eine gemeinsame Lösung offerieren.

Die nachfolgende Infografik verdeutlicht, in welchem Land nur staatliche oder nur privatwirtschaftlich getriebene e-Identity-Lösungen nutzbar sind, wo sowohl staatliche als auch private Lösungen bzw. wo keine relevanten Lösungen zur Verfügung stehen.

gesetzlich verpflichtet, die behördliche Kommunikation ausschließlich digital abzuwickeln - eine entsprechend weitverbreitete Nutzung ist folgerichtig. Diese liegt in Dänemark bei nahezu 100%, in Finnland bei mehr als 60% sowie in Norwegen und Schweden bei mehr als 70% der Bevölkerung. Ein interessanter Einblick in die digitale Normalität der nordischen Länder, wird im FinTech Podcast #136 „Payment in den Nordics“ von den Kollegen von Arkwright Consulting gegeben.

Nachfolgend haben wir darüber hinaus im Speziellen die DACH-Region ausgewählt und möchten die dort jeweils vorzufindende Lösungslandschaft in Deutschland, in Österreich sowie in der Schweiz exemplarisch beschreiben.

e-Identity in Deutschland

Deutschland hat mit der Herausgabe des Personalausweises im Checkkartenformat mit integriertem RFID-Chip bereits im Jahr 2010 mit der Etablierung eines staatlichen e-Identity-Schemes begonnen. Die Hard- und Software zur Nutzung der Online Ausweisfunktion wird von verschiedenen Unternehmen bereitgestellt, der Staat übt jedoch eine Kontrollfunktion aus. Die Lösungen müssen den vorgegebenen Kriterien entsprechen. Obwohl durch den Aufsatz auf den Personalausweis die Verbreitung des e-ID-Mittels groß ist, bleibt die Nutzung hinter den Erwartungen zurück. Als Ursache wurde unter anderem die bis zum letzten Jahr für Bürger optionale Aktivierung der Online Ausweisfunktion gesehen. Mindestens ebenso starken Einfluss dürften die bisher überschaubaren Einsatzmöglichkeiten der Online Ausweisfunktion ausüben, in denen der fehlende Anreiz zur Nutzung der Funktion zu sehen ist.

Produkt (alphabetisch sortiert)	Anbieter	Ownership	Funktionsumfang				
			I	A	D	T	S
Deutscher e-Identity-Scheme auf Basis des deutschen Personalausweises (nPA)	Deutschland	Staatlich	x	x	-	-	x
Giropay-ID	Giropay GmbH	Privat	-	x	-	-	-
Helix Alpha (Release Alpha)	Blockchain Helix	Privat	x	x	x	-	-
Identity™ Giro	Identity Trust Management AG	Privat	x	-	-	-	-
Idento.One (in Entwicklung)	Orbiter GmbH	Privat	-	x	x	-	-
Login-Allianz DEA (in Entwicklung)	United Internet AG (Schirmherr)	Privat	-	x	x	x	-
PostID	Deutsche Post AG	Privat	x	-	-	-	-
SmartWallet, SmartLogin (in Entwicklung)	Jolocom GmbH	Privat	x	x	x	-	-
Verimi (in Entwicklung)	Verimi GmbH	Privat	x	x	x	-	-
YES (in Entwicklung)	YES Europe GmbH	Privat	x	x	x	-	x

Tabelle 1: Übersicht e-Identity-Initiativen und -Systeme in Deutschland / Stand Januar 2018

Neben dem staatlichen e-Identity-Scheme sind in Deutschland auch privatwirtschaftliche Lösungen aktiv. Der Funktionsumfang der Lösungen ist jedoch geringer als der des staatlichen Schemes, sie erreichen keine digitalen Identifizierungen nach den

