Apple Identity Wallet

Disruption als Katalysator digitaler Transformation

Artur Burgardt
Maarten Oestreich
Pierre Heugle

November 2019
Blogpost

Key Facts

- Im Umfeld des kontinuierlich wachsenden Digitalisierungsgrades wird verstärkt im Rahmen analoger Geschäftsprozesse der Teilbereich starker Identifizierung und Authentifizierung Privat- und juristischer Personen in die digitale Welt überführt. Hierbei ist ein exponentiell steigendes, Industrie-übergreifendes Marktpotential digitaler Identitätsverwaltung ersichtlich

- Die Marktsignifikanz des technologischen Fortschritts wird durch das regulatorische und katalytische Einwirken des Europäischen Parlaments und Rates in Form der eIDAS (electronic identification, authentication and trust services) Verordnung untermauert. Die bestehende Nachfrage nach definierter Interoperabilität wird weiterführend in der Anzahl bereits notifizierter, bzw. in Prüfung befindlicher nationaler eID-Schemes verdeutlicht

- Auf Basis des am 19. September veröffentlichen iOS 13 Betriebssystems besteht erstmalig die Möglichkeit, den neuen Personalausweis via der eID-Funktionalität ebenfalls auf Apple Geräten auszulesen und die abgeleitete Identität für digitale Anwendungsbereiche zu verwenden

- Unter Berücksichtigung kürzlich durch Apple veröffentlichter Komponenten in Form des CryptoKits zur möglichen Etablierung Hardware-basierter Wallets als Voraussetzung zur sicheren, lokalen Ablage digitaler Identitätsinformationen, fokussierter Marktpositionierung der Apple Login Funktionalität als primäre Authentifizierungsmöglichkeit, als auch des am 24.10.2019 veröffentlichen Patents zur sicheren Ablage und Wiederverwendung von Identitätsinformationen (Identity Credential Verification Techniques) können die erforderlichen Kernbereiche eines vollumfassenden Identitätsmanagementsystems bereitgestellt werden

- Eine aktive Vermarktung des neuen Personalausweises in Form der eID-Funktionalität und einhergehende Ausrichtung zur Verwendung der Android- und iOS-Geräte führt zur aktiv geförderten Kundenakzeptanz Endgeräte-basierter Identifizierung und damit einhergehend einer indirekten Senkung der Markteintrittshürden einer Apple / Google Identity Wallet. Zeitgleich würde dies dazu führen/ hat dies das Potential die Wertschöpfungskette wiederholter, eID-basierter Identifizierungen abzuschneiden, da auf Basis initialer Identitätserfassung eine digitale Kopie abgeleitet und im Secure Element zur Wiederverwendung gelagert wird

- Bei konsequenter Umsetzung avisierter Apple / Google Strategieausrichtung fällt der Anwendungsfall wiederkehrender Durchführung digitaler Identitätsprüfung, z.B. in Form von Video-Ident und somit das Hauptgeschäftsfeld derzeitiger Marktteilnehmer digitaler Identifizierungslösungen weg

- Aufgrund technologischer Alternativen schließt sich das Handlungsfenster zur aktiven Marktteilnahme und profitabler Bereitstellung vorgehaltener Identitätsinformationen, beispielswiese seitens des Finanz- und Versicherungssektors

- Die mittelfristig vollumfängliche Digitalisierung sensibler Identitätsinformationen unter Anwendung des kundenzentrierten, Endgeräte-basierten Datenhaltungskonzeptes und bequemer, integrativer Wiederverwendung ohne notwendige Neu-Identifizierung kann sich disruptiv auf die momentane Marktsituation auswirken. Derzeitige Strategieausrichtungen des öffentlichen und privaten Sektors sollten zur Vermeidung potentieller Verdrängung aus dem exponentiell wachsenden und höchst profitablen Identitätsmarkt neu kalibriert werden

Die ab iOS 13 für Drittanwendungen zugängliche NFC-Schnittstelle (Near Field Communication) stellt in Kombination mit dem am 24. Oktober 2019 veröffentlichen Patent zur sicheren Ablage und Wiederverwendung von Identitätsinformationen eine Besonderheit im Vergleich zur bisherigen Strategie von Apple dar.

Im Umfeld des exponentiell steigenden, Industrie-übergreifenden Digitalisierungsgrades wird verstärkt der Teilbereich starker Identifizierung und Authentifizierung der Privat- und juristischer Personen in die digitale Welt überführt. Die fortschreitende Entwicklung entsprechender Services wird multifaktoriell sowohl seitens des technologischen Reifegrads zur Verfügung stehender Identifizierungs- und Authentifizierungslösungen in Hinblick notwendiger Sicherheit und Identifikationsmittelakzeptanz als auch seitens der klaren Nutzererwartung hinsichtlich medienbruchfreier, digitaler Produkte, begünstigt. Hierauf aufbauend erwachsen neue, auf die starke Identifizierung / Authentifizierung fußende Segmente signifikanter Marktrelevanz wie z.B. e-Health und Smart Cities. Innerhalb bestehender Industrien sensibler Kundenidentitäten (z.B. Banking, Insurance) entsteht additiv die Möglichkeit, Prozesse regulierter Identitätsprüfung vollumfänglich entlang geltender Compliance- und Security-Anforderungen zu digitalisieren.

In diesem Kontext stellt die veröffentliche iOS 13 Betriebssoftware in Bezug auf die für partielle Anwendungsfelder zugänglichen NFC-Schnittstelle (Near Field Communication) eine Besonderheit übergreifender, auf ein geschlossenes Ökosystem ausgerichteter Apple Strategie dar. Hierdurch ist es erstmalig, wie auf den Android Geräten bereits etabliert, möglich, den neuen Personalausweis via der eID-Funktionalität auszulesen und die abgeleitete Identität für digitale Anwendungsbereiche zu verwenden. Zwar ist die Marktakzeptanz dieser Lösung derzeit aufgrund historisch teilweise komplexer Onboardingprozesse und nur selektiv zur Verfügung stehender Anwendungsfälle reglementiert, jedoch wirkt die, seit 15.07.2017 regulatorisch vorgeschriebene, automatische Aktivierung der eID Funktionalität und voraussichtlich kurzfristige Aberkennung regulatorischer Konformität alternativer Identifizierungsmethoden in Form des Video-Ident Verfahrens für GwG-konforme (Geldwäschegesetz) Anwendungsfälle diesem Defizit entgegen. Somit wird bei Betrachtung des übergreifenden Marktpotentials und Gegebenheit des digitalen Identitätsmanagements statt einer außerordentlichen Einzelentscheidung eine übergreifende, voraussichtlich vorbereitete Strategieausrichtung ersichtlich. Diese Ableitung verfestigt sich sowohl unter Berücksichtigung des bei der Apple Worldwide Developers Conference 2019 angekündigten CryptoKits zur möglichen Etablierung Hardware-basierter Wallets als Voraussetzung zur sicheren, lokalen Ablage digitaler Identitätsinformationen, als auch der fokussierten Marktpositionierung der Apple Login Funktionalität als primäre Authentifizierungsmöglichkeit. Die initiale Annahme gezielter Strategieausrichtung wird zuletzt durch die jüngsten, am 24.10.2019 veröffentlichtes Apple Patente zur sicheren Ablage und Wiederverwendung von Identitätsinformationen (Identity Credential Verification Techniques - Pub. No. 20190325125, 20190327228) bestätigt. Diese sind jeweils separat auf die Identifikationsmittel Führerschein, Personalausweis ausgerichtet und entlang der Teilbereiche sicherer Erstellung, Ablage und Übertragung digitaler Identitätsinformationen strukturiert.

