Bankstil

Identity Economy

Identity-Ökosysteme in Deutschland

(Studie)

Autor: Ralf Keuper (Bankstil / Identity Economy)

Mai 2019

Inhalt

Zusammenfassung

Digitale Identitäten für Personen, Geräte und Unternehmen sind dabei, Wirtschaft und Gesellschaft zu transformieren. In einigen Regionen, wie in Skandinavien, ist diese Entwicklung bereits weit fortgeschritten. In Deutschland dagegen fehlt es an Lösungen, die aus dem Stand eine kritische Größe erreichen. Es überwiegen die Versuche, die alte Deutschland AG in das digitale Zeitalter zu überführen. Der Staat agiert hierzulande, anders als in Estland, zurückhaltend. Die Bankengruppen sind derweil damit beschäftigt, eigene Standards für digitale Identitäten zu etablieren. Auch der Handel ebenso wie die Medienunternehmen versuchen sich in Alleingängen. Die Industrie hat den Handlungsbedarf erkannt und bereits erste gemeinsame Initiativen gestartet. Die Aussichten, dass eine der Lösungen die kritische Größe erreicht, schwinden indes mit jeder weiteren Allianz[1].

Die Identity-Ökosysteme in Deutschland sind - bis zu einem bestimmten Grad - ein Abbild der geschilderten Gemengelage. Jedoch hat sich hier eine Dynamik entwickelt, die darauf hoffen lässt, dass daraus vitale und überlebensfähige Ökosysteme entstehen, die in der Lage sind, die für die Wirtschaft und Gesellschaft nötigen Lösungen bereitzustellen. Sie repräsentieren darüber hinaus einen Wissenspool, der landesspezifische und internationale Entwicklungen, sei es auf technologischem oder regulatorischem Gebiet, aufnehmen und verarbeiten kann. Ermöglicht wird das durch das Zusammenspiel von standortspezifischem Wissen, Identity-Startups, IT-Sicherheitsunternehmen, Investoren und wissenschaftlichen Einrichtungen.

Angesichts der alten und neuen Akteure, die in das Geschäft mit den digitalen Identitäten drängen, stehen die deutsche und europäische Wirtschaft vor der Herausforderung, die Spielregeln der Plattformökonomie zu adaptieren und für sich zu nutzen. Das wiederum wird ohne ein Mindestmaß an branchenübergreifenden Kooperationen, Interoperabilität der Lösungen und ohne Einigung auf Standards kaum gelingen. In diesen Prozess sind die Identity-Ökosysteme als Impulsgeber fest eingebunden. Auch hier kommt es darauf an, den Wissens- und Erfahrungsaustausch der Identity-Ökosysteme, sowohl auf nationaler wie auch auf internationaler Ebene zu vertiefen und zu verstetigen.

In den nächsten Jahren werden wir sehen, wie sich einstmals getrennt voneinander agierende Branchen weiter annähern und unter dem Dach großer Digitaler Ökosysteme wie Apple oder Google vereint werden. Digitale Identitäten, u.a. in Kombination mit internationalen Zahlungssystemen, werden dabei eine Schlüsselrolle übernehmen. Vitale und vielfältige Identity-Ökosysteme, sog. Diamanten (Michael E. Porter), sind für die deutsche und europäische Volkswirtschaft unabdingbar. Diese Notwendigkeit zu verdeutlichen und Chancen aufzuzeigen, sind Ziele der vorliegenden Studie.

[1] Vgl. dazu: Die deutsche Wirtschaft versaut sich mit Uneinigkeit die Chance auf einen eigenen Universal- Login

Einleitung

In Deutschland, wie in vielen anderen Ländern auch, hat das Thema Digitale Identität in den letzten Jahren an Bedeutung gewonnen. Das lässt sich u.a. an den Login-Allianzen belegen, die 2018 an den Start gegangen sind, wie Verimi, netID und ID4me. Seitdem wird in der Öffentlichkeit intensiv über den Nutzen digitaler Identitäten für Bürger, Kunden und Unternehmen diskutiert. Das umso mehr, als unter den Nutzern die Sorge wächst, die Internetkonzerne wie Facebook und Google könnten nicht so verantwortungsvoll mit ihren Daten umgehen, wie es eigentlich geboten wäre.

Die Verlags- und Werbeindustrie befürchtet, von Facebook und Google, die schon jetzt den Markt für online-Werbung dominieren, noch abhängiger und aus dem Geschäft gedrängt zu werden. Die Industrie, der Handel und der Mittelstand beobachten die Entwicklung ebenfalls mit gemischten Gefühlen. Sollte sich im B2B-Sektor wiederholen, was bereits im B2C-Bereich durch die Social-Logins von Facebook und Google eingetreten ist, dann droht auch hier der Verlust der Kundenschnittstelle. Die Erkenntnis greift um sich, dass eine Wirtschafts- und Exportnation wie Deutschland mit seinem starken industriellen Kern zur verlängerten Werkbank werden könnte. Sichere Digitale Identitäten für Maschinen und Geräte sind der Schlüssel, um als Produktions- und Forschungsstandort weiterhin relevant zu bleiben. Der Handel und die Banken sind besonders gefährdet, da sich die Kundenschnittstelle bzw. die digitalen Kontrollpunkte im Internet bereits weitgehend in den Händen von Google, Amazon, Apple und Alibaba befinden.

Abgerundet wird die Strategie der großen digitalen Plattformen und Ökosysteme durch online Bezahlverfahren (Google Pay, Apple Pay, Alipay, Amazon Pay) und, wie im Fall von Google und Apple, durch abgeleitete digitale Identitäten auf dem Smartphone[2]. Das lässt irgendwann kaum noch Platz für andere Anbieter.

Daraus wird deutlich, dass sich der Wirkungsgrad digitaler Identitäten nicht auf Lösungen für Personen beschränkt, sondern volkswirtschaftliche Dimensionen hat. Ohne Übertreibung lassen sich Digitale Identitäten daher als die Dampfmaschinen der digitalen Ökonomie bezeichnen[3].

In dem Report *Identity in a Digital World A new chapter in the social contract*[4] hebt das World Economic Forum die Bedeutung Digitaler Identitäten für die Wirtschaft und Gesellschaft hervor:

> *For businesses, verifiable identities create new markets and business lines, better customer experiences, improved data and a tool against fraud.*

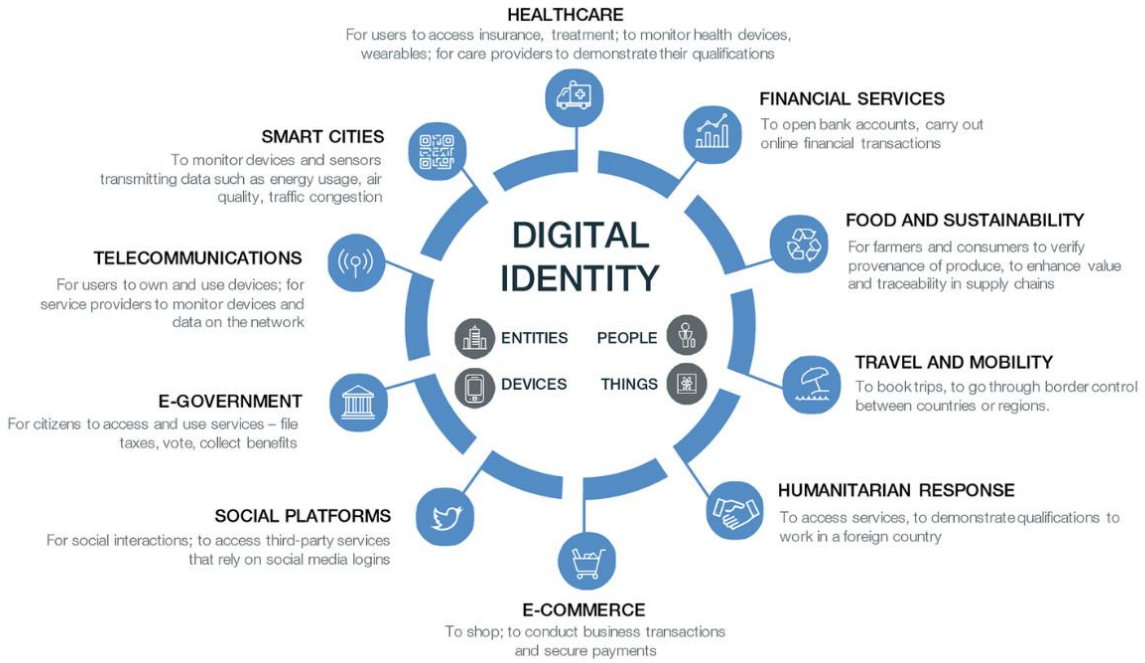
[2] Apple strebt nach der Vormachtstellung bei der digitalen Identifizierung

[3] Identity is the Steam Engine of the Digital Economy

[4] Identity in a Digital World A new chapter in the social contract

For governments, they offer a new way of governing: better delivery of services, a more engaged citizenry and a tool against corruption and crime. For individuals, they open up (or close off) the digital world, with its jobs, political activities, education, financial services, healthcare and more.