Vorschriften des GwG. So hat die Deutsche Post mit PostID seit 2015 eine Lösung im Angebot, die es Kunden ermöglicht, nach einer erstmalig vorgenommenen Identifizierung die Identitätsdaten zu archivieren und in anderen, nicht den GWG-Erfordernissen unterliegenden Identifizierungsprozessen erneut zu verwenden. Die Verbreitung und Nutzungshäufigkeit dieses Service ist leider bislang hinter den Erwartungen zurückgeblieben. Mit *Identity™ Giro* und *Giro-pay-ID* existieren darüber hinaus Lösungen, die die in den Banksystemen erfassten Nutzerdaten für Identifizierungen oder Verifizierungen (Altersverifikation) nutzbar machen. An dieser Stelle setzt auch YES an. Ziel ist es, dem Nutzer zu ermöglichen, seine bei seiner Bank erfassten Identitätsdaten digital für andere Anbieter zu nutzen. YES will dabei die Infrastruktur zur Verfügung stellen, die es ermöglicht, die ID-Daten des Nutzers mit Zustimmung des Kunden aus dem Banksystem zu den anfragenden Unternehmen zu übermitteln. Digitale Zustimmungs- und Signaturdienste sollen ebenso Bestandteil des Angebotes von YES sein, welches der CEO Daniel Goldscheider auf der NOAH17 im November letzten Jahres in London vorgestellt hat. Das Timing ist bewusst gewählt: YES positioniert sich bei Banken als Enabler eines Freemium Modells für die den Banken durch die PSD2 auferlegte Öffnung des Online Banking. Die Fiducia & GAD IT AG hat bereits einen eigenen ähnlichen Vertrauensdienst für die Genossenschaftliche Finanzgruppe angekündigt (Arbeitstitel CAS).

Im Jahr 2017 kündigten zwei unternehmensübergreifende privatwirtschaftliche Initiativen ihren Markteintritt an. *Verimi* hat sich zum Ziel gesetzt, „die sicherste und nutzerfreundlichste Vertrauensplattform für Identitätsdienste und Zahlungen in Europa“ zu werden. Das Gemeinschaftsunternehmen, in das mehrere Unternehmen mit einem großen Nutzerstamm wie Allianz, Axel Springer, Deutsche Bank und Telekom investiert sind, hat im Dezember 2017 bekannt gegeben, dass es in diesem Frühjahr mit einer Login-Lösung an den Markt gehen will. Die Nutzer können sich zentral bei *verimi* registrieren und sich mittels dieser Registrierung bei anderen Services anmelden und einloggen. Die Weitergabe der Daten erfolgt nur auf Wunsch der Nutzer, die Integration eines Opt-ins für elektronische Kommunikationsdaten gemäß e-Privacy Verordnung ist ebenso mit angekündigt. Neben einem eigenen Authentifizierungssystem ist die Kooperation mit Mobile Connect avisiert. In Ausbauphasen ist die Integration des elektronischen Personalausweises vorgesehen. Die zweite Initiative, die ebenso aus einer Initiative kundenstarker Unternehmen entstanden ist, plant spätestens zum 25. Mai live zu gehen. Die Initiatoren RTL, ProSiebenSat.1 und United Internet planen in der Rechtsform einer Stiftung eine *Login Alliance* am Markt zu etablieren. Details zum Funktionsumfang der Lösung sind gegenwärtig noch nicht offiziell kommuniziert.

Neben diesen unternehmensübergreifenden e-ID-Systemen gibt es weitere privatwirtschaftlich getriebene Initiativen zur Etablierung einer e-Identity-Lösung. Die Blockchain Helix AG, die Jolocom GmbH und die Orbiter Gruppe setzen dabei jeweils auf die Blockchain-Technologie. Mit *Helix Alpha* hat Blockchain Helix im letzten Jahr ein erstes

Release veröffentlicht. Die Client Anwendung soll für den Nutzer als persönliche Datencockpit und Archiv fungieren und es dem Nutzer zukünftig erlauben, das geplante Trust-Provider Netzwerk zu nutzen. Angebundene Trust Provider, beispielsweise Banken und Versicherungen, können über dieses mit Einwilligung des Nutzers Identitätsdaten austauschen. Auch *Jolocom* bietet eine Alpha Version, die Zugang zur zugehörigen Smart Wallet bietet, in der der Nutzer seine ID Daten speichern und bei verschiedenen Anbietern verwenden kann. *Idento.One* der Orbiter Gruppe fokussiert ebenso auf das Thema Datenmanagement und positioniert sich als der Treuhänder für die sichere Verwahrung von Daten und digitalen Vermögenswerten.