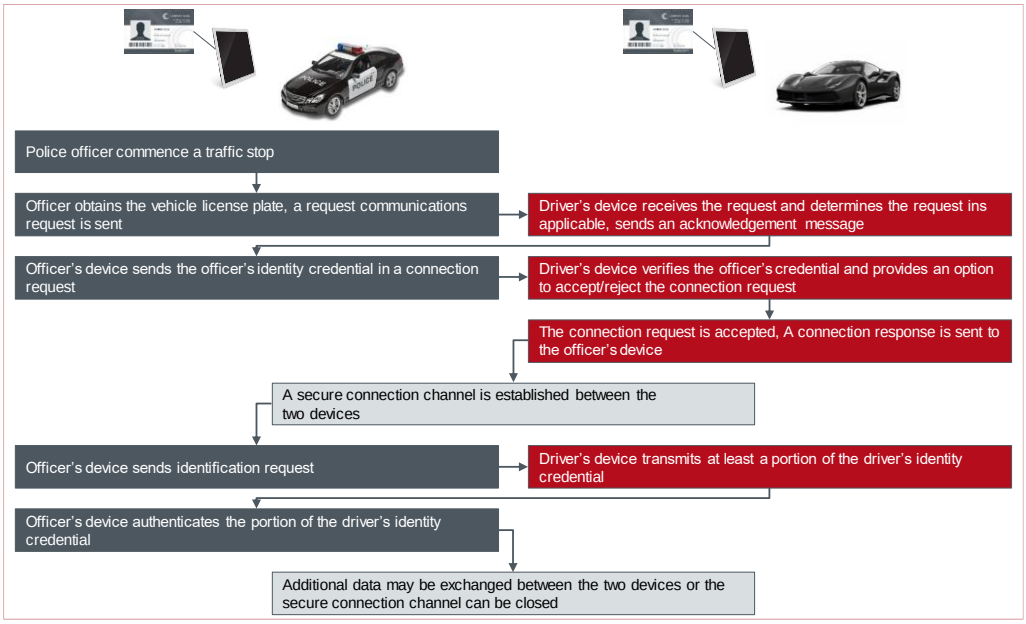

Abbildung 1 – Auszug Apple Patent - Beispielprozess zur Identitätsbereitstellung und Verifikation

Hierdurch werden die seitens eines vollumfassenden Identitätsmanagementsystems notwendigen Komponenten der starken Identitätsvalidierung, lokaler Datenhaltung und nachgelagerter Authentifizierung vereint. Dieses Vorgehen erlaubt es Apple nicht nur alleinig sich als digitaler Identitätsanbieter zu etablieren, sondern ebenfalls die notwendigen, technischen Voraussetzungen zur avisierten Positionierung innerhalb des profitablen e-Health Bereiches zu schaffen. Der Aufsichtsrat der Apple Inc. beschloss die Ergänzung der Konzernstrategie um e-Health-Komponenten für Hardware, Software und Services. Mittlerweile postuliert der CEO des Unternehmens, Tim Cook, diesen Aspekt als den größten zukünftigen Werttreiber des Unternehmens und gleichzeitig den größten Beitrag für die Gesellschaft; er spricht in diesem Zusammenhang von der globalen Gemeinschaft. Hierbei wurden im Jahr 2018 zeitgleich drei Funktionalitäten der Apple Watch (EKG Sensor, Pulssensor zur Erkennung von Vorhofflimmern, Sturzsensor) durch die Lebensmittelüberwachungs- und Arzneimittelbehörde der Vereinigten Staaten FDA zugelassen, bzw. befinden sich in finaler Prüfung.

Neben Apple treibt ebenfalls das Technologieunternehmen Google als Hauptakteur den technologischen Fortschritt sicherer und bequemer Kundenidentifizierung / Authentifizierung voran. Entlang der Entwicklerkonferenz Google I/O 2019 wurde das Bestreben kommuniziert, elektronische Identitäten vollumfänglich auf die Google Geräte zu überführen und die Nutzung dieser via dedizierter API anzubieten. Initial soll das System dahingehend aufgesetzt werden, den qualifizierenden Nachweis über den Besitz eines Führerscheins gemäß ISO 18013-5 erbringen zu können. Die Grundlage hierzu wurde, neben weiteren anverwandten Standards, seit Jahren aktiv von Google begleitet und mitentwickelt.

Exponentiell steigendes Marktpotential digitaler Identität Industrie-übergreifend ersichtlich

Bei Betrachtung des exponentiell steigenden Markpotentials Identitäts-basierter Anwendungsfälle ist die frühzeitige Strategieausrichtung globaler Technologieunternehmen Apple und Google vollumfänglich begründbar. Innerhalb des e-Health Industriesegments wird im Jahr 2018 ein Marktwert in Höhe von 142 Milliarden Dollar ersichtlich, welcher voraussichtlich, exponentiell wachsend im Jahr 2020 die 200 Milliarden Dollar Marke überschreitet (siehe Abbildung 2).

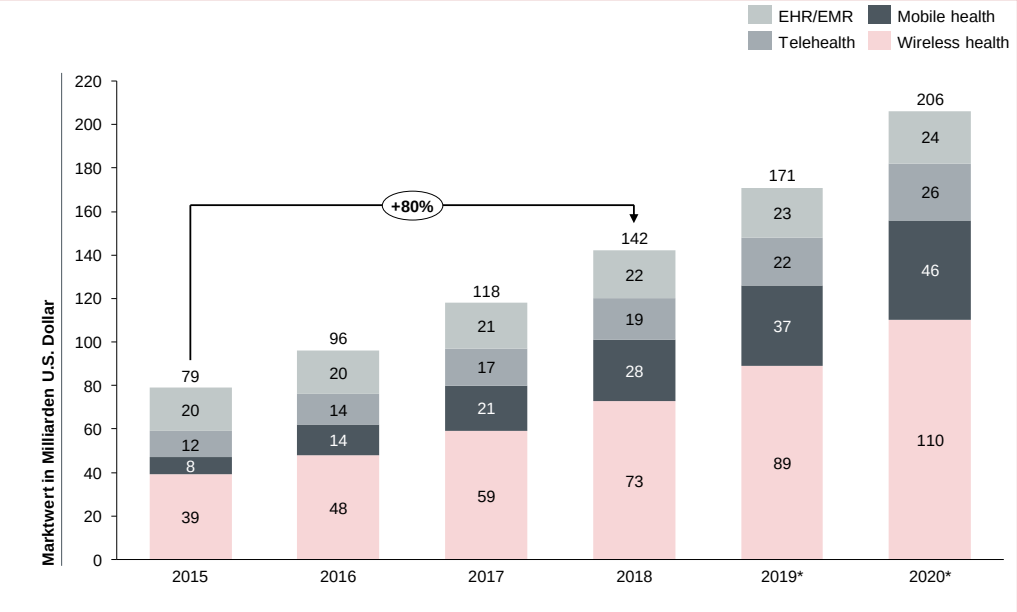

Abbildung 2 - Marktwert des globalen, digitalen Gesundheitsmarktes von 2015 bis 2020 in Milliarden U.S. Dollar (* Prognose 2019, 2020)

Weiterhin wird beispielhaft innerhalb des aufkommenden IoT-Industriezweiges im Jahr 2018 ein globaler, in den letzten 4 Jahren um 50% gestiegener Umsatz in Höhe von 94 Milliarden Dollar erwartet (siehe Abbildung 3). Auf Basis derzeitiger Prognose steigt dementsprechend die Anzahl installierter IoT-Geräte in den nächsten 5 Jahre um 133% (siehe Abbildung 4).