Das Zusammenspiel der verschiedenen Bereiche, die mittels Digitaler Identitäten erschlossen, vernetzt oder erweitert werden können, veranschaulich die folgende Grafik:



Identity in everyday lives. Quelle: WEF

Umso wichtiger ist es für eine Wirtschafts-, Forschungs- und Kulturnation wie Deutschland daher, auf diesem zukunftsträchtigen Gebiet über funktionierende Infrastrukturen/Ökosysteme sowie Unternehmen zu verfügen, die in der Lage sind, die Probleme der Kunden zu erkennen und zu lösen. Bislang hat sich in Deutschland noch keine Identifizierungslösung am Markt durchgesetzt, die einen ähnlichen Verbreitungsgrad erreicht hätte wie die BankID in Norwegen und Schweden. In Deutschland beschränkt sich der Staat weitestgehend darauf, mit dem neuen Personalausweis und der eID die weltweit sicherste Lösung entwickelt zu haben. Trotz überlegenem Sicherheitsniveau halten sich die Bürger bei der Verwendung des neuen Personalausweises zum Zweck der digitalen Identifizierung noch zurück. Die Zahl der Anwendungsfälle im Banking nimmt indes zu[5]. Im Bankenumfeld haben sich für das digitale Onboarding der Kunden die Video-Ident-Verfahren etabliert. Ob und wie lange diese von vielen als "vorübergehende Brückentechnologie" bezeichnete Variante vom Regulator, aber auch von den Banken und Kunden, noch akzeptiert

[5] Sparkasse stellt automatisierte Kundenidentifikation über den Personalausweis vor

wird, bleibt abzuwarten. Die Anbieter von Video-Ident-Verfahren wie IDnow bieten bereits Lösungen an, welche die Verfahren der Künstlichen Intelligenz mit biometrischen Merkmalen kombinieren.

Ein internationaler Trend, der sich noch verstärken dürfte und über kurz oder lang vor Deutschland nicht Halt machen wird.

Wie bereits in der Studie Die Fintech-Startup-Ökosysteme in Deutschland praktiziert, wird auch die vorliegende Arbeit das Identity Ökosystem aus verschiedenen Perspektiven beleuchten. Untersuchungsgegenstand sind die Identity Hubs in Deutschland mit ihrem regionalen Ökosystem, bestehend aus Unternehmen/Startups, IT-Sicherheitskonzernen, Events, Wissenschaftlichen Einrichtungen/Projekten, Verbänden und Investoren/Acceleratoren.

Folgende Fragen werden dabei leitend sein:

- Wie kommt es, dass sich viele Identity-Startups und Unternehmen in Metropolen wie Berlin, München und Frankfurt angesiedelt haben, aber auch in Gelsenkirchen/Bochum, Kiel und Darmstadt, wogegen Hamburg kaum ins Gewicht fällt?
- Welche Zutaten, Komponenten sind nötig, damit ein Identity-Ökosystem auf Mitarbeiter, Forscher und Investoren eine hohe Anziehungskraft ausübt?
- Wie lassen sich der Erfolg und die Zukunftsfähigkeit eines Identity-Ökosystems einigermaßen sicher bewerten (Anzahl der Unternehmen, Patente, Forschungsprojekte, Anzahl an Investments/Beteiligungen)?

Deutschland, das ist eine der zentralen Aussagen, ist mit 30 Startups (Bundesdruckerei, G+D sowie andere etablierte Unternehmen aus dem Umfeld nicht mit gezählt), die sich ausschließlich dem Thema Identifizierung/Authentifizierung widmen, schon jetzt ausgesprochen vielfältig[6]. Das gilt auch für die untersuchten Identity-Ökosysteme, die einen ähnlichen Reifegrad erreicht haben, wie die Fintech-Startup-Ökosysteme vor fünf Jahren. Die enge Verbindung mit Cybersecurity, Dokumentenmanagement, Payments, Signaturen, IoT, Blockchain, Künstlicher Intelligenz, Biometrie sowie ihr branchenübergreifender Charakter werden dafür sorgen, dass die Identity-Ökosysteme langlebiger sein werden, als die Fintech-Startup-Ökosysteme.

[6] Die Identity-Startups in Deutschland (Schaubild)

Definition der wichtigsten Begriffe

Ökosystem (Frederic Vester)

An Definitionen, was unter einem Ökosystem zu verstehen ist, mangelt es zwar nicht, jedoch bringen nur wenige die Sache so auf den Punkt, wie die von Frederic Vester:

Die Gesamtheit einer Lebensgemeinschaft (Biozönose) zusammen mit ihrer Umwelt, in der sie integriert ist und mit der sie zu einem überlebensfähigen System organisiert ist, wird .. als Ökosystem bezeichnet[7].

Definition Identity – Ökosystem

Ein Startup bzw. noch relativ junges Unternehmen mit dem Schwerpunkt auf Lösungen für die digitale Identifizierung/Authentifizierung ist Bestandteil einer urbanen Lebensgemeinschaft, womit nicht zwangsläufig Metropolen gemeint sind. Diese Lebensgemeinschaft setzt sich u.a. zusammen aus Investoren, anderen Startups und einem (formellen und informellen) Netz aus verschiedenen Veranstaltungen zum gegenseitigen Kennenlernen.

Zur näheren Umwelt zählen Universitäten und Institute, die für die Versorgung mit frischen Ideen (Ideenräume) und neuen Mitarbeitern (Begabungspool) von großer Bedeutung sind. Weiterhin gehören dazu auch die Kommunen mit ihren verschiedenen Angeboten und Initiativen im Bereich der Existenzgründung und Wirtschaftsförderung. Ebenso lassen sich hier Unternehmen, insbesondere aus den Bereichen Telekommunikation, Chipkarten, IT-Sicherheit und Verteidigung einordnen. Weniger von Bedeutung ist die unmittelbare räumliche Nähe zu Beratern (Wirtschaftsprüfer, Anwälte, Unternehmensberater, Analysten, Journalisten/Blogger) und staatlichen Institutionen und Verbänden, die mit dem Ökosystem häufig von Fall zu Fall interagieren.

In der Summe bilden die verschiedenen Elemente ein überlebensfähiges System – ein Identity - Ökosystem.

Definition Identifizierung, Authentisierung, Authentifizierung, Autorisierung

Identifizierung:

Um die Identität einer natürlichen Person zweifelsfrei festzustellen, geben Staaten entsprechende Ausweisdokumente aus. In Deutschland ist das der neue Personalausweis. Bis vor wenigen Jahren war hierfür die Anwesenheit der ausweisenden Person und der überprüfenden Person/Instanz im selben Raum oder in unmittelbarer Nähe nötig. Mit der Einführung des Video-Ident-Verfahrens wurde die Anwesenheitspflicht wie z.B. bei der Eröffnung eines Bankkontos überflüssig. Per Video-Verbindung weist sich der Antragsteller gegenüber der prüfenden Person mit seinem Personalausweis aus, den er vor der Kamera in verschiedenen Positionen schwenken muss, ebenso wie seinen Kopf. In dem Zusammenhang spricht man auch von verifizierten Identitäten.

[7] Leitmotiv vernetztes Denken

Bei der Authentisierung legt die Person ein Dokument vor, das ihre Identität bestätigt, wie durch Vorlage eines Personalausweises. Es existieren drei Möglichkeiten für eine Person, die eigene Identität zu behaupten:[8]

- sie hat geheime Informationen, die nur ihr bekannt sind (z.B. Passwort)
- sie besitzt einen Identifizierungsgegenstand (z.B. Personalausweis)
- sie ist selbst das Identifizierungsobjekt (z.B. biometrische Merkmale wie Fingerabdruck).

Bei der Authentifizierung erfolgt der Nachweis bestimmter, behaupteter Eigenschaften einer Person, eines Gegenstandes oder Gerätes.

Die Autorisierung räumt einer Person, welche die Schritte Authentisierung und Authentifizierung erfolgreich absolviert hat, bestimmte Rechte ein.

Zusammenfassend können alle drei Begriffe anhand eines EDV-Systems wie folgt verdeutlicht werden:

1. **Authentisierung:**
   Eingabe von Login-Daten in einem EDV-System (Behauptung einer Identität)
2. **Authentifizierung:**
   Überprüfung der Behauptung durch das EDV-Systems inkl. Ergebnis der Prüfung (Verifizierung der Behauptung aus 1.)
3. **Autorisierung:**
   Prüfung der Rechte und Konsequenz (Einräumung oder Verweigerung von Rechten).