Neben dem etablierten staatlichen e-Identity-Scheme gibt es in Deutschland somit eine Reihe privatwirtschaftlicher Initiativen, die für die nahe Zukunft die Etablierung eines e-Identity-Systems angekündigt haben. Für den Bereich e-Government wird der entscheidende Faktor die Digitalisierung von Verwaltungsdiensten sein, um einer Anwendung des staatlichen Identitätsmittels Raum zu geben. Und auch die privatwirtschaftlichen Initiativen - marktgerechte Convenience und Sicherheit vorausgesetzt - stehen und fallen in der Benutzerakzeptanz mit den Anwendungsfällen. Entscheidend wird hier, wie weit es gelingt, nicht nur singuläre Anwendungsfälle, sondern Ökosysteme zu etablieren, die zahlreiche, sich gegenseitig befördernde relevante Services für die Nutzer bieten. Das Jahr 2018 wird hier sicher der Beginn einer längeren Reise.

e-Identity in Österreich

Österreich hat im Jahr 2003 bereits relativ früh einen amtlichen und elektronischen Ausweis zur Nutzung einzelner digitaler e-Government-Anwendungsfälle etabliert – die *Bürgerkarte*. Seitdem wurden zu diesem staatlichen Identifikationsmittel auch privatwirtschaftliche Lösungen entwickelt und etabliert, welche die nachfolgende Tabelle zusammenfasst.

Produkt (alphabetisch sortiert)	Anbieter	Ownership	Funktionsumfang				
			I	A	D	T	S
Bürgerkarte	Österreich	Staatlich	x	x	-	-	x
e-Identifikation	STUZZA - Studiengesellschaft für Zusammenarbeit im Zahlungsverkehr GmbH	Privat	-	x	-	-	-
Handy-Signatur und App	A-Trust Gesellschaft für Sicherheitssysteme im elektronischen Datenverkehr GmbH	PPP	x	x	-	-	x
MIA (vor Markteintritt)	Österreichische Staatsdruckerei GmbH	Privat	x	x	x	-	-

Tabelle 2: Übersicht e-Identity-Initiativen und -Systeme in Österreich / Stand Januar 2018

Wie eingangs erwähnt, ist die Bürgerkarte Österreichs nationales e-Identity-Mittel, welches den Zugriff auf e-Government Anwendungen ermöglicht und zum digitalen Signieren verwendet werden kann. Für die Entwicklung und technische Infrastruktur der Handy Signatur zeichnet die A Trust GmbH verantwortlich. A-Trust bietet die Möglichkeit, die Services der Bürgerkarte mit diversen Medien nutzbar zu machen. So kann eine

Vielzahl von Smartcards, beispielsweise Dienstaussweise, Zutrittskarten oder Gesundheitskarten als e-ID-Mittel aktiviert werden, die digitale Signatur wird darauf jeweils freigeschaltet. Aber auch eine mobile Lösung der Bürgerkarte wurde mit der *Handy-Signatur* lanciert. Diese stellt aktuell die verbreitetste Form der e-ID in Österreich darstellt und erreicht eine Verbreitung von ca. 12% der österreichischen Bevölkerung mit einer durchschnittlichen täglichen Transaktionsanzahl von 18.000. Seit mittlerweile fünf Jahren befindet sich zudem ein Angebot der österreichischen Banken am Markt, das durch die STUZZA realisierte Produkt *e-Identifikation*. Dieses macht die bei den Banken vorliegenden Identitätsdaten für elektronische Identifikationen nutzbar macht. Die Österreichische Staatsdruckerei hat mit MIA im Jahr 2015 ein weiteres e-ID-Produkt vorgestellt. Es handelt sich dabei um ein digitales Ausweissystem für Smartphones, welches es erlaubt, den Personalausweis, den Führerschein und weitere Identitätsdokumente digital zu verwenden. MIA ist aktuell noch nicht verfügbar, da bislang noch kein Beschluss der Republik Österreich vorliegt, MIA offiziell einzuführen.