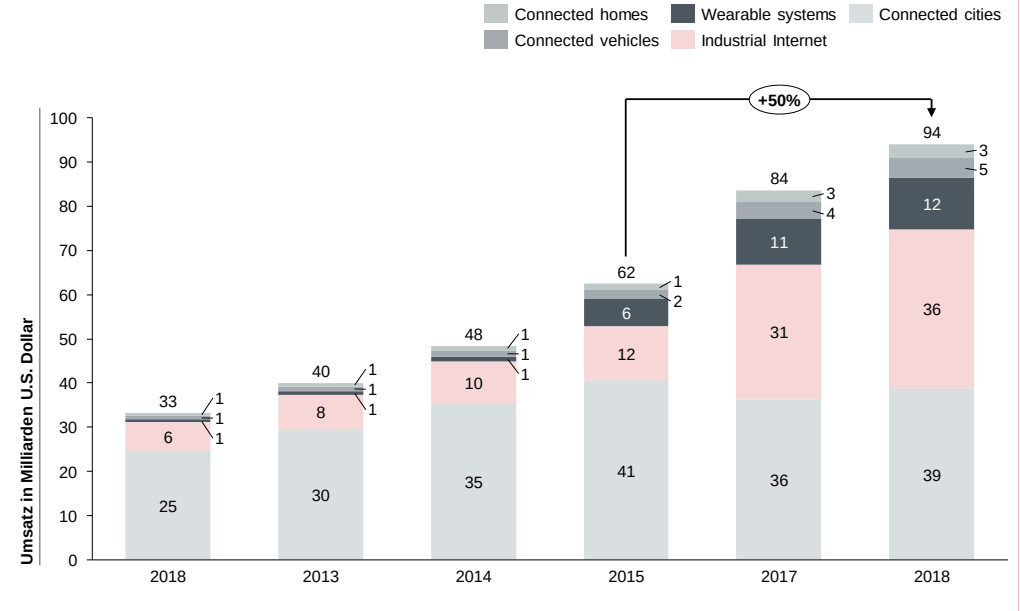

Abbildung 3 - Umsatz im Bereich Internet of Things weltweit von 2012 bis 2018 (in Milliarden U.S. Dollar)

Zur möglichen Beherrschung der Vielzahl (voraussichtlich 62 Milliarden im Jahr 2024 – siehe Abbildung 4) verbundener Geräte in Hinsicht notwendiger Identitätszuweisung und Betrugsprävention verfestigen sich die notwendigen Identitätsmanagementsysteme, inklusive dazugehöriger Technologien, Standards und Interoperabilitätskonzepten auf dem globalen Markt.

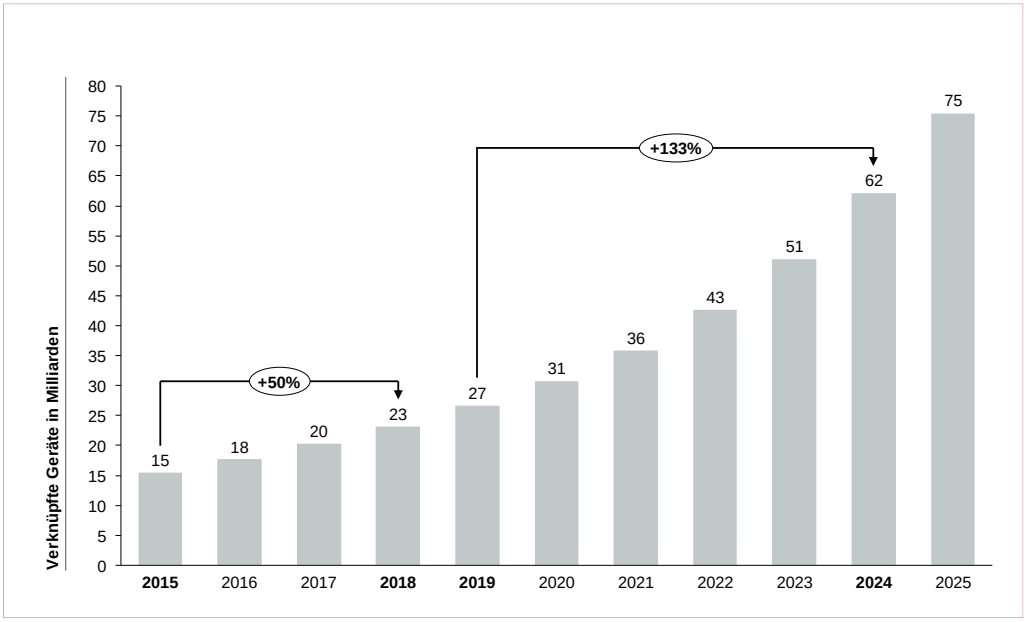

Abbildung 4 - Anzahl installierter IoT-Geräte in Milliarden

Das signifikant steigende Marktpotential digitaler Identitäten wird neben aufkommenden Geschäftsbereichen (z.B. e-Health, Internet of Things) ebenfalls innerhalb bereits etablierter Segmente, wie z.B. des Banking und Payment Sektors ersichtlich.

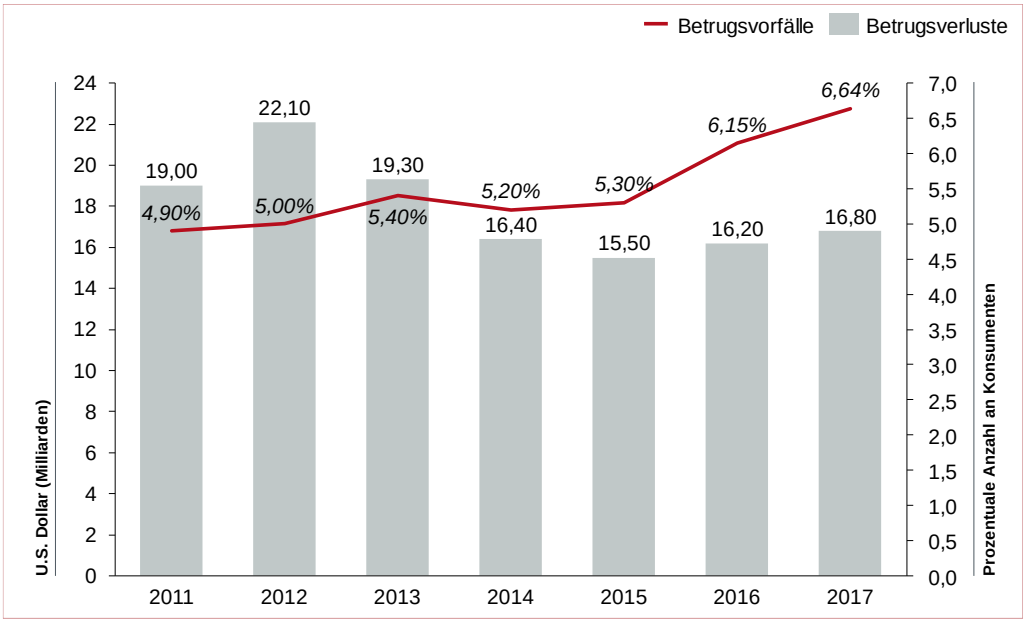

Abbildung 5 - Anzahl gemeldeter Betrugsvorfälle und des resultierend erlittenen, budgetären Schadens in Vereinigten Staaten 2011 - 2017

Zusammenführend sind 61% (~ 13.48 Mrd. U.S. Dollar) des in den Vereinigten Staaten im Jahr 2018 erlittenen Betrugsschadens auf Identitätsdiebstahl zurückzuführen. Unter Berücksichtigung signifikant ansteigender CNP-Betrugsraten (Card not present, +94% im Jahr 2017 in Vergleich zu 2014 – siehe Abbildung 6) ist die Etablierung technologisch ausgereifter Identitätsmanagementsysteme und hierauf aufbauender, moderner Authentifizierungsverfahren der notwendige Haupttreiber zur Minimierung und Beherrschung des durch digitalen Identitätsdiebstahl entstehenden Risikopotentials.