Social Login

Die schwächste Form der Identifizierung ist das sog. Social Login, wie es von Facebook (Facebook-Connect) und Google (Gmail) angeboten wird. Hierbei können sich die Nutzer mit ihrem Gmail-Account bei verschiedenen Seiten im Internet, wie beim E-Commerce, anmelden, ohne dafür extra ein separates Formular ausfüllen und ein Passwort anlegen zu müssen. Die Einsatzmöglichkeiten des Social Logins sind jedoch begrenzt. So sind Banken im Zuge des "Know Your Customer" (KYC-)Prozesses dazu verpflichtet, die Identität ihrer Benutzer genau zu überprüfen. Auf diese Weise soll sichergestellt werden, dass Banken nicht für Geldwäsche missbraucht werden. Dazu gehören die Überprüfung von Ausweisdokumenten und eine Risikobeurteilung von Personen bezüglich Betrugsverhalten.

Obwohl beispielsweise Facebook eine Klarnamenspflicht in den AGB festhält und diese auch teilweise durchzusetzen versucht, reicht die Qualität der gelieferten Identitäten nicht für vertragliche Beziehungen. Reine Online-Shops können diese Probleme umgehen, indem sie Bestellungen per Vorkasse oder

[8] Authentisierung, Authentifizierung und Autorisierung

Kreditkartenbelastungen abrechnen. Die Überprüfung der Identität wird bei Kreditkarten an den Kartenaussteller ausgelagert [9].

Methodisches Vorgehen

Ein Identity-Ökosystem im Sinne der vorliegenden Studie setzt sich aus folgenden Elementen zusammen:

- Startups / Junge Unternehmen
- Unternehmen / Konzerne aus der Bereichen IT-Sicherheit
- Investoren/Acceleratoren/Inkubatoren
- Events/Netzwerktreffen
- Wissenschaftliche Einrichtungen/Forschungsprojekte

Hinweis:

Die vorliegende Studie erhebt keinen Anspruch auf Vollständigkeit. Als Informationsgrundlage dient u.a. die auf dem Blog Identity Economy, wie in den Wochenrückblicken, dokumentierten Meldungen sowie die dort veröffentlichen Analysen. Weitere Quellen sind persönliche Gespräche wie auch Interviews der letzten Jahre mit den diversen Akteuren in der deutschen Identity-Szene. Abgerundet wird das Bild durch die Beschäftigung mit den diversen Studien und Veröffentlichungen auf dem Gebiet Cybersecurity/Identity. Wenngleich die Studie keine Vollständigkeit anstrebt und auch nicht anstreben kann, so besteht das Ziel dennoch darin, ein möglichst vollständiges und kohärentes Bild zu zeichnen.

Die Methodik folgt einerseits den Prinzipien der evidenzbasierten Wissenschaft, d.h. die Hypothesen werden anhand der Anzahl stützender Belege geprüft, um daraus vorläufige Schlussfolgerungen ableiten zu können[10]. Auf der anderen Seite werden Analogien dazu verwendet, Ähnlichkeiten mit anderen Bereich, die nicht sofort auf der Hand liegen, herauszustreichen, um im Anschluss daran zu prüfen, inwieweit sich die Erkenntnisse/Muster der einen Domäne auf die andere übertragen lassen[11].

Standorttheoretische und wirtschaftshistorische Einordnung

Während die klassischen Standorttheorien, wie die von Alfred Weber, Walter Christaller und Johann Heinrich von Thünen, räumlichen Distanzen und damit Transportkosten eine hohe Bedeutung bei der Wahl eines Standortes einräumten, stellen neuere Ansätze eher weiche Faktoren, wie das kulturelle Umfeld - häufig auch als Lebensqualität bezeichnet - in den Vordergrund. Beispielhaft dafür ist Richard Florida mit den drei T's - Talente, Technologie und Toleranz[12].

[9] Wo bleibt der Siegeszug von Social Login?

[10] Vgl. dazu: Heureka - Evidenzkriterien in den Wissenschaften. Ein Kompendium für den interdisziplinären Gebrauch

[11] Die Analogie. Herz des Denkens

[12] The Rise of the Creative Class

Für die flächendeckende Verbreitung technologischer Innovationen hat sich der Begriff der Spillover-Effekte etabliert. Robert K. von Weizsäcker und Martin Steininger haben diesen Effekt in ihrem Beitrag *Profilbildung und regionale Standortstrategie durch Wissen. Das Beispiel der Technischen Universität München*[13] näher untersucht. Darin formulieren sie am Beispiel der Region München die These, dass räumlich begrenzte Wachstumsimpulse u.a. das Ergebnis einer strategischen Akkumulation regionalen Humankapitals sind, d.h. es existiert ein standortgebundenes (implizites) Wissen. Dieses Wissen ist nicht ohne weiteres auf andere Standorte übertragbar bzw. nicht imitierbar. Das trifft in besonderer Weise auf die Identity-Startups zu, die ihren Erfolg in weiten Teilen dem standortgebundenen Wissen verdanken.

Wie kein anderer Autor hat Michael E. Porter die Standorttheorie in den letzten Jahrzehnten beeinflusst und mit seinen Arbeiten voran gebracht. In seinem Buch *Nationale Wettbewerbsvorteile* hebt Porter die erfolgskritische Bedeutung des jeweiligen Heimatmarkes und der Region für Unternehmen hervor. Das Zusammenspiel verschiedener Faktoren (Humanvermögen, Materielle Ressourcen, Wissensressourcen, Kapitalressourcen, Infrastruktur) ist es, das einen Standort für Branchen besonders attraktiv macht. In dem Zusammenhang wählt Porter den bildhaften Ausdruck "Diamant".

> *Der "Diamant" ist ein sich wechselseitiges verstärkendes System. Die Wirkung des einen Bestimmungsfaktors hängt vom Zustand der anderen ab. Günstige Nachfragebedingungen z.B. ergeben keinen Wettbewerbsvorteil, wenn der Konkurrenzzustand nicht ausreicht, die Unternehmen zu einer Reaktion darauf zu veranlassen. Vorteile bei einem Bestimmungsfaktor können auch Vorteile bei anderen hervorrufen oder sie aufwerten.*

Jedes der hier untersuchten Ökosysteme kann für sich - wenngleich in unterschiedlicher Ausprägung - den Status eines "Diamanten" nach Porter für sich beanspruchen. Ebenso lässt sich festhalten, dass Spillover-Effekte, wie sie von von Weizsäcker und Steininger beschrieben wurden, für die hier analysierten Ökosysteme relevant sind.

Das erklärt auch, warum ein Standort wie Kiel für Identity-Startups und Unternehmen ein geeignetes Umfeld bietet. Dort und in der näheren Umgebung (Flintbek) hat sich über Jahrzehnte ein Wissen in den Bereichen (Marine-)Kommunikation und Smart Card angesammelt, das nun in neue Anwendungen wie die Gesundheitskarte/eID und Video-Identverfahren übertragen werden kann. Wo dieses Humankapital und Erfahrungswissen fehlen, kann auch ein urbanes Umfeld, das bezogen auf Deutschland höchsten Ansprüchen genügt, wie in Hamburg oder Köln/Düsseldorf, dieses Defizit nicht ausgleichen.

Das unterscheidet die Startups und Unternehmen aus dem Identity-Umfeld von Fintech- und Blockchain-Startups.

[13] Profilbildung und regionale Standortstrategie durch Wissen Das Beispiel der Technischen Universität München

Pfadabhängigkeiten

Problematisch wird die Ansammlung von Wissen und Unternehmen, die an einem Ort in dem gleichen Sektor tätig sind, dann, wenn die Umwelt sich in einer Geschwindigkeit verändert, die ein rasches Handeln und eine neue strategische Ausrichtung erfordern. Die bereits erwähnten von Weizsäcker und Steininger sprechen in dem Zusammenhang auch von der *Eigentorthese des impliziten Wissens*[14].

Sichtbar wird das in Deutschland generell an der Fixierung auf hardware-spezifische Aspekte und die Betonung des Berufsbildes des Ingenieurs. Der Glaube ist noch immer weit verbreitet, dass das beste und qualitativ hochwertigste Produkt die Käufer überzeugt[15]. Diese Einstellung hat mit dazu geführt, dass Deutschland über die Jahre den Anschluss in vielen Wirtschaftszweigen, wie der Herstellung von Mobiltelefonen und Personal Computern, verloren hat. In der Plattformökonomie spielen deutsche wie überhaupt europäische Unternehmen keine nennenswerte Rolle. Es scheint den deutschen Ingenieuren nicht zu gelingen, mittels Software die informationsintensiven Produkte und Services nutzerfreundlich zu gestalten[16]. Dadurch wird die Kundenschnittstelle immer häufiger von Unternehmen wie Apple, Google, Amazon und Alibaba übernommen, die auf ihren Plattformen verschiedene Produkte und Services anbieten können. Ob die Zukunft der deutschen Wirtschaft im B2B-Geschäft, in der Systemintegration und der dezentralen KI liegt, und ob dieses Geschäftsmodell ausreicht, bleibt abzuwarten[17].