Österreich bleibt seit vielen Jahren seiner Linie treu, e-Identity-Mittel kontinuierlich auszurollen. Ein universell einsetzbares und für diverse Medien verfügbares Signaturbasiertes Verfahren ermöglicht hier die notwendige Flexibilität unterschiedlicher Ansätze. Um die eIDAS-Konformität in der Ausgabe dieses e-Identity-Mittels zusätzlich zu erhöhen, soll als Ausgabeweg zukünftig eine Aktivierung dieser Funktionalität bei Passbestellungen und -erneuerungen durchgesetzt werden. Darüber hinaus soll die Anzahl unterstützter Einsatzbereiche durch Integration zusätzlicher Attribute, wie beispielsweise das Geburtsdatum und die Adresse, erweitert werden.

e-Identity in der Schweiz

Die Schweiz befindet sich als Nicht-EU-Mitglied und einer damit einhergehenden lediglich „zeitverzögerten defacto-Regulierung“ in der komfortablen Situation, neue regulatorische Initiativen aus Europa aus nächster Nähe zu beobachten und erst nachdem sich die Situation sortiert hat, die funktionierenden Lösungswege einzuschlagen. Im Bereich der e-Identity-Lösungen platzierte die Schweiz im Jahr 2010 mit der *Suisse ID* bereits frühzeitig einen eigenen Lösungsentwurf, der sich auf dem Markt jedoch nicht durchsetzen konnte. Die nachfolgende Tabelle fasst die aktuell verfügbaren/angekündigten e-Identity-Mittel in der Schweiz zusammen.

Produkt (alphabetisch sortiert)	Anbieter	Ownership	Funktionsumfang				
			I	A	D	T	S
eID Zug	Zug, basierend auf Consensys uPort	Staatlich	x	x	x	-	-
Schaffhauser eID+	Stadt Schaffhausen, basierend auf Procivis eID+	Staatlich	x	x	x	-	-
SwissID	SwissSign AG	Privat	x	x	x	-	x

Tabelle 3: Übersicht e-Identity-Initiativen und -Systeme in der Schweiz / Stand Januar 2018

Für das Scheitern des im Jahr 2010 im Rahmen einer öffentlich-privaten Partnerschaft lancierten e-Identity-Verfahrens SuisseID sind unterschiedlichen Gründe zu sehen. So waren beispielsweise die hohen Initialkosten und die wenig zeitgemäße technische Realisierung mit USB-Stick bzw. Smartcard und Reader eine zu hohe Hürde für die geringe Anzahl verfügbarer Anwendungsfälle. Dies soll nun eine Allianz aus einer Reihe von Großkonzernen ändern. Ende vergangenen Jahres haben sich analog zum deutschen verimi-Ansatz branchenübergreifend neun Konzerne zusammengetan, um aus der vor sich hin dümpelnden SuisseID eine erfolgreiche SwissID zu machen. Dabei soll nun ein dezentraler e-Identity-Ansatz zum Einsatz kommen. An das System sollen mehrere Anbieter angebunden werden, die als e-Identity Provider jeweils eigene Datenbanken mit den Personendaten ihrer Kunden führen. Kunden können auch bei mehreren e-Identity-Providern registriert sein. Waren ursprünglich ausschließlich private Unternehmen als e-Identity-Provider vorgesehen, so enthält das als Kompromiss erzielte Konzeptpapier der Swiss Data Alliance jetzt öffentliche Ämter als e-Identity-Provider. Darüber hinaus soll der ID-Vermittler, der zwischen die e-Identity-Provider und die Relying Parties geschaltet ist, für die Anonymisierung der Anfragen sorgen, sodass die e-Identity-Provider keine Kenntnis über die konkret genutzten Relying Partner bzw. deren Services erlangen. Das Gemeinschaftsunternehmen *Swiss Sign Group* soll als Vermittler zu den einzelnen e-Identity-Providern auftreten. Bis zum Sommer 2018 wird der Bundesrat ein Gesetzentwurf vorlegen mit klaren Regeln für einen staatlich anerkannten elektronischen Identitätsnachweis für privatwirtschaftliche e-Identity-Provider. Die konkrete Ausgestaltung ist damit im Detail noch offen.