Zeitgleich können auf Basis aufkommender, regulatorisch konformer Identifizierungslösungen innerhalb der strikt regulierten Finanzindustrie die abgeleiteten Prozessketten (z.B. Know-Your-Customer) vollumfänglich digitalisiert, verschlankt und optimiert werden.

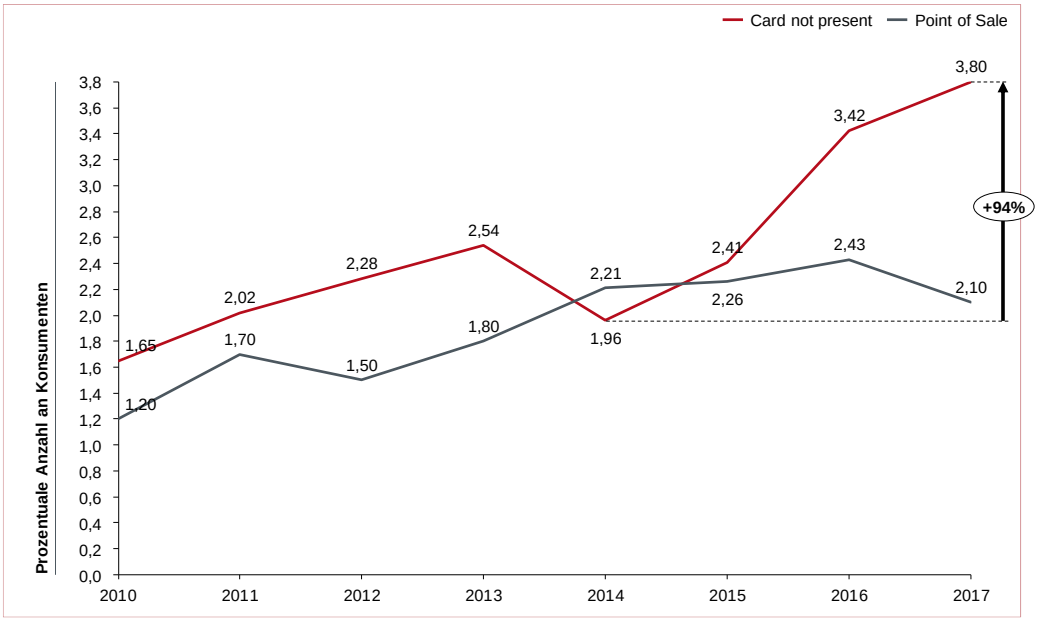

Abbildung 6 – Prozentualer Anteil von Card not Present / Point of Sale Betrugsfällen in Vereinigten Staaten 2010 - 2017

Die europaweit geltende eIDAS (electronic identification, authentication and trust services) Verordnung dient als Katalysator des digitalen Identitätsmarktes

Übergreifend wird das exponentiell wachsende Marktpotential digitaler Identitäten durch das regulatorische und katalytische Einwirken des Europäischen Parlaments und Rates in Form der eIDAS (electronic identification, authentication and trust services) Verordnung (EU) Nr. 910/2014 untermauert. Diese hebt somit die Signaturrichtlinie 1999/93/EG auf und forciert u.a. auf Basis notwendiger Schaffung inter-staatlicher Interoperabilität den Abbau digitaler Hürden europaweiter Bürgeridentifizierung im Umfeld öffentlicher Services. Hiermit soll das europäische Marktpotential digitaler, auf starker Kundenidentifizierung / Authentifizierung fußender Anwendungsfälle gehoben werden. Da es sich bei der, seit Juli 2016 (Art. 52) vollumfänglich geltenden eIDAS Verordnung um unmittelbar anwendbares Recht handelt, gilt es, die abgeleiteten nationalen Vorgaben mandatorisch in allen 28 EU-Mitgliedstaaten umzusetzen. Die bestehende Nachfrage definierter Interoperabilität wird weiterführend in der Anzahl bereits notifizierter, bzw. in Prüfung befindlicher nationaler eID-Schemes verdeutlicht, welche spätestens 12 Monate nach erfolgter Notifizierung seitens aller Mitgliedsstaaten bei Umsetzung nationaler Online-Services öffentlicher Stellen national anerkannt werden müssen (Verordnung Nr. 910/2014 – Kapitel II, Artikel 6).

Der hieraus abgeleitete Wachstumsstrom digitaler Kundendatennutzung und Kommunikation wird übergreifend seitens der EU-DSGVO und e-Privacy Verordnung, fokussierend auf kundenzentrierten Datenschutz zur transparenten Informationsverwertung und Bereitstellung gestützt.

Status Notifizierungsverfahren nach Ländern

Status Notifizierungsverfahren nach Schemata

Land	Level of Assurance[4]	Status
Belgien	Hoch	Notifiziert
Kroatien	Hoch	Notifiziert
Tschechien	Hoch	Notifiziert
Estland	Hoch	Notifiziert
Deutschland	Hoch	Notifiziert
Italien - eID	Hoch	Notifiziert
Italien - SPID	Niedrig – Hoch	Notifiziert
Lettland	(Hoch)	Pre-notifiziert
Luxemburg	Hoch	Notifiziert
Portugal - eID	Hoch	Notifiziert
Portugal - Mobil	(Hoch)	Peer-reviewed
Portugal - Attribute	(Hoch)	Pre-notifiziert
Spanien	Hoch	Notifiziert
Niederlande	Substanziell – Hoch	Notifiziert
Vereinigtes Königr.	Niedrig – Substanziell	Notifiziert
Slowakei	(Hoch)	Pre-notifiziert
Dänemark	tbd	Pre-notifiziert

Abbildung 7 - Status eID Schemes Notifizierungsverfahren

Global agierende, technologiegetriebene und cross-industriell ausgerichtete Plattformen sind prädestiniert den Markt digitaler Identitätsmanagementsysteme auf Basis bereits signifikanter Kundenbasis zu forcieren

Aus der dargestellten Nachfrage digitaler, starker Kundenidentifizierung und Authentifizierung abgeleitet, etablieren sich drei Ausprägungen möglicher Geschäftsmodelle innerhalb des digitalen Identitätsmanagement Ökosystems:

- **Identifizierungs- / Authentifizierungslösungsanbieter:** Unternehmen spezialisiert auf die Forschung, Entwicklung und Bereitstellung digitaler Lösungen des Identitätsnachweises (z.B. Video- und Call Center Agent- / Video- und Algorithmus-basierte Prüfung, NFC-spezifische Verwendung des neuen Personalausweises) auf Basis anerkannter Identifikationsmittel (z.B. Personalausweis, Pass) und nachgelagerter Kundenauthentifizierung (z.B. Gesichts- / Stimmenerkennung).

- **Identitätsorchestrator:** Zusammenführung bestehender Identifizierungs- und Authentifizierungslösungen via zentraler, konsolidierter API zur Simplifizierung avisierter Integrationen mehrerer Identifizierungs- und Authentifizierungsmethoden.