Auch der Bereich Identity/Cybersecurity weist ähnliche Defizite auf. Es überwiegt die Fixierung auf technologische Fragen, die Optimierung bestehender Verfahren und Sicherheitsaspekte. Es scheint so, als dass deutsche technologische Innovationen erst über den Umweg USA für die deutschen Verbraucher und Unternehmen wieder interessant werden. Bislang ist es nicht gelungen, den Medienträger Smartcard durch eine virtuelle Alternative zu ersetzen[18]. Das ist einer der Gründe für die geringe Akzeptanz des neuen Personalausweises. Neueste Bestrebungen, wie im Projekt Optimos 2.0, weisen zumindest in die richtige Richtung.

Es soll nicht verschwiegen werden, dass „Security Made in Germany“, wie im Fall G-Data, ein wichtiges Alleinstellungsmerkmal sein kann.

[14] Wobei hier hinzugefügt werden muss, dass im Zusammenhang mit der vorliegenden Untersuchung das Explizite Wissen von ebenso großer Bedeutung ist.

[15] Vgl. dazu: German 'Digitalisierung' versus American innovation

[16] Vgl. dazu: “Wir brauchen einen Ruck durch Politik, Forschung, Unternehmen und Gesellschaft” – Interview mit Prof. Dr. August-Wilhelm Scheer

[17] Vgl. dazu: Deutsche Industrie benötigt gemeinsam betriebene Datenaustauschplattformen

[18] Vgl. dazu: Das Smartphone als virtuelle Smartcard

Die Identity-Ökosysteme

Die Identity-Ökosysteme in Deutschland unterscheiden sich derzeit in der Ausprägung der jeweiligen Komponenten. In einigen Fällen fehlen einzelne Komponenten, wie in Kiel in Form örtlicher Investoren und fester Veranstaltungen mit Bezug zum Themenkomplex Cybersecurity/Identity. Fehlen mehrere dieser Komponenten oder sind die vorhandenen noch zu schwach ausgeprägt, wie im Fall von Saarbrücken und Bonn, werden diese Ökosysteme (noch) nicht berücksichtigt.

Identity-Ökosystem Berlin

Startups

Startup	Geschäftsmodell	Technologie	Zielkunden	Verifizierte Identitäten
Jolocom	Self Sovereign Identity (SSI), Identity Claim Verification	Blockchain/Sovrin	Endkunden	Ja
WebID Solutions	B2B(2C), KYC	Video-Ident, KI	Banken, Versicherungen	Ja
Authenteq	B2B2C, KYC	Blockchain, Biometrie, Künstliche Intelligenz		Ja
Taqanu	B2B2C, KYC	Blockchain (public), Attestation Network (Abacus Fabric), Mobile Application	Banken, Versicherungen, Öffentliche Verwaltungen, Soziale Einrichtungen	Ja
YPTOKEY	B2B2C	Blockchain, Mobile Application, Marketplace, Ecosystem for cross-industry collaboration and co-innovation	Unternehmen, Banken, Handel	Nein
Spherity	B2B2C	Digital Twins, Agent Technology, Ocean Protocol, SSI	Industrie / IoT	
Verimi	B2B2C, KYC, SSO	Cloud, Kryptografie, WebID Solutions, Nexus, Signicat	Unternehmen, Banken, Handel, Öffentliche Verwaltungen	Ja
ID.Berlin	Bürger Berlins / SSO	E-Mail – Account, Passwort	Öffentliche Verwaltung	Nein

			Berlin und 100 deutsche Internetportale	

Unternehmen/Konzerne im Bereich IT-Sicherheit/Cybersecurity

Unternehmen	Kernkompetenz	Technologie	Zielkunden
Bundesdruckerei	Sichere Identitäten und sichere Digitalisierung	Smart Card, eID, IDChain, Mobile ID/Optimos 2.0/ Mobile BügerID, Trust Center	Banken, Versicherungen, Öffentliche Verwaltungen
Nexus	Sichere Digitale Identitäten für die Industrie	PKI, RFID-Karten, OTP-Token, Mobile IDs	Industrie / IoT
gematik	IT-Dienstleistungsunternehmen im Gesundheitswesen	Telematik, Elektronische Patientenakte	Gesundheitssektor

Veranstaltungen/Events mit Bezug zum Thema Identifizierung

Ausrichter	Veranstaltung
DWeb Berlin (Meetup)	Your decentralized identity
Auth Heroes Berlin (Meetup)	
Omnisecure	
The Blockchain for Social Good Berlin	Blockchain for Good – Digital Identity
European Commission	Cyber Investor Days
Private Gruppe (Meetup)	Cyber Security Berlin

Investoren/Acceleratoren/Inkubatoren mit Aktivitäten im Bereich Identifizierung

Name	Schwerpunkt	Beteiligungen
Bundesdruckerei	Cybersecurity	Dermalog, Cryptovision
Finleap	Cybersecurity	Perseus
inQventures (adesso AG)	Cybersecurity	

Verbände und Interessenvertretungen mit Bezug zum Thema Identifizierung

Name	Aufgabenspektrum
Bundesblock	Verbreitung der Blockchain-Technologie in Deutschland
Bitkom	Interessenvertretung der deutschen IKT-Branche
Sichere Digitale Identität Berlin Brandenburg (Verein)	Information der Öffentlichkeit und Beratung von Politik und Wirtschaft
Unternehmensnetzwerk Cybersecurity	Standortinitiative

Wissenschaftliche Einrichtungen und Forschungsprojekte mit dem Schwerpunkt Identity/Cybersecurity

Name	Forschungsschwerpunkt/Projekte
Optimos 2.0	Entwicklung einer offenen, praxistauglichen Infrastruktur für mobile Services auf Basis der eID (abgeleitete Mobile ID)
Fraunhofer FOKUS	Innovationscluster „Next Generation ID“
	Digitale Identitäten in der Blockchain. Erfahrungen aus der Entwicklung
	Digitale Identitäten und Cybersecurity
FU Berlin / Fraunhofer AIESEC	Stiftungslehrstuhl für elektronische Identitäten
Hasso-Plattner-Institut	HPI Identity Leak Checker
	Secure Identity Lab
Mobile selbstverwaltete Bürgeridentität auf Basis einer Blockchain-Bürgeridentität	Im Projekt soll eine mobile Bürgeridentität auf Basis einer Blockchain für vier Anwendungsfälle im Mobilitätsbereich erstellt werden. Sie basiert auf dem internationalen Standard Decentralized Identifiers (DID) und ist damit eine Self Sovereign Identity.

Identity-Ökosystem München

Startups

Name	Geschäftsmodell	Technologie	Zielkunden/ Zielmarkt	Verifizierte Digitale Identitäten
IDnow	B2B2C	Video-Ident, Künstliche Intelligenz, Biometrie	Banken, Versicherungen	Ja
IDEE	B2B2C	QR, Künstliche Intelligenz, Forensic, Blockchain	Handel/Retail, Banken, Mobility	Nein
keyp	B2B	Keyp Identity Framework (Keyp Identity Terminal, Keyp Marketplace, Keyp Wallet)	Öffentliche Verwaltung, Industrie, Handel, Finanzdienst-leistungen,	Ja
Rempartec	B2B	Smart Card, eSignature, one-time-passcode, Authentication Server, Displays, Cloud, Secure VPN, Secure SSH	Finanzdienst-leistungen, Industrie, Handel	Nein
Datarella (RAAY)		Blockchain, RAAY Operating System/Protocol, Tokenization	Banken, Finanzdienst-leistungen	Nein
re:claimID	B2B2C	GNU Name System (GNS), Attribute-based-Encryption (ABE),	Unternehmen und Endkunden	Nein

Unternehmen/Konzerne im Bereich IT-Sicherheit/Cybersecurity

Unter-nehmen	Kern-kompetenz	Technologie	Zielkunden
Giesecke + Devrient	Lösungen zur Absicherung von Bezahlvorgängen, Identitäten und Daten	Cybersecurity, Secure Elements (Bank Card, SIM Card, ID Card, M2M Module)	Banken, Versicherungen, Handel, Industrie, Öffentliche Verwaltung, IoT
Rhode & Schwarz	IT-Sicherheit	Cybersecurity, Funktechnik, Messtechnik, Medientechnik, Flugsicherungstechnik, Netzwerktechnik	Militär, Medien, Telkos, Unterhaltungselektronik, Netz-werkausrüstung, Industrie
Gemalto (Deutschland)	Authentifizierung, Identizierung, Datenschutz, Sichere Online-kommuni-kation	Smartchips, Biometrie, Server-Platform, Scanner	Militär, Telkos, Industrie, Banken, Versicherungen, Öffentliche Verwaltung, Gesundheit
ForgeRock (Deutschland)	Authentifizierung, Identitfi-zierung, Sichere Online-Kommunikation, Datenschutz		Banken, Öffentliche Verwaltung, Gesundheit, Handel, Medien, Telkos, IoT/Connected Cars
Klarna	Zahlungsdienstleistung, Authentifizierung, Finanzierung	API,	Händler, Endkunden
Exceet Card	Identifizierung, Authentifizierung	Smart Card	Handel, Banken, Versicherungen, Öffentliche Verwaltung, Industrie
Infineon	Halbleiterpro-duktion, Sensorik, Authentifizierung, Identifizierung	Smart Card, NFC	Industrie, Handel, Militär, Telkos, Banken, Öffentliche Verwaltungen/Staatliche Institutionen