Parallel zu dieser Diskussion haben auf lokaler Ebene zwei Schweizer Gemeinden bereits eigene e-Identity-Mittel auf Blockchain-Basis bereitgestellt. Die Stadt Zug bietet seit Herbst 2017 mit *Zug ID* eine Ethereum-Blockchain-basierte Lösung an (es handelt sich um uPort von Consensus). Die ID-Daten liegen hier im digitalen Schließfach der App des Nutzers, die Stadt überprüft und bestätigt lediglich die Identität der Person. Zur Überprüfung muss der Nutzer der Zug ID einmalig persönlich im Stadthaus vorstellig werden. Die Ausgabe der e-ID's erfolgt bereits, die Anwendungsfälle werden jedoch erst nach und nach geschaffen. Der Kanton Schaffhausen hat im Dezember letzten Jahres das e-Identity-Mittel *Schaffhauser eID+* pilotiert. Diese nutzt die ebenfalls Blockchain-basierte Lösung eID+ von ProCivis. Beide Initiativen sollen zunächst mindestens bis Frühjahr 2018 laufen.

Sowohl auf regionaler, als auch auf nationaler Ebene existieren mit den aufgeführten Initiativen in der Schweiz Ansätze für den Aufbau von e-Identity-Systemen, die kurzfristig eine weitere Ausgestaltung erfahren werden. Insbesondere die Etablierung erster Anwendungsfälle wird hier spannend, wobei Swiss ID auf ein Portfolio aus vorangegangenen Aktivitäten einzelner Initiatoren zurückgreifen kann.

Fazit

Wir haben uns die europäische e-Identity-Landschaft angesehen mit dem Ziel, ein Gefühl dafür zu bekommen, welches Land bei der Etablierung eines e-Identity-Ökosystems besonders erfolgreich agiert und was zu den Erfolgsfaktoren zu zählen ist. In Summe haben wir 30 Länder mit insgesamt 94 e-Identity-Systeme bzw. -Initiativen analysiert.

Übergreifend betrachtet, tut sich sehr viel: Die staatlichen Lösungen entwickeln sich länderübergreifend langsam aber stetig weiter. Der Fokus liegt dabei hauptsächlich auf der Bereitstellung digital auslesbarer und online nutzbarer e-Identity-Mittel für e-Government-Anwendungsfälle sowie digitaler Signaturen. Die eIDAS wird hier im Hinblick auf europaweite Nutzung der nationalen Lösungen für Aufwind sorgen. Gleichzeitig existieren privatwirtschaftliche Ansätze, die eigene Identifizierungsmittel bereitstellen und/oder die verfügbaren staatlichen Mittel integrieren, insbesondere für höherwertige Anwendungsfälle. Bekanntestes und erfolgreichstes Beispiel hierfür sind die durch Banken getriebenen Initiativen in den skandinavischen Ländern. Diese kooperativen Ansätze - bei denen mehrere Parteien ihre Kräfte gebündelt haben - zeichnen sich durch hohe Akzeptanz und Relevanz in ihren Märkten aus. Positiv hervorzuheben sind sowohl die Beispiele *bankID* (Norwegen), *BankID* (Schweden) und *TUPAS* (Finnland) als Kooperationslösung der jeweilig führenden nationalen Banken als auch *NEM ID* aus Dänemark als Kooperation zwischen Staat und einem spezialisierten IT Provider der Banken mit dem gemeinsamen und konsequenten Fokus auf die Digitalisierung aller behördlichen und wirtschaftlichen Kommunikationsprozesse. Die Kooperationsbereitschaft hat an dieser Stelle unweigerliche Vorteile: Man löst das berühmte Henne-Ei-Problem und/oder vermeidet Mehrkosten durch gegenseitige Konkurrenz.

