ppi

Digitale Identitäten

Banken positionieren sich als Identitätsanbieter



INHALT

Management Summary 3

Einleitung
Digitale Interaktion erfordert digitale Identitäten 4

Marktüberblick
Aufbruchsstimmung in allen Sektoren 5

Funktionalitäten
Enge Grenzen durch Regulierung 7

Herausforderungen
Es fehlt die kritische Masse 8

Chancen und Lösungsansätze für Banken
Das Potenzial ist vorhanden 11

Fazit
Einen neuen Ansatz wagen 14

Management Summary

- Digitale Identitäten sind aus unserem Alltag nicht mehr wegzudenken. Für Konsumenten, Unternehmen und Behörden bilden sie oftmals die Grundlage für Kommunikation, E-Commerce und E-Government. Zukünftig wird die zunehmende Vernetzung von Geräten und Maschinen im Zeitalter des Internet of Things den Bedarf an sicheren Authentifikationsmechanismen weiter steigen lassen.

- Die Anbieterlandschaft im Bereich Digitale Identitäten ist sehr heterogen. Neben hoheitlichen Verfahren wächst die Zahl kommerzieller ID-Anbieter stetig: Zusätzlich zu Google, Facebook und asiatischen Anbietern wie AliPay oder WeChat drängen Unternehmen unterschiedlichster Branchen auf den Markt.

- Die derzeit vorhandenen ID-Lösungen sind ausschließlich Silos. Kaum eine Applikation hat eine kritische Masse. Der Weg nach vorne kann nur siloübergreifende Interoperabilität sein.

- Die Vielzahl der unterschiedlichen Initiativen und ID-Anbieter auf dem Markt führt zu einer gefühlten Unsicherheit seitens der Nutzer. Vielfach wächst die Befürchtung, dass Daten unkontrolliert weitergegeben werden könnten und die Kontrolle über die eigene Identität verloren geht.

- Kreditinstitute besitzen einen qualitativ hochwertigen Bestand an Personendaten. Sie genießen ein hohes Maß an Vertrauen und sind auch aufgrund ihrer strengen KYC-Prozesse als Anbieter von ID-Lösungen prädestiniert.

- Effizient wäre ein föderiertes System von ID-Providern, das grenzüberschreitend sämtliche Akteure miteinander vernetzen kann. Von einem bank-basierten-Modell können alle an einem ID-Austausch beteiligten Partner profitieren.

Einleitung

Digitale Interaktion erfordert Digitale Identitäten

Online-Dienste sind mittlerweile ein elementarer Baustein unseres digitalen Alltags und begleiten uns in sämtlichen Lebenslagen. Die globale Vernetzung ermöglicht es uns, digitale Dienstleistungen fast überall auf dem Planeten in Anspruch zu nehmen und das rund um die Uhr. In nahezu allen Wirtschaftsbereichen hat die Digitalisierung Einzug genommen und teilweise die klassischen Kommunikationsmedien, Produkt-Absatzkanäle und begleitende Geschäftsprozesse grundlegend verändert. Neue Marktteilnehmer geben mit digitalen Innovationen neue Impulse in etablierten wie auch neuen Wirtschaftszweigen und schaffen es so, sich nicht unerhebliche Marktanteile zu sichern. Oftmals handelt es sich hierbei um kleine Unternehmen, die sich aufgrund ihrer geringen Größe wesentlich besser an sich ändernde Marktgegebenheiten anpassen oder neue Produktideen schneller umsetzen können, als dies alteingesessenen Konzernen mit komplexen Unternehmensstrukturen möglich ist. Insbesondere im Finanzsektor ist in den vergangenen Jahren eine große Anzahl an FinTechs entstanden, die mit innovativen Ideen vorzugsweise an der Kundenschnittstelle den Kreditinstituten Marktanteile abnehmen könnten.

Dort, wo in der Prä-Digitalisierung-Ära eine direkte Interaktion auf persönlicher Ebene zwischen Verbraucher und Händler, Kunde und Bank oder auch Person und Person stattfand, konnten die beteiligten Akteure zweifelsfrei identifiziert werden. Im Rahmen von digitalisierten Geschäftsprozessen ohne direkte persönliche Kontaktaufnahme besteht die Herausforderung in der rechtsverbindlichen Identifikation von an der Kommunikation beteiligten Digitalen Identitäten.