Veranstaltungen/Events mit Bezug zum Thema Identifizierung

Ausrichter	Veranstaltung
Center Digitalisierung.Bayern	Tech Days Munich
Human-centered Data Management & Innovation Meetup	
TCP/ID – Decentralised Future of Identity Munich (Meetup)	
KuppingerCole	European Identity & Cloud Conference
Munich Identity Meetup	
Sicherheitsnetzwerk München	Munich Cyber Security Conference 2019

Verbände und Interessenvertretungen mit Bezug zum Thema Identifizierung

Name	Aufgabenspektrum
Sicherheitsnetzwerk München – Arbeitsgruppe Blockchain & ID-Federations	Bündelung der Kompetenzen und deren Sichtbarmachung, Anbahnung und Durchführung gemeinsamer F&E-Verbundvorhaben, Verbesserung der Rahmenbedingungen, Gestaltung technischer Standards und deren internationale Durchsetzung, Entwicklung des Fachkräftepotentials, Entwicklung von Außenbeziehungen

Investoren/Acceleratoren/Inkubatoren mit Aktivitäten im Bereich Identifizierung

Name	Schwerpunkt	Beteiligungen
G+D Ventures	Cybersecurity	IDnow
Bayerische Beteiligungsgesellschaft mbH (BayBG)	Cybersecurity	

Wissenschaftliche Einrichtungen und Forschungsprojekte mit dem Schwerpunkt Identity/Cybersecurity

Name	Forschungsschwerpunkt/Projekte
Fraunhofer AIESEC	re:claimID

Identity-Ökosystem Gelsenkirchen/Bochum/Essen

Startups

Name	Geschäfts-modell	Technologie	Zielkunden/ Zielmarkt	Verifizierte Digitale Identitäten
XignSys	B2B2C	e-Signature, QR, SSO, Dokumenten- und Workflowmanagement, Kryptografie	Handel,	Nein
Cryptovision	B2B2C	Smart Card, PKI, Digital Signature, Kryptografie, eID	Militär, Banken, Industrie, Handel	Nein
Idento.one	B2B2C	Blockchain, Kryptografie, Graphentechnologie	Banken, Industrie, Handel	Ja

Unternehmen/Konzerne im Bereich IT-Sicherheit/Cybersecurity

Unter-nehmen	Kern-kompetenz	Technologie	Zielkunden
G-Data	IT-Sicherheit	Kryptografie, Antivirus	Endkunden, Unternehmen
Rhode & Schwarz Cybersecurity GmbH	IT-Sicherheit	Cybersecurity, Funktechnik, Messtechnik, Medientechnik, Flugsicherungstechnik, Netzwerktechnik	Militär, Medien, Telkos, Unterhaltungselektronik, Netzwerkausrüstung, Industrie
Secunet AG	IT-Sicherheit	Kryptografie, Biometrie, Elektronische Signaturen	Handel, Industrie, Öffentliche Verwaltung, Verkehr/Logistik, Militär, IKT

escrypt	IT-Sicherheit	Kryptografie	Industrie, Smart City

Veranstaltungen/Events mit Bezug zum Thema Identifizierung

Ausrichter	Veranstaltung
istis AG International School of IT-Security	CYBICS 2019 (Digitalisierung meets Cyber Security)
Horst-Götz-Institut für IT-Sicherheit	ITS Connect – Jobmesse für IT-Sicherheit
Messe Essen	Security Essen
CUBE 5	Cybersecurity Founder Meetup

Investoren/Acceleratoren/Inkubatoren mit Aktivitäten im Bereich Identifizierung

Name	Schwerpunkt	Beteiligungen
Startup Secure: Inkubator für IT-Security in Bochum	Cybersecurity	
eCapital	Cybersecurity	eCapital plant für die nähere Zukunft, sich an Digital Identit-Startups zu beteiligten

Wissenschaftliche Einrichtungen und Forschungsprojekte mit dem Schwerpunkt Identity/Cybersecurity

Name	Forschungsschwerpunkt/Projekte
Max-Planck-Institut für Cybersicherheit	Cybersicherheit
Hort-Götz-Institut für IT-Sicherheit	Cybersicherheit
Institut für Internet-Sicherheit für mehr Vertrauenswürdigkeit und IT-Sicherheit	Blockchain, Vertrauenswürdige IT-Systeme, Zahlungssysteme und Banktransaktionen, Security for Smart Card, Smart Grids, Smart Traffic, Smart Home and Internet of Things
Exzellenzcluster CASA	Cybersicherheit, Interdisziplinäre Forschung (Technik und Psychologie)
Eurobits (Europäisches Kompetenzzentrum für IT-Sicherheit Bochum)	Cybersicherheit

Identity-Ökosystem Frankfurt/Darmstadt

Startups

Name	Geschäftsmodell	Technologie	Zielkunden/ Zielmarkt	Verifizierte Digitale Identitäten
Authada	B2B2C/KYC	eID, Kryptografie, Voice, Digital Signature/QES	Handel, Finanzdienstleister, Öffentliche Verwaltungen	Ja
Blockchain Helix	B2B2C/KYC	Blockchain, SSI	Handel, Finanzdienstleister, Telkos, Industrie	Ja
ChainID	Forschung/Prototyp (main incubator)	Blockchain, SSI	Finanzdienstleister	

Unternehmen/Konzerne im Bereich IT-Sicherheit/Cybersecurity

Unter-nehmen	Kern-kompetenz	Technologie	Zielkunden
Signicat	Digital Identity Provider	eID, Digital Signature, API	Finanzdienstleister, Öffentliche Verwaltung, Telkos, Automobilindustrie
Keyidentity	IAM	QR-Token, Push-Toklen	Banken, Versicherungen, Gesundheit, Industrie

Veranstaltungen/Events mit Bezug zum Thema Identifizierung

Ausrichter	Veranstaltung
Innopay	Wine and Identity
Digital Hub für Cybersecurity	Matchmaking

Investoren/Acceleratoren/Inkubatoren mit Aktivitäten im Bereich Identifizierung

Name	Schwerpunkt	Beteiligungen
main incubator	Fintech, Regtech,	Authada
FinLab AG	Fintech, Blockchain, Tokenization	Authada, Blockchain Helix

StartupSecure (Inkubator)	Cybersicherheit	
Hessian Israeli Partnership Accelerator (HIPA)	Cybersicherheit	

Wissenschaftliche Einrichtungen und Forschungsprojekte mit dem Schwerpunkt Identity/Cybersecurity

Name	Forschungsschwerpunkt/Projekte
Fraunhofer SIT	Cybersecurity, Identity and Privacy, IT Forensics
Digital Hub for Cybersecurity	Cybersecurity

Identity-Ökosystem Kiel

Startups

Name	Geschäftsmodell	Technologie	Zielkunden/ Zielmarkt	Verifizierte Digitale Identitäten
Coronic	B2B2C	Biometrie, Sprachsteuerung, Kryptografie	Banken	Nein
Hanko	B2B2C	Passwortlose Authentifizierung, Biometrie	E-Commerce, Banken, Gesundheit	Nein
WebID Solutions	B2B2C	Video-Ident, Künstliche Intelligenz, Biometrie	Banken, Versicherungen, Fintech-Startups	Ja

Unternehmen/Konzerne im Bereich IT-Sicherheit/Cybersecurity

Unternehmen	Kernkompetenz	Technologie	Zielkunden
Idemia	Augmented Identity	Self Sovereign Identity, Biometrie,	Finanzdienstleister, Telkos, Industrie, Öffentliche

		Smart Card, Selfie, QR	Verwaltungen
Hagenuk/ Thales	Sichere Kommunikation	Cybersicherheit	Militär, Industrie, Öffentliche Verwaltung, Finanzdienstleister, Handel
Ingenico Healthcare eID	Systemlösungen für die Gesundheitsbranche	Kartenlesegeräte, Terminals, eID	Gesundheitsbranche

Rohdiamanten und geschliffene Diamanten

Unter Verwendung der Metapher vom Diamanten nach Porter lassen sich für die hier untersuchten Identity-Ökosysteme folgende Schlussfolgerungen ziehen:

Die facettenreichsten Identity-Ökosysteme sind, so zumindest das Ergebnis dieser Untersuchung, das von Berlin, dicht gefolgt von München. In gewisser Weise können wir hier von geschliffenen Diamanten sprechen, die jedoch noch der Weiterbearbeitung bzw. des letzten Schliffs bedürfen. Berlin verfügt über die ausgewogenste Mischung aus Startups, Unternehmen, Investoren, Wissenschaftlichen Einrichtungen/Projekten, Veranstaltungen und Verbänden. Letzteres sicherlich auch aufgrund der Tatsache, dass Berlin als Regierungssitz als Standort für Verbände und Interessenorganisation besonders anziehend ist.