Zusätzlich zur Offenheit für Kooperationen erweist sich die Fokussierung auf dedizierte Anwendungsfälle als notwendig in der Etablierung von e-Identity-Systemen. Dabei spielen sowohl vergleichbare regulatorische Anforderungen eine wesentliche Rolle, als auch die Verbindung von Anwendungsfällen, die zusätzliche Services zu den etablierten Produkten ermöglichen. Insofern besteht die Herausforderung insbesondere darin, Vielfalt als Bereicherung und Triebkraft für die weitere Entwicklung und Verbreitung gemeinsamer e-Identity-Systeme zu nutzen und diese nicht durch Konkurrenz zur Beschränkung zu führen.

Quellenangaben

- 1 FinTech Podcast #136, Payment in den Nordics, 19.01.2018, <https://paymentand-banking.com/fintech-podcast-136-payment-in-den-nordics>
- 2 Bundesministerium für Digitalisierung und Wirtschaftsstandort Wien, Digital Roadmap Austria, zuletzt abgerufen am 30.01.2018, <https://www.digitalroadmap.gv.at/>
- 3 derStandard.at, Mia: Österreichische Ausweis-App macht Daten ohne Speichern zugänglich, 29.04.2016, zuletzt abgerufen am 30.01.2018, <https://derstandard.at/2000035996259>
- 4 Österreichische Staatsdruckerei, MIA, zuletzt abgerufen am 30.01.2018, <https://www.mia.at/>
- 5 STUZZA, e-Identifikation, zuletzt abgerufen am 30.01.2018, <http://eservice.stuzza.at/de/kundenservice/e-identifikation-e-id.html>
- 6 A-SIT Zentrum für sichere Informationstechnologie, Handy-Signatur und Bürgerkarte, zuletzt abgerufen am 30.01.2018, <https://www.buergerkarte.at/>
- 7 Handelsblatt, verimi-Chefin Donata Hopfen im Interview, 26.01.2018, zuletzt abgerufen am 30.01.2018, <http://www.handelsblatt.com/20886236.html>
- 8 Neue Zürcher Zeitung, Neun Schweizer Grosskonzerne preschen bei der elektronischen Identität voran, 21.11.2017, zuletzt abgerufen am 30.01.2018, <https://www.nzz.ch/ld.1331019>
- 9 Eidgenössisches Justiz- und Polizeidepartement EJPD, Eine staatlich anerkannte digitale Identität: Bundesrat bringt Gesetz bis Sommer 2018, 15.11.2017, zuletzt abgerufen am 30.01.2018, <https://www.ejpd.admin.ch/ejpd/de/home/aktuell/news/2017/2017-11-15.html>
- 10 Business-on.de, Interview mit FinTech-Pionier WebID und Geschäftsführer Frank Stefan Jorga, zuletzt abgerufen am 30.01.2018, http://www.business-on.de/berlin/_id27376.html
- 11 Vorstellung YES auf der NOA London <https://www.noah-conference.com/videos/?/show/LALz9Fia8Pfo5fyb>
- 12 Blockchain Helix Pressemeldung zu Helix Alpha <https://www.openpr.de/news/985780>
- 13 Jolocom, Präsentation zur Smart Wallet <https://www.slideshare.net/jolocom/jolocom-revolutionizing-identity>