Der Bedarf an rechtsverbindlicher Identifikation ohne persönlichen Kontakt ist da.

Grundlage einer vertrauenswürdigen Digitalen Identität ist heute typischerweise die Verifikation durch lizensierte Ident-Verfahren, wie beispielsweise PostIdent oder VideoIdent. Sie basieren auf der

Überprüfung eines amtlichen Ausweisdokuments durch speziell geschulte Mitarbeiter von Ident-Dienstleistern. Im Rahmen von Online-Identifikationen oder im Bereich des E-Governments kommt der neue Personalausweis (nPA) mit aktivierter eID-Funktion zum Einsatz. Sämtliche Verfahren erfüllen den Zweck der Überführung der physischen in eine virtuelle Identität.

Lizensierte Ident-Lösungen und hoheitliche Verfahren überführen physische Identitäten in die virtuelle Welt.

Doch es existieren nicht nur verifizierte Digitale Identitäten, sondern auch eine Vielzahl mehr oder weniger vertrauenswürdige Identitäten sowie solche mit fehlenden oder falschen Attributen. Nicht nur betrügerische Absichten sind eine Erklärung hierfür, sondern auch das Bedürfnis von Personen nach Privatsphäre und dem Schutz ihrer persönlichen Daten.

Marktüberblick

Aufbruchsstimmung in allen Sektoren

In Europa sind zahlreiche nationale ID-Initiativen zu finden, die sich primär auf dem Gebiet der staatlichen eID-Schemata bewegen und deren Basis in der Regel das nationale Ausweisdokument ist. Zum Einsatz kommen hierbei kontaktbehaftete oder kontaktlose physische Medien, die je nach Ausprägung mit speziellen Kartenlesern oder über die NFC-Schnittstelle von Smartphones und Tablets verwendet werden können. Zusätzlich verbreiten sich digitale Zertifikate, die im Netz rein elektronisch die Identitätsprüfung aus der Ferne erlauben.

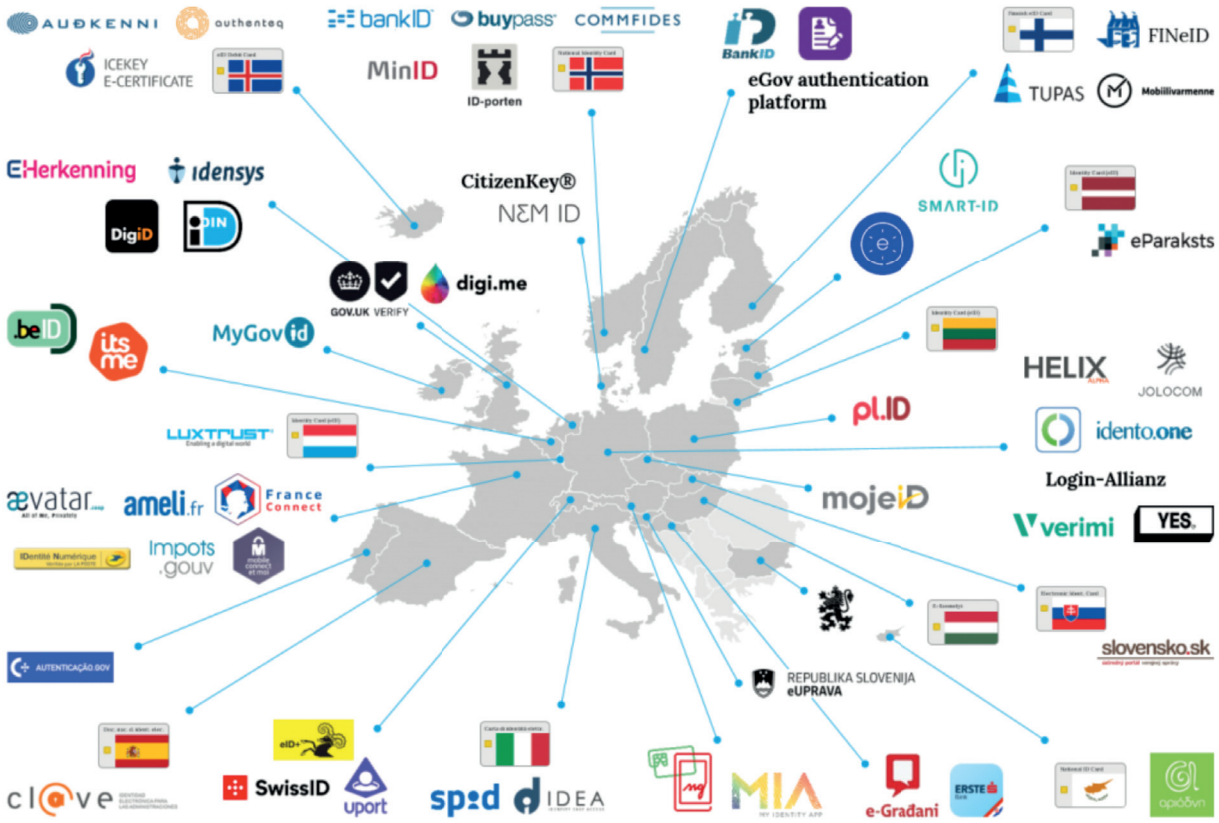
Um eine europaweite Interoperabilität zu gewährleisten, hat die EU im Rahmen der eIDAS-Verordnung Vorgaben erlassen, die eine grenzüberschreitende Nutzung der jeweiligen nationalen virtuellen eIDs ermöglichen soll. Vor allem aber wird der Einsatz von qualifizierten elektronischen Signaturen und darauf basierenden Fernsignaturen, die der handschriftlichen Unterschrift gleichgestellt sind, europaweit einheitlich geregelt.