München besticht durch potente Unternehmen wie Giesecke + Devrient, Rhode & Schwarz und Infineon ebenso wie durch IDnow als einem der dynamischsten und wohl dem internationalsten Startup in Deutschland auf dem Gebiet der digitalen Identifizierung. Was ein wenig überrascht, ist die vergleichsweise geringe Anzahl an wissenschaftlichen Einrichtungen und Projekten in der bayerischen Landeshauptstadt.

Das Identity-Ökosystem mit dem umfangreichsten Angebot an wissenschaftlichen Einrichtungen ist zweifelsohne Bochum zusammen mit Gelsenkirchen und Essen. Beeindruckend ist auch die Zahl national führender Unternehmen aus der IT-Sicherheit wie G-Data, Rhode & Schwarz Cybersicherheit und escrypt. Nukleus des Ökosystems ist die Ruhr-Universität Bochum. Lücken bestehen im Bereich Veranstaltungen/Vernetzung sowie bei den Investoren. Kurzum: Bochum ist noch ein Rohdiamant, der jedoch nur wenig Schliff benötigt, um mit Berlin und München in etwa gleich ziehen zu können.

Etwas überraschend mag sein, dass der Raum Frankfurt/Darmstadt trotz seiner unbestreitbaren Wirtschaftskraft und hervorragenden Infrastruktur als Standort für ein Identity-Ökosystem relativ schwach ist. Die unmittelbare Nähe zu den Banken und Investoren, die herausragende Stellung von Darmstadt als Hub für Cybersicherheit hat sich - bislang jedenfalls - noch nicht als besonders fördernd für die Gründung von Startups sowie die Ansiedlung etablierter Unternehmen aus dem Umfeld

Identifizierung/Authentifizierung/Cybersicherheit herausgestellt. Ausnahmen sind Authada, Blockchain Helix und ChainID. Aus der Reihe der Investoren sind die FinLab AG und der main incubator zu nennen. Ein Rohdiamant, der noch einiger Bearbeitung bedarf.

Etwas unausgewogen ist das Faktorbündel in Kiel. Das ist sicherlich auch darauf zurückzuführen, dass die Unternehmen am Standort eher aus der Produktion und weniger aus der Forschung stammen, wie die damalige Orga Kartensysteme GmbH, deren F+E über Jahrzehnte in Paderborn angesiedelt war. Großen Einfluss hat die Verteidigungsindustrie mit Schwerpunkt Marine. Internationale Konzerne, die aus der Rüstungsindustrie stammen oder hier zumindest sehr aktiv sind, wie Thales, sehen den Standort Kiel eher als Produktionsstandort und Sprungbrett in den deutschen Markt. Ähnlich dürfte es sich mit Ingenico verhalten. Prägend für Kiel als einem der wichtigsten Ökosysteme für Identifizierung und Authentifizierung sind, wie bereits erwähnt, das Militär und die Gesundheitsbranche wie überhaupt die Smart Card. Also eher Hardware als Software (mit Ausnahmen wie WebID Solutions). Ein Rohdiamant mit Potenzial.

Erfolgskritische Standortbedingungen für Identity-Ökosysteme

Eine wichtige Erkenntnis der Wirtschaftsförderung der letzten Jahrzehnte ist, dass sich Standorte, die für technologie- und wissensintensive Branchen und Unternehmen attraktiv sind, nicht am Reißbrett entworfen und auch nicht durch einen kaum versiegenden Strom an Fördergeldern aus dem Boden gestampft werden können[19]. Bestimmte Voraussetzungen müssen bereits gegeben sein, wie eine gut ausbaute Wissenschaftslandschaft, gut ausgebildete Mitarbeiter, ein großer Nachfragemarkt und große Unternehmen, die einen Ring kleinerer Unternehmen an sich ziehen[20]. Erfolgskritisch ist ebenfalls der Wissenstransfer am Standort, der durch verschiedene Veranstaltungen und (gemeinsame) Forschungsprojekte begünstigt wird. Weiterhin ist es wichtig, dass die Unternehmen am Standort die Entwicklungen am Markt rechtzeitig antizipieren, was bedeuten kann, ganze Produktionszweige aufzugeben oder aber zumindest stark zurückzufahren, wie bei G+D, ohne dass dadurch das Ökosystem verödet.

[19] Vgl. dazu: Desaster um Cluster-Republik Deutschland

20 Vgl. dazu: How to Make a Region Innovative

Zersplitterter Markt in Deutschland und Europa

Der Markt für Cybersecurity und Identity in Deutschland und Europa ist fragmentiert. Im Gegensatz zu den USA oder Israel hat es bislang kein deutsches Unternehmen geschafft, in diesem Bereich weltweit Geltung zu erlangen[21].

> *Die Weltzentren für Cyber-Sicherheit liegen überall – nur nicht in Europa. Der Markt der Cybersicherheitsanbieter ist zerklüftet: Zwischen Einzelberatern, internationalen Großanbietern und mittelständischen Anbietern, die teils exzellente Technologien haben, aber unbekannt sind*[22].

Zu einem ähnlichen Befund gelangen das Fraunhofer Institut für Sichere Informationstechnologie in Darmstadt, das Max Planck-Institut für Softwaresysteme in Saarbrücken und das Karlsruher Institut für Technologie (KIT) in ihrem Positionspapier Cybersicherheit in Deutschland.

> *In Deutschland gibt es nur eine sehr kleine Zahl von in der Cybersicherheit auch international erfolgreicher Unternehmen. Dies ist besonders deutlich sichtbar, wenn man Deutschland z.B. mit Israel vergleicht: Deutschland hat grob zehnmal mehr Einwohner als Israel. Eine Studie von Cybersecurity Ventures verzeichnet unter den Top-500 Anbietern weltweit 25 aus Israel, davon 8 unter den Top-100, aber nur 11 aus Deutschland, davon keines unter den Top-100.*

Zu den wenigen Ausnahmen in Europa zählt der französische Thales-Konzern, der nach der abgeschlossenen Übernahme von Gemalto der weltweit größte Cybersecurity-Konzern ist[23].

Was das Marktpotenzial von Identifizierungslösungen betrifft, gehen aktuelle Schätzungen davon aus, dass sich das Marktvolumen von zuletzt 10 Mrd. Dollar bis zum Jahr 2023 auf 24 Mrd. Dollar erhöhen wird[24].

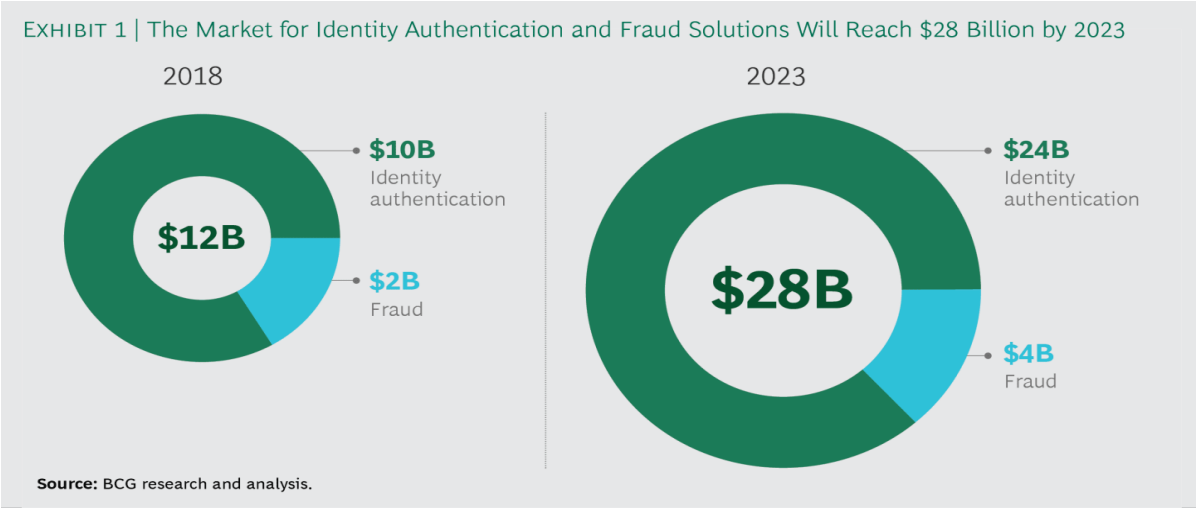
---

[21] Vgl. dazu: Warum Europas High-Tech-Konzerne weltweit hinterherhinken

[22] Vgl. dazu: Warum so viele Manager die Cybersicherheit lieber beiseite schieben, statt anzugehen, analysiert PwC-Profi Jörg Asma