- **Identitätsmanagementsysteme:** Auf die potentielle Vorhaltung, Verwaltung und Weitergabe erhobener, digitaler Identitäten ausgerichtete Systeme, welche z.T. bestehende, marktübliche Identifizierungslösungen beinhalten und mit weiteren Identitätsorchestratoren kooperieren. Hierbei können Konzepte zentraler und dezentraler Datenhaltung unterschieden werden. Dabei wird ein notwendiger Netzwerkpunkt zur Marktorganisation und Standardisierung etabliert.

In diesem Kontext stehen die dargestellten Geschäftsmodelle in synergetischer Abhängigkeit unter Verfolgung differenzierter Strategieausrichtung.

- Die Identifizierungs- / Authentifizierungslösungsanbieter fokussieren hierbei auf Optimierung bestehender und Entwicklung neuer, interaktionsärmerer Identifizierungs- und Authentifizierungsverfahren (z.B. Algorithmus-basierte Dokumentenerkennung, Voice Recognition, Behaviourmetrics).

- Die Identitätsorchestratoren avisieren die überproportional wachsende Anzahl integrierter Identifizierungs- und Authentifizierungsmethoden.

- Die Identitätsmanagementsysteme streben die stärkst mögliche, cross-industrielle Marktverbreitung zur Wiederverwendung erhobener Identitäten entlang aller gängiger Sicherheitsstufen / Level of Assurance (ISO/IEC 29115) an.

Aufgrund möglicher, direkter oder via Identitätsorchestratoren indirekter Integration der Identifizierungs- / Authentifizierungslösungsanbieter und Wiederverwendung einmalig digital erhobener Identität, bieten die Identitätsmanagementsysteme, voraussichtlich in Form eines infrastrukturellen Ankers des digitalen Handels, im relativen Vergleich das signifikanteste Marktpotential.

In diesem Zusammenhang sind dementsprechend global agierende, cross-industriell ausgerichtete Technologieunternehmen prädestiniert den Markt digitaler Identitätsmanagementsysteme auf Basis bereits signifikanter Kundenbasis zu forcieren. Hierbei wird im initialen Schritt die mandatorische Erstellung einer niedrigschwelligen Identität zur möglichen Angebotsnutzung positioniert. Bei Erreichung signifikanter Marktakzeptanz des etablierten Produktes wird die generierte Identität zur Authentifizierung bei Drittapplikationen angeboten, sodass das Unternehmen verstärkt als Identitätsadministrator und Anbieter wahrgenommen wird. Entlang fortlaufender Ausrichtung weiterer, Industrie-übergreifender Angebote entsteht die notwendige Omnipräsenz vorgehaltener, digitaler Identität und des hiermit verknüpften, steigenden Kundenvertrauen. Im finalen Schritt etabliert sich das Unternehmen bei Integration weiterer Identifizierungs- / Authentifizierungslösungsanbieter als digitales Identitätsmanagementsystem hoher Qualitätsgüte, welches eine starke Kundenbindung an das bereits weitverbreit akzeptierte Ökosystem hervorruft.

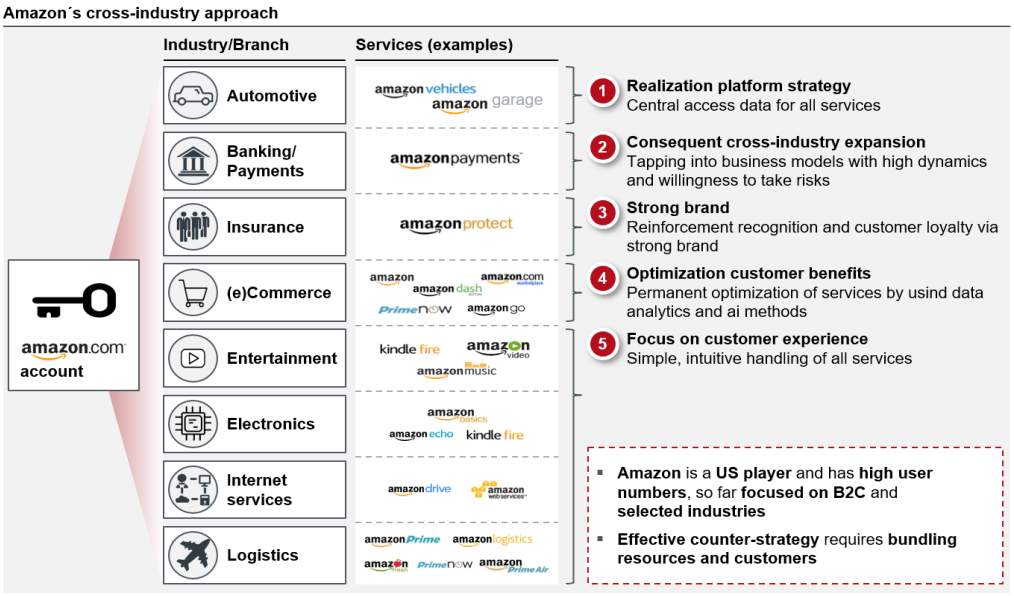

Abbildung 8 - Übersicht Amazon Cross-Industrie Ausrichtung

Dies kann beispielhaft anhand des Unternehmens Amazon verdeutlicht werden, welches diverse Services und Produkte derzeit unter Verwendung selbiger Identität innerhalb 8 unterschiedlicher Branchen mit einem, im Jahr 2016 globalen Gesamtumsatz in Höhe von ~140 Milliarden USD anbietet.

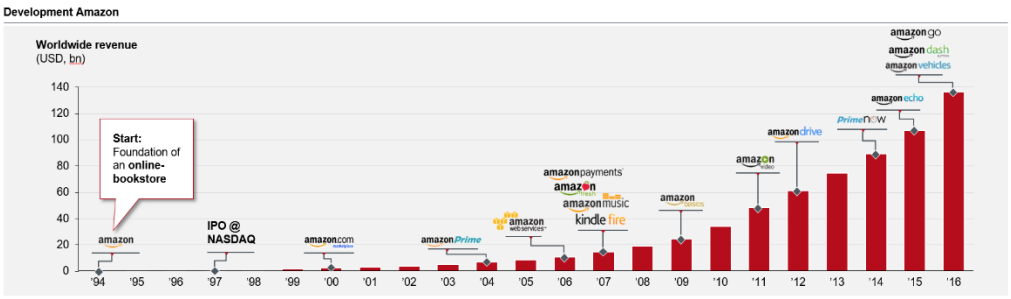

Abbildung 9 - Weltweiter Umsatz von Amazon 1994 - 2016 in Milliarden U.S. Dollar

Die weiteren internationalen Plattformanbieter in Form von Google, Apple, Facebook und Alibaba waren unter Verfolgung vergleichbarer Strategieausrichtung in der Lage die Kundenanzahl entlang der letzten Jahre überproportional zu steigern.

Vergleichbare Marktstärke geht ebenfalls von global agierenden Card Schemes aus, welche einerseits durch Verwendung zukunftsweisender Identifizierungs- / Authentifizierungsverfahren eigenoptimiert den anwachsenden, digitalen Betrug eindämmen, andererseits via weltweiter Beteiligung an Bezahlprozessen unter minimaler Strategieadjustierung die Komponenten vorangehender Identifizierung / Authentifizierung vollintegriert anbieten können.

In diesem Zusammenhang wurde seitens MasterCard eine Digital Identity Initiative ausgerufen und initiale Kooperationen zur gemeinsamen Entwicklung zukunftsweisender Identitätsmanagementinnovationen mit Microsoft (Dezember 2018) und Samsung (Mai, 2019) initiiert. Das bestehende Konzept fokussiert hierbei eine dezentrale Datenhaltung und zentrale Markt- und Netzwerkorchestration.