eIDAS-Verordnung regelt den grenzüberschreitenden Einsatz virtueller Identitäten.

Neben den staatlichen Verfahren wächst der Markt der kommerziellen ID-Anbieter stetig und sorgt für eine Vielzahl individueller Identitätslösungen: Google und Facebook kommt hierbei eine Vorreiterstellung im Segment der Sozialen Medien zu; aktuell versuchen sie, ihre ID-Dienste branchenübergreifend und weltweit zu verankern. Daneben formen sich Gegenpole aus anderen Wirtschaftsbereichen, wie beispielsweise die „Datenallianz“, der Unternehmen aus der TV- und Online-Medienbranche angehören, und den Sparkassen und Genossenschaftsbanken, die bereits eigene ID-Lösungen im Angebot haben oder deren Einführung planen. Auch branchenübergreifende Zusammenschlüsse wie der Dienst VERIMI, dem Unternehmen aus der Finanz-, Automobil-, Reise- und Medienbranche angehören, versuchen zunehmend, Marktanteile zu gewinnen.

Google, Facebook, Datenallianz und branchenübergreifende Zusammenschlüsse kämpfen um Marktanteile.

Überblick europäischer e-Identity-Initiativen und Systeme



Quelle: asquares / Stand: Januar 2018

Darüber hinaus besitzen auch andere internationale Unternehmen – insbesondere aus dem asiatischen Raum – das Potenzial, neben ihrem Kerngeschäft künftig zusätzlich Identitätsdienstleistungen anzubieten. AliPay und WeChat verfügen in ihren Heimatmärkten über sehr hohe Marktanteile, expandieren derzeit weltweit und sind mittlerweile auch in Deutschland einsatzbereit. Hinzu kommt die Möglichkeit, die staatliche chinesische eID mit einem WeChat-Konto zu verknüpfen und somit Identitätsdienste grenzüberschreitend in Anspruch nehmen zu können. Wie bei den GAFA-Unternehmen[1] liegt hier der entscheidende Vorteil in der weiten Verbreitung und hohen Nutzungsquote durch den Anwender.

Asiatische Player punkten mit weiter Verbreitung und hohen Nutzungsquoten.

Funktionalitäten

Enge Grenzen durch Regulierungen

Die über die jeweiligen ID-Provider angebotenen Services ähneln sich in ihren Kernfunktionen. So ist die Grundlage einer jeden Digitalen Identität ein Nutzerprofil, das über mehr oder weniger verifizierte Attribute einer natürlichen Person verfügt und das