[23] Vgl. dazu: Thales-Konzern: Ein echtes Schwergewicht im Markt für Digitale Identitäten

24 Vgl. dazu: A Great Digital Identity Solution Is One You Can't See



Die Rolle von Standards und Technologien – „Security Made in Germany" – Regulierung als Standortvorteil

Damit sich Lösungen, die einen bestimmten Kundenbedarf adressieren, durchsetzen können, reicht der Einsatz der neuesten Technologien nicht aus. Selbst eine perfekte Customer Journey ist nicht genug. Ohne entsprechende Infrastruktur und Standards bleibt der Erfolg, d.h. die Erreichung der kritischen Masse oder die Skalierung des Geschäftsmodells aus. Da hilft dann auch das beste Marketing wenig. In Deutschland haben wir das Phänomen, dass jede Branche versucht, ihre eigenen Standards mit mehr oder weniger proprietären Lösungen zu schaffen. Genannt seien die Entwicklungen im deutschen Bankenmarkt und in der Gesundheitsbranche. Anders als in Ländern wie Schweden, Norwegen und Estland, wo die Initiative von der Regierung und den dortigen Banken[25] und Telkos ausging, beschränkt sich der deutsche Staat auf die eID sowie auf die Förderung einzelner Projekte, die nur selten zusammenfinden. Ohne die Regulierung auf EU-Ebene, wie mit eIDAS und der Vision des Digitalen Binnenmarktes, sähe die Lage wohl noch schlechter aus. Ergebnis ist ein zersplitterter Markt mit vielen Anbietern und Lösungen, von denen aber nur sehr wenige die kritische Masse erreichen werden. Insofern wird schon recht bald, d.h. in 1-2 Jahren, ein Konsolidierungsprozess, wie derzeit bei den Fintech-Startups, einsetzen. Neue Anbieter wie Klarna und demnächst wohl auch PayPal, Mastercard, Visa und Apple werden den Druck auf die Identity-Startups noch erhöhen. In den Startlöchern stehen auch die diversen Kreditauskunfteien wie Crif und arvato/Infoscore. Lösungen, die nicht gleich schon zu Beginn zumindest den europäischen Markt im Visier haben, werden es sehr schwer haben.

Die Blockchain-Technologie bietet die Möglichkeit, selbstverwaltete digitale Identitäten zu verbreiten und/oder neuen Institutionen, wie Identity Banks, zum Durchbruch zu verhelfen. Damit rückt die Vision des *Internet of Me*[26] bzw. der *Me-*

[25] Banks have been the catalyst for Nordic digital identity success

[26] Internet of Me – The web itself is the only platform we need

Economy oder des *Be Your Own Bank* in greifbare Nähe. Deutschland und Europa sind überdies ein guter Nährboden für Lösungen aus dem Bereich der Selbstverwalteten Digitale Identitäten (SSI)[27], wie die Beispiele Jolocom, Blockchain Helix, ChainID, reclaim:ID und die ID-Chain zeigen. Großen Einfluss auf den Identity-Markt werden die Verfahren der Künstlichen Intelligenz und die Biometrie ausüben. Momentan gibt es Überlegungen zur Gründung einer Biometrie-Bank[28], die zunächst in den Entwicklungs- und Schwellenländern zur Bezahlung und Identifizierung, z.B. in Flüchtlings-Camps, zum Zuge kommen soll. Einer aktuellen Studie zur Folge, nehmen die Bedenken der Kunden bei dem Gebrauch biometrischer Lösungen ab[29].

Regulierung kann zu einem Standortvorteil werden. Das gilt in besonderer Weise für den Bereich Cybersecurity/Identity. Michael E. Porter stellt dazu fest:

> *Besonders vorteilhaft sind scharfe Regulierungen, die sich international ausbreitende Normen vorwegnehmen. Sie bringen den Unternehmen des Landes einen Vorteil bei der Entwicklung von Produkten und Dienstleistungen, die anderswo geschätzt werden. Soziale Belange, wie die Umwelt, die immer stärker differenzierende Faktoren auf den fortschrittlichen Märkten, und die Regulierung beeinflusst wiederum die Reaktion der Unternehmen eines Landes darauf.*

Unter Berücksichtigung der Diskussionen um den Schutz der personenbezogenen Daten, der steigenden Zahl von Identitätsdiebstählen und der Kontroverse um die Marktmacht der großen digitalen Plattformen wie Google und facebook[30] könnte man die Einführung der Datenschutzgrundverordnung wie auch die geplante ePrivacy-Richtlinie als Schritt in die richtige Richtung interpretieren. Der CEO von Apple, Tim Cook, jedenfalls empfiehlt seinem Land, sich die DSGVO zum Vorbild zu nehmen[31]. Insofern könnte „Security Made in Germany“ ein Verkaufsargument werden. In dem bereits erwähnten Positionspapier *Cybersicherheit in Deutschland* schreiben die Autoren:

> *Deutschland zeichnet sich durch Offenheit, Schutz von Menschenrechten und gesellschaftliche Stabilität aus – Eigenschaften, die Deutschland zum idealen Standort für Hochtechnologiefirmen und Arbeitsort für hochqualifizierte Mitarbeiter machen. Die Fortschreibung und Ausgestaltung der Cybersicherheitsstrategien brauchen feste, ressortübergreifende Strukturen.*

[27] Vgl. dau: EU-Bericht fordert dezentrale digitale Identitäten – Blockchain soll helfen

[28] Vgl. dazu: Eine Bank für "nackte Kunden"

[29] Vgl. dazu: Biometrische Authentifizierungsverfahren

[30] Sofern der Eindruck nicht täuscht, wird facebook seine eigene digitale Währung FaceCoin als Digitale Identität verwenden. Vgl. dazu: FaceCoin als Digital Identity – “Central Bank of Facebook”

[31] Vgl. dazu: Tim Cook calls for GDPR-style privacy laws in the US

Digitale Identitäten, Payments, Signaturen, Smart Contracts und Dokumentenmanagement bilden künftig eine Einheit

Die vernetzte Wirtschaft erfordert, dass Prozesse und Arbeitsschritte, die heute noch überwiegend manuell erledigt werden oder welche die Anwesenheit der beteiligten Personen erfordern, durch digitale Varianten ersetzt, zumindest aber ergänzt werden. Das wird über kurz oder lang zu einer Annäherung von Payments, Digitalen Identitäten, Qualifizierten Elektronischen Unterschriften und Dokumentenmanagement führen[32]. Hierfür wird häufig der Sammelbegriff *Digital Transaction Management* verwendet. In dem Zusammenhang weiterhin von Bedeutung ist die Robotic Process Automation. Sofern sich die Blockchain-Technologie durchsetzt, können Smart Contracts für die automatische Ausführung der verschiedenen Arbeitsschritte sorgen. Im Bereich Payments könnte mit der Etablierung eines europäischen Zahlungsnetzwerkes (Scheme), wie Bluecode, ein Gegengewicht zu Visa und Mastercard geschaffen werden, der es europäischen Identity-Startups ermöglicht, unabhängig(er) zu werden. Das gilt umso mehr, als Visa und Mastercard ihrerseits dabei sind, sich als Identity-Provider zu positionieren[33].