Die avisierte Apple / Google Strategieausrichtung lokaler Identitätsspeicherung und direkter Informationsweitergabe führt zur Trennung bestehender Wertschöpfungskette wiederholter, eID-basierter Identifizierungen.

Bei Betrachtung von Apples Produkt- und Kommunikationsfokussierung in Richtung des Identitäts-sensiblen e-Health Marktes, der Bereitstellung kryptographischer Technologien in Form des CryptoKits zur möglichen Etablierung Hardware-basierter Wallets als Voraussetzung zur sicheren, lokalen Ablage digitaler Identitätsinformationen und der Markt-aggressiven Positionierung der Apple Login Funktionalität ist die partielle Öffnung der NFC-Schnittstelle zur digitalen Identitätserfassung und die Patentierung sicherer Ablage und Wiederverwendung von Identitätsinformationen der nächste logische Schritt zur Besetzung des profitablen Identitätsmarktes.

Dies eröffnet zeitgleich die Möglichkeit den neuen Personalausweis, die eID Funktionalität nutzend, per NFC auf den iOS Geräten auszulesen und die, mit starker Identitätsprüfung behafteten Anwendungsfälle vollumfänglich zu digitalisieren. Der Gesamtprozess kann in diesem Zusammenhang auf Basis der europäisch geltenden eIDAS Verordnung auf dem höchsten Sicherheitslevel eIDAS high eingestuft und in Behörden-nahen Bereichen etabliert werden.

Hierbei sind mit dem, innerhalb moderner Endgeräte befindlichen, entkoppelten Chips (Secure Element) zur Ablage sensibler Informationen, dem etablierten CryptoKit, der Apple Login Funktionalität und dem übergreifenden Konzept digitaler Identity Wallet die, bis auf die erforderliche Nutzung offizieller Identifizierungsmittel (z.B. Personalausweis / Pass) initialer Kundenidentifizierung, notwendigen Voraussetzungen zur vollumfänglichen Identitätsdigitalisierung und Wiederverwendung bereits gegeben.

In diesem Kontext werden auf Basis der für Drittanwendungen freigegebenen NFC Schnittstelle sowohl die jeweils lokalen, heterogenen Regulatorik- und Sicherheitsanforderungen des privaten und öffentlichen Sektors digitaler Identitätsprüfung, als auch diverse technologische Ausprägungen offizieller Identifikationsmittel ersichtlich. In der Folge dessen kann kein übergreifendes Produkt digitaler Identifizierung innerhalb des geschlossenen Ökosystems seitens Apple ohne externe Unterstützung nationaler Strukturen bereitgestellt werden. Zur Mitigation dieser Situation können die globalen Technologieanbieter durch die aktive Kooperation mit lokalen Lösungsanbietern und staatlichen Institutionen von notwendigen, lokalen Marktkenntnissen profitieren und mittelfristig eine vollumfänglich digitale Identität etablieren.

Zwar bestehen im Marktsegment digitaler Identitätsverwaltung weiterführende Konzepte zentraler / dezentraler, Server-getriebener Datenhaltung (z.B. netID, Verimi). Aufgrund der größtmöglichen Eigenbestimmung bei lokaler Informationsspeicherung, integrierter Authentifizierungsmöglichkeiten und hoher Kundenbasis niederschwelliger Identitäten ist jedoch im relativen Vergleich von einem signifikanten Erfolg Geräte-basierter Identitätsverwaltung auszugehen.

Das Gefahrenpotential für die öffentliche Hand besteht hierbei in der indirekten, jedoch aktiven Vermarktung der Apple / Google Identity Wallet in Form eines staatlich akzeptierten Vertrauensankers als notwendiges Vehikel zur flächendeckenden Positionierung der eID Funktionalität. Sobald dieser Zustand realisiert wurde, besteht seitens Apple / Google auf Basis der europaweit geltenden eIDAS Verordnung die Auswahlmöglichkeit einer, im relativen

Vergleich zur eID Funktionalität verstärkt auf Convenience ausgerichteten, bestenfalls Software-basierten Methode zur initialen Personenidentifizierung und nachfolgender eIDAS Notifizierung der, unter Verwendung des Secure Elements abgeleiteten, vollumfänglich digitalisierten Identität auf dem Vertrauensniveau substanziell. Unabhängig von nationalen Sicherheitsvorgaben und avisierter Positionierung eigener, staatlich geförderter Identifizierungslösungen wird man das notifizierte Verfahren entlang des europäischen Rechts für eine Vielzahl an Anwendungsfällen akzeptieren müssen. Da auf Basis initialer Identitätserfassung eine digitale Kopie abgeleitet und im Secure Element zur Wiederverwendung gelagert wird, schneidet dieses Konzept additiv die Wertschöpfungskette wiederholter, eID-basierter Identifizierungen ab.

Da aufgrund der voraussichtlichen Apple / Google Strategieausrichtung frühestmöglicher Realisierung des Marktpotentials digitaler Identitäten die Technologieunternehmen bei potenziell vorliegenden Alternativen auf europäischer Ebene keine Rücksicht auf nationale Gegebenheiten nehmen werden können, gilt es, seitens staatlicher Institutionen zur Vermeidung mittelfristiger, Technologie-getriebener Verdrängung kurzfristig und pro-aktiv ein aktives und gemeinschaftliches, auf die bestmögliche Convenience / Security Balance ausgerichtetes Kooperationsmodell zu definieren.

Auf Basis avisierter Apple / Google Strategieausrichtung fällt der Anwendungsfall wiederkehrender Durchführung digitaler Validierung, z.B. in Form von Video-Ident und somit das Hauptgeschäftsfeld derzeitiger Marktteilnehmer digitaler Identitätsvalidierung weg.

Neben aufkommenden Herausforderungen des öffentlichen Sektors im Kontext skizzierter Strategieausrichtung globaler Technologieunternehmen gilt es, die Zukunftsfähigkeit derzeitiger Marktteilnehmer digitaler Identitätsvalidierung (z.B. via Video-Ident) zu hinterfragen. Aufgrund des Apple / Google Lösungsansatzes Geräte-basierter Datenspeicherung und Wiederverwendung wird man zwar weiterhin auf eine initiale Identitätsprüfung zur Ableitung digitaler Identität angewiesen sein, jedoch fällt in diesem Fall der Anwendungsfall wiederkehrender Durchführung digitaler Validierung, z.B. in Form von Video-Ident und somit das Hauptgeschäftsfeld derzeitiger Marktteilnehmer weg. Somit wird es erforderlich sein, sich entweder als Preferred Supplier gegenüber Apple / Google zu positionieren oder das Geschäftsfeld auf die umliegenden Mehrwertdienste zu verlagern.

Aufgrund technologischer Alternativen schließt sich das Handlungsfenster zur aktiven Marktteilnahme und profitablen Bereitstellung vorgehaltener Identitätsinformationen seitens des Finanz- und Versicherungssektors.

Da die auf dem Secure Element gelagerte Identität einerseits via initialer Prüfung offizieller Identifikationsmittel andererseits jedoch ebenfalls aus bestehenden Quellen bereits erhobener Identität abgeleitet werden kann, gilt es, additiv die Marktrelevanz identitätshaltender Unternehmen (z.B. Banken, Versicherungen) bei kurzfristiger Realisierung der Apple / Google Strategieausrichtung zu prüfen. Aufgrund mittelfristiger, vom Secure Element ausgehender Wiederverwendung persönlicher Informationen und der Möglichkeit initialer Personenprüfung in Kooperation mit etablierten Identifikationsdienstleistern schließt sich das Handlungsfenster zur

aktiven Marktteilnahme und Veräußerung vorgehaltener Identitätsinformationen seitens der Akteure im Finanz- und Versicherungsumfeld.