- 14 Swiss Data Alliance, Konzeptpapier zur Swiss ID, <https://www.swissdataalliance.ch/aktuelles-content/konzept-fur-die-digitale-identitat-in-der-schweiz-vorgestellt>
- 15 IT-Finanzmagazin, Konkurrenz zu YES, Verimi und CAS? idento.one will Identitäten per Smart-Contracts (Blockchain) verwalten, <https://www.it-finanzmagazin.de/?p=62446>
- 16 IT-Finanzmagazin, fiducia & GAD IT in Münster: Die COM17 – viel Migration und der Wunsch nach mehr Innovation bei VR-Banken, <https://www.it-finanzmagazin.de/?p=49306>
- 17 European Commission Joinup, Italy starts EU-wide peer review of its eID system, <https://joinup.ec.europa.eu/news/eidas-pre-notification>
- 18 Giropay, Online ausweisen mit Giropay-ID, <https://www.giropay.de/kaeuffer/online-ausweisen/>
- 19 Identity™, Identity™ Giro - Identitätsprüfung über ein bestehendes Konto innerhalb von einer Minute, <https://www.identity.tm/giro.html>
- 20 Idento.one, Personal Data Banking Provider, <http://idento.one/>
- 21 Ralf Keuper @ Bankstil, PSD2 und DSGVO: Datenschutz auf unterschiedlichem Niveau?, <https://bankstil.de/psd2-und-dsgvo-datenschutz-auf-unterschiedlichen-niveau>
- 22 Deutsche Post AG, POSTID - Ihr Ausweis im Internet, <https://www.deutsche-post.de/de/p/postid.html>
- 23 verimi Website, <https://verimi.de/>
- 24 Stadt Zug, Blockchain-Identität für alle Einwohner, http://www.stadtzug.ch/de/ueberzug/ueberzugrubrik/aktuelles/aktuellesinformationen/?action=showinfo&info_id=383355
- 25 Paul Kohlhaas, Zug ID: Exploring the First Publicly Verified Blockchain Identity, <https://medium.com/uport/38bd0ee3702>
- 26 Kanton Schaffhausen, Schaffhauser eID+, <https://www.sh.ch/Schaffhauser-eID.5016.0.html>

Autoren



Andrea Müller verfügt über langjährige Erfahrung in der Gestaltung von Digitalisierungs- und Transformationsprozessen im Finanzsektor sowie in der Fertigungsindustrie. Als Wirtschaftsinformatikerin und Ökonomin wirkte sie dabei in verantwortlichen Positionen in Industrie- und Beratungsunternehmen.



Dr. Andreas Windisch ist Managing Director bei asquared. Er ist Diplom-Informatiker und promovierter Ingenieur. Er wirkte in leitenden Positionen bei Automobil-, Technologie- und Beratungsunternehmen und verfügt über langjährige Erfahrungen im Bereich des IT-Transformationsmanagements, insb. im Banken- und Finanzdienstleistungssektor.



Über asquared

Asquared ist eine Unternehmensberatung aus Berlin. Mittelpunkt der Arbeit ist die Erarbeitung praktischer Lösungsansätze für den regulatorisch, technologisch und/oder gesellschaftlich induzierten Wandel, verbunden mit der jeweilig unmittelbaren Anwendung und Bestätigung im industriellen Umfeld.

Unser Augenmerk liegt stets auf Business und Technologie und ihrem Wechselspiel. Von der Neuausrichtung der Strategie, über das (Re)Design von Produkten und Services bis hin zur Operationalisierung – wir gestalten die Veränderung. Auf allen Ebenen.

Ausgewählte Erkenntnisse dieser theoretischen und praktischen Forschungsarbeiten stellen wir in Form von Publikationen und Fachvorträgen einer breiteren Öffentlichkeit zur Verfügung.

asquared GmbH


Pappelallee 78/79


10437 Berlin - Deutschland

Telefon +49 (0) 30 22 66 79 60


E-Mail contact@asquared.team

 asquared.company

 asquared.blog

 twitter.com/asquaredgmbh

 [instagram.com/asquaredgmbh](https://www.instagram.com/asquaredgmbh)

 [linkedin.com/company/asquared](https://www.linkedin.com/company/asquared)