Geschäftsmodelle passen sich dem Heimatmarkt an

Momentan lassen sich die verschiedenen Geschäftsmodelle der Anbieter noch relativ genau voneinander abgrenzen. Abgesehen von dem gemeinsamen Nenner Sicherheit und Identifizierung/Authentifizierung, adressieren die Lösungen unterschiedliche Bedürfnisse. Dabei überwiegen die Anforderungen der Unternehmenskunden, wenngleich der Endkunde dabei im Blickfeld ist (B2B2C). Neben dem schnellen Onboarding neuer Kunden und einer stärkeren Kundenbindung spielt hier das Thema Betrugsprävention (KYC) eine große Rolle. Lösungen, welche überwiegend die Bedürfnisse der Nutzer adressieren, sind dagegen rar gesät. Sie kommen in der Regel aus dem Blockchain-Umfeld mit dem Schwerpunkt auf Selbstverwaltete Digitale Identitäten. Ein Sonderfall ist sicherlich der Rüstungssektor. Hier liegt der Fokus auf der Verhinderung von Cyberattacken auf Unternehmen und militärische Einrichtungen. Fast alle älteren Anbieter, die heute große Unternehmen sind, haben sich auf Umwegen dem Thema Digitale Identität genähert. Ein bislang noch relativ unbeackertes Feld, dafür wohl das mit dem größten Potenzial, ist das Internet der Dinge bzw. die Industrie 4.0 (Digitale Zwillinge). Hier gibt es bislang nur wenige Anbieter, die sichere digitale Identitäten für Maschinen und Geräte im Sortiment führen, wie Nexus. Der Bereich Industrie 4.0/Connected Cars könnte für deutsche oder europäische Anbieter von Identifizierungslösungen ein, womöglich der einzige Weg sein, um eine internationale Spitzenposition zu erreichen, was im Consumer-Geschäft auf direktem Weg nahezu

[32] Digitale Signaturen, Payment und Smart Contract gehen künftig zusammen

[33] Mastercard mit verbraucherzentriertem Modell für digitale Identitäten

unmöglich ist. Wie das Beispiel Israel mit seinen zahlreichen „Unicorns“ zeigt, ist ein großer Heimatmarkt nicht zwingend, um auch international Erfolg zu heben. Ohne Anbindung an ein dynamisches digitales Ökosystem (z.B. Automobilbranche, Industrie, Handel, Banking) werden es die Identity-Startups, jedenfalls diejenigen mit dem B2B2C-Ansatz, jedoch schwer haben die kritische Masse zu erreichen. Mobile abgeleitete Digitale Identitäten könnten für Startups, die sich direkt an die Endkunden wenden, der Schlüssel zum Erfolg sein. Gleiches gilt für selbstverwaltete Digitale Identitäten auf Blockchain-Basis. Hier könnte der Heimatmarkt Deutschland/Europa groß genug sein. Ein weiteres Gebiet mit Zukunftspotenzial sind Sichere Digitale Identitäten für Unternehmen bzw. für juristische Personen[34]. Noch in Kinderschuhen befinden sich die Geschäftsmodelle, deren Kern die Monetarisierung der Identitäts- und weiteren personenbezogenen Daten bildet. Jedenfalls zeichnet es sich ab, dass Daten einen Vermögensstatus erlangen, der ähnlich schutzbedürftig ist, wie heute die finanziellen Vermögenswerte. Nicht umsonst schreibt Dave Birch: Identity is he new money[35].

Die entscheidende Frage der nächsten Jahre wird sein, welcher Anbieter entweder eines der genannten Segmente als Marktführer erobern sogar alles aus einer Hand anbieten kann, wie es Thales bereits in Teilen verwirklicht hat. Gehört die Zukunft auch hier den Konzernen? Welche Rolle wird der Staat, die EU übernehmen?

Ohne Interoperabilität und Kooperationsbereitschaft wird es kaum gehen

Der Schlüssel für den Erfolg der verschiedenen Startups und Initiativen in Deutschland und Europa ist die Interoperabilität der Lösungen. Da ein Akteur allein kaum die nötige kritische Masse erreichen kann, empfiehlt es sich, die Lösungen so auszulegen, dass die Nutzer des einen Service ihre Daten auf einen anderen übertragen können. Abgesehen davon müssen die Nutzer sich mit ihrer ID problemlos auf den Seiten der Händler, Banken und Unternehmen anmelden können, d.h. es darf kein Zwang bestehen, ein bestimmtes Login-Verfahren zu verwenden. In der Studie *E-Identity-Lösungen in Europa – Ein europäischer Vergleich*[36] erwähnen Andreas Windisch und Andrea Müller als positives Beispiel für Kooperationen die skandinavischen Länder:

> *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*

[34] Vgl. dazu: Verifizierungen von Firmenkunden im EU-Binnenmarkt
[35] Identity is he New money
[36] Studie E-Identity-Lösungen in Europa – Ein europäischer Vergleich

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.

Davon sind wir hierzulande noch weit entfernt.

Die Kooperationsbereitschaft schließt natürlich auch die Identity-Ökosysteme in Deutschland mit ein. Sofern sich auch hier die Tendenz durchsetzt, sein „eigenes Ding" machen zu wollen und das Rad neu zu erfinden, wird die Unübersichtlichkeit und die Zersplitterung der Kräfte gefördert. Das hieße, den föderativen, dezentralen Ansatz, der Europa in der Vergangenheit so erfolgreich gemacht hat[37], zu überdehnen. Von Vorteil wären, wie bereits 2007 in *Elektronisches Identitätsmanagement. Mehr Einfachheit, Datenhoheit und Datensicherheit in unserer virtualisierten Welt*[38] gefordert, Leuchtturmanwendungen. Die Autoren sahen damals die Chance, der E-Perso könnte Katalysator für die flächendeckende Verbreitung weiterer ID-Lösungen mit entsprechenden Mehrwertdiensten sein. Mit Optimos 2.0 könnte dieser Wunsch in Erfüllung gehen.

Konsequenzen für die Identity-Ökosysteme

Die deutschen Identity-Ökosysteme zeichnen sich durch eine Mischung von hardware- und softwarebasierten Lösungen aus; besonders sichtbar an den Standorten Berlin und München. Ein starker Kern aus großen und kleineren Unternehmen aus der IT-Sicherheit ist eine wichtige Bedingung für den langfristigen Erfolg, sowohl des Ökosystems wie auch der Unternehmen. Forschungseinrichtungen erzielen nur dann die gewünschte Wirkung, wenn ihre Ausstrahlung so stark ist, dass Unternehmen und Startups bereit sind, sich hier anzusiedeln. Sofern diese Bedingung erfüllt ist, hat auch ein Standort wie Bochum gute Chancen[39]. Die Nähe zu Metropolen ist dagegen nicht zwingend für den Erfolg eines Ökosystems, wie die Beispiele Kiel und Bochum zeigen. Unternehmen und Startups, die es schaffen, sich in ihrem jeweiligen Ökosystem zu behaupten, haben demnach gute Chancen, auch international Fuß zu fassen. Es fällt auf, dass Unternehmen wie G+D, Rhode & Schwarz und die Bundesdruckerei in mehreren Ökosystemen gleichzeitig aktiv sind; das gilt vor allem für Rhode & Schwarz.

[37] Vgl. dazu: Wie die Dezentralisierung Europa zum Handels- und Produktionszentrum der Welt machte
[38] Elektronisches Identitätsmanagement. Mehr Einfachheit, Datenhoheit und Datensicherheit in unserer virtualisierten Welt
[39] Vgl. dazu: "Im Ruhrgebiet lebt das richtige Mindset"

Kooperationen unter den Ökosystemen sind nötig und wünschenswert, schon alleine um unnötige Doppelarbeiten zu vermeiden.

Um der Blickverengung zu entgehen, ist es von Vorteil, den Erfahrungsaustausch mit ausländischen Identity-Ökosystemen zu suchen, wie im Fall des Hessian Israeli Partnership Accelerator (HIPA). Der Wirtschaftswissenschaftler Ricardo Haussmann von der Harvard University hat herausgefunden, dass man, wenn man die Geschichte eines Ortes kennt, vorhersagen kann, welche Industriezweige neu entstehen, verschwinden bzw. wachsen oder schrumpfen werden. Haussmann empfiehlt Ländern, die vor der Entscheidung stehen, in welche Branchen sie als nächstes investieren sollten, sich ein erfolgreiches Land anzuschauen, das ihnen zwei Jahrzehnte zuvor ähnlich war[40]. Beispiele, die bereits genannt wurden: Estland und Skandinavien. Dazu noch Kanada[41].

[40] Länder scheinen sich für Industriezweige zu entscheiden, die mit denen verwandt sind, die sie bereits haben.

[41] Kanadische Banken setzen auf Verified.Me

Anhang

Identity Startups und Unternehmen außerhalb der untersuchten Identity-Ökosysteme

Name	Kernkompetenz	Standort
Identity Trust Management	Identity as a Service	Düsseldorf
Governikus	Authentifzierung/Identifizierung	Bremen
Nect	Digitale Authentifizierung	Hamburg
Identos	Identifizierungslösungen für die Gesundheitsbranche	Mannheim
SkiDentity	Mobile eID as a Service	Michelau
Talisman.id	Digitale Identität auf Blockchain-Basis	Hildesheim
BioID	Biometric authentication software	Nürnberg
Dermalog	Technologischer Marktführer in Deutschland für die biometrische Identifizierung	Hamburg
Crif Bürgel	Digital Identity Check	Hamburg
Post	Post Ident	Bonn
Kobil Deutschland	IAM / IT-Security	Worms
Arvato/Post	Digital Identity Check	Gütersloh
SCHUFA	Auskunftei, SCHUFA-Identitätscheck	Wiesbaden
netID	Login-Allianz	Montabaur
YES	Offenes Identity Scheme für Banken und deren Kunden	Lachen/Schweiz
ID4me	Föderatives, dezentrales Identitätsmanagement, SSO	Brüssel