Die hoheitliche Verfügbarkeit von Identitäten ist basierend auf der Marktdurchdringung mobiler Endgeräte bei gleichzeitiger Kontrolle sicherheitsrelevanter Features durch Hersteller als Kooperationsmodell zu verhandeln.

Die Identifizierung und Anerkennung von Persona in der physischen bzw. analogen Welt ist eine hoheitliche Aufgabe, über die gesetzliche Instanzen wachen. Dem zunehmenden Bedarf nach anerkannten starken Identifizierungen im digitalen Datenraum wurde von staatlicher Seite mittels der eID Initiative begegnet. Allerdings zeigen sich, wie eingangs erläutert, aktuell noch praktische Barrieren, die einem großflächigen Einsatz bzw. der festen Etablierung als zentrales Element, entgegenstehen.

Der gravitativen Wirkung der Hardware-Anbieter müssen sich auch Institutionen der Legislative stellen, da diese im Markt mobiler Endgeräte als Eintrittstor dahinterliegender Identitätsverwaltung nicht umgangen werden können. Denn die zunehmende Verfügbarkeit mobiler Endgeräte mit entsprechender Sicherheitshardware (Secure Element) zur starken Authentisierung bei gleichzeitig hoher Convenience (Biometrie) weckt große Bergehrlichkeit bei Endkunden und damit den Bürgern des Staats.

Zur Absicherung der mittelfristigen Steuerungshoheit des Staates sollte ein gemeinsames Kooperationsmodell definiert werden (siehe Kooperationsprojekt OPTIMOS 2.0). Dies ist notwendig, da ein einseitiges Vorgehen wie im zuvor beschriebenen Beispiel zu mangelnder Anerkennung des Systems oder aber einer regulatorischen Unsicherheit sowie potenzieller Standort-Arbitrage führen kann. Ein kurzfristig gemeinschaftlicher Ansatz kann hierbei die notwendige Berücksichtigung staatlicher Eigeninteressen gewährleisten. Bei der Herleitung eines entsprechenden Ansatzes muss grundlegend die systembezogene Interoperabilität hinsichtlich standardisierten Datenformats, Portabilität zwischen Geräten und dem bruchfreien Zugang über unterschiedliche Zugangskanäle gewährleistet sein. Schwerer wiegt jedoch die Tatsache, dass ein solches System das Rahmenwerk hoheitlicher und supra-nationaler Anforderungen und Interessen berücksichtigen und seine kontinuierliche Einhaltung sicherstellen muss. Dies gilt umso mehr, als dass für technisch organisatorische Anforderungen sowie die geforderten Sicherheitsniveaus für nationale und europäische Anerkennung (eIDAS) bisher kein einheitlicher Konsens existiert.

Bisher hielten Hersteller dem Zugriff auf die Sicherheitshardware und den systemintegrierten Anwendungen ihrer Komponenten aus wirtschaftlichen und strategischen Gründen die Hand vor. Die Freigabe erfolgte nur für ausgewählte Partner und vielversprechende Use Cases; dabei gilt etwa die Identifikation und Autorisierung der aktiven Persona als zentrale Infrastruktur für digitale Dienste wie z.B. Mobile Payments. Eine Dienstleistung, die bereits zum festen Geschäftsrepertoire der Hardware-Anbieter avanciert ist.

Das Momentum aus dem aktuellen Paradigmenwechsel der großen Hardware-Anbieter bietet sich an, in einem kooperativen Vorgehen richtungsweisende Grundlagen für technische und regulatorische Standards zu schaffen. Dabei ist die aktive Teilnahme hoheitlicher Stellen an entsprechenden Pilotprojekten von elementarer Bedeutung. Diese können dabei durch

Innovationen privater Initiativen getrieben werden, um kurzfristig prototypische Umsetzungen zu erzielen, die mittels iterativen Verfahrens die praktische Anwendbarkeit sicherstellen.

Diese können zur Absicherung der eigenen, mittelfristigen Gestaltungshoheit von staatlicher Seite begleitet werden. Zur Sicherstellung der Anerkennung auf Nutzerseite kann der Staat eine „Bürgschaft“ für das System übernehmen, in dem die genutzte Infrastruktur als Vertrauensanker durch die hoheitliche Seite zur Verfügung gestellt wird.

Zur möglichen Realisierung des beschriebenen Kooperationsansatzes wird empfohlen dedizierte Sicherungsmaßnahmen zu evaluieren und ggf. zu etablieren:

- Dynamisierung von in kulturell und historischen Erfahrungsmustern gefangenen Strukturen auf Basis zyklischer Rotationen innerhalb etablierter Gremien

- Etablierung und Pilotierung von Public Private Partnership-Modellen in agileren Kontexten mit kürzeren Laufzeiten, exakteren Zielparametern sowie attraktiven jedoch schärferen Bonus- wie Malus-Regelungen

- Übergreifender fachlicher Austausch zwischen Verwaltungs- und Industriestrukturen in kommunikativ geschützten Räumen, (z.B. Chatham House Rules), um freien Informations- und Erfahrungsaustausch zu stimulieren und selbstreferenzielle Argumentationen insbesondere zu vertraulichen und auf wenige Kompetenzträger verteilten Informationen folgenfrei validieren zu können

Identifizierungsanbieter bieten Brückentechnologie zwischen analogen Identitäten (hoheitliches Dokument) und digitalen Diensten; mit zunehmender Verfügbarkeit digitaler Identitäten ist Verlagerung zu Mehrwertdiensten zum Erhalt der Relevanz erforderlich.

Bisher haben Identifizierungsanbieter die Brückentechnologie zwischen analoger Identität (hoheitliches Dokument) und digitaler Authentifizierung gestellt. Getrieben durch die zunehmende Verfügbarkeit digitaler Identitäten auf Basis der Ökosysteme mobiler Endgerätanbieter wird der Markt jedoch mittelfristig einem signifikanten Wandel unterworfen sein.

Bisher herrschte bei Identifikationsdienstleistungen eine Abstufung zwischen unterschiedlichen Identifizierungsniveaus vor, die in Abwägung zwischen Sicherheit und Convenience klassifiziert wurden (z.B. Foto-Ident, AI (Artificial intelligence)-Ident, Video-Ident). Die bisher konträr stehenden Dimensionen Sicherheit und Convenience können jedoch durch die Etablierung digitaler Identitäten, welche direkt in Endgeräte integriert sind, zunehmend miteinander realisiert werden.

Dieser Wandel birgt Potenzial für etablierte Identifizierungsanbieter, das eigene Knowhow und bewährte Lösungen pro-aktiv zum Onboarding für neue, gerätebasierte Produkte anbieten zu können. Dieser Akt kann kurzfristig vollzogen werden, um das eigene Produktportfolio den sich anbahnenden Veränderungen anzupassen. Um mittelfristig eine Schlechterstellung gegenüber

dem Markt zu vermeiden bzw. positiv am Wandel zu partizipieren, sind jedoch tiefgreifendere Anpassungen notwendig. Das aktuelle Umfeld kann zur horizontalen wie auch zur vertikalen Integration genutzt werden, um zukünftig Mehrwertdienste anbieten zu können. Dies umfasst beispielsweise die Aggregation verschiedener Länder, um diese parallel bedienen zu können und bisher technisch unterschiedliche Verfahren zu vereinheitlichen. Additiv bietet sich die Ausweitung auf KYC Prozesse an, so z.B. Sanktions- und PEP-Prüfungen aber auch Unternehmensidentifizierung und qualifizierte elektronische Signatur. Diese Geschäftsfeldverlagerung in Richtung nachgelagerter Prozesse kann als notwendiger Stellhebel zur Vermeidung des direkten Wettbewerbs und Sicherstellung mittelfristiger Marktrelevanz betrachtet werden.

Zur Vermeidung direkter Marktverdrängung und Sicherstellung mittelfristiger Partizipation am digitalen Identitätsmarkt sollte seitens identitätshaltender Unternehmen eine pro-aktive, Plattform-getriebene Marktstrategie in Kooperation mit internationalen Technologiedienstleistern definiert werden.

In etablierten Märkten mit legislatorisch verankerten Anforderungen hinsichtlich der erhobenen, identitätsbezogenen Daten, thematisieren Unternehmen aktuell die Weiterverwendung des intern zur Verfügung stehenden Datenfundaments. Dies trifft insbesondere auf Unternehmen mit Geschäftstätigkeit im Banking oder Versicherungsbereich, zu. Getrieben durch die rasante Entwicklung von Services im Bereich des Identifikation- und Authentifikationsmanagement, stehen diese unter dem Zugzwang sich mittelfristig mit neuen Produkten zu positionieren. Dies wird jedoch getragen durch die per se hohe Qualität der vorhandenen Kunden- und Nutzerdaten. Diese Informationen sind prädestiniert, subsequent komplementäre Geschäftsfälle wie Kreditabschlüsse zu bedienen oder additiv für öffentliche Dienste im Rahmen von eGovernment-Initiativen genutzt zu werden.

Als Referenz kann hierbei auf verschiedene BankID Verfahren verwiesen werden, welche sich durch hohe Convenience und Accessibility auszeichnen und sich damit einer hohen Attraktivität im skandinavischen Raum erfreuen. Diesen Unternehmen ist gemein, dass sie zur Abbildung entsprechender Geschäftsprozesse intern bereits über eine entsprechende Infrastruktur zum gesicherten Abruf (SCA / Strong Customer Authentication) verfügen.

Die Nutzung vorhandener, identifikationsbezogener Daten bietet für den Endnutzer ein signifikant höheres Level an Convenience im Vergleich zur Neu-Identifizierung. Insofern deren Nutzung für die allokierten Services autorisiert ist, können entsprechende Dienstleistungen speditiv und pragmatisch umgesetzt werden.

Diesen Vorteil nutzend, gilt es, seitens Identitätsvorhaltender Unternehmen, vornehmlich der Finanz- und Versicherungsbranche, das derzeitige Handlungsfenster zur profitablen Marktteilnahme des Identitätsmanagements in Form Markt-offener Strategie zu realisieren. Ein gegenläufiger Ansatz geschlossener Systeme und interner Verwendung von Kundeninformationen zu Analysezwecken wird stets durch den abgeleiteten Vertrieb eigener Produkte ohne die Möglichkeit des direkten Profits auf Basis vorgehaltener Identitäten reglementiert sein. Additiv wird dieses Vorgehen durch liberalisierende Marktkräfte fortlaufend unterwandert. Somit gilt es, zur Vermeidung mittelfristiger Marktverdrängung im Umfeld des

digitalen Identitätsmanagements, einen Ansatz föderaler Plattformökonomie und API / Open Banking Strategie zu verfolgen. Als notwendige Voraussetzung aktiver Marktbeteiligung und des möglichen Angebotes von Identitätsinformationen müssen im Vorfeld die erforderlichen, operativen Maßnahmen definiert werden. Auszugsweise gilt es, einerseits die vielfältig organisch gewachsenen Legacy Systeme in Richtung standarisierter Technologien (z.B. OAuth 2.0, OpenID Connect) zur Sicherstellung notwendiger Interoperabilität auszurichten, andererseits die, vornehmlich innerhalb von Großunternehmen aufgrund von z.T. separat etablierter Subprodukte isolierten / lose gekoppelten Identitätssilos innerhalb eines Identitätsmanagementsystems (z.B. keycloak, Auth0, Okta), zu konsolidieren.

Fazit

Die mittelfristig vollumfängliche Digitalisierung sensibler Identitätsinformationen unter Anwendung des Kundenzentrierten, lokalen Datenhaltungskonzeptes und bequemer Wiederverwendung ohne notwendige Neu-Identifizierung wirkt sich disruptiv auf die momentane Marktsituation aus. Derzeitige Strategieausrichtungen des öffentlichen und privaten Sektors müssen zur Vermeidung potentieller Verdrängung aus dem exponentiell wachsenden und höchst profitablen Identitätsmarkt neu kalibriert werden. Hierbei gilt es, frühzeitig und pro-aktiv mit den globalen Technologieanbietern gemeinschaftliche Kooperationsmodelle zu definieren oder die Geschäftsmodelle in Richtung übergreifender Mehrwertdienste zu verlagern.

Quellen

1. Statista 2019 – Value of global digital health market by major segment 2015-2020
2. Statista 2019 – Internet of Things Dossier
3. Javelin Strategy & Research - 2018 Identity Fraud: Fraud Enters a New Era of Complexity
4. Apple Patent 24.10.2019 - Identity credential verification techniques

Artur Burgardt ist Managing Partner bei CORE. Bei CORE konzentriert sich Artur Burgardt unter anderem auf die Konzeptionierung und Implementierung digitaler Produkte. Seine Schwerpunkte liegen in den Bereichen des Identitätsmanagements, innovativer Payment- und Bankenprodukte, moderner Technologien / technischer Standards, Architekturkonzeptionierung und deren Einsatz in komplexen heterogenen Systemumgebungen.

Mail: artur.burgardt@core.se

Maarten Oestreich ist Senior Expert Manager bei CORE. Zu seinen Schwerpunktthemen zählen digitale Identitäten, Authentisierungsverfahren, IT-Management, Produktmanagement, Requirements Engineering, agile Methoden und Design Thinking / User-Centered Innovation. Seine Erfahrungen beziehen sich unter anderem auf die Entwicklung und Einführung einer Micro-Service basierten neuen Systemlandschaft für missionskritische Prozesse in einem internationalen Versicherungsunternehmen**.**

Mail: maarten.oestreich@core.se

Pierre M. Heugle ist Transformation Associate bei CORE. Er hat einen Master in Business Administration und in International Project Managment absolviert. Seine Schwerpunktthemen sind Projektmanagement, Business Intelligence und Prozess- & Qualitätsmanagement. Seine Erfahrungen beziehen sich unter anderem auf die Konzeption und Implementierung eines BI-basierten Reporting-Systems und der Steuerung von Entwicklerteams für diverse Projektmanagement-Tools.

Mail: pierre.heugle@core.se

CORE SE
Am Sandwerder 21-23
14109 Berlin | Germany
https://core.se/
Phone: +49 30 263 440 20
office@core.se

COREtransform GmbH
Am Sandwerder 21-23
14109 Berlin | Germany
https://core.se/
Phone: +49 30 263 440 20
office@core.se

COREtransform GmbH
Limmatquai 1
8001 Zürich | Helvetia
https://core.se/
Phone: +41 44 261 0143
office@core.se

COREtransform Ltd.
Canary Wharf, One Canada Square
London E14 5DY | Great Britain
https://core.se/
Phone: +44 20 328 563 61
office@core.se

COREtransform MEA LLC
DIFC – 105, Currency
House, Tower 1
P.O. Box 506656
Dubai I UAE Emirates
https://core.se/
Phone: +97 14 323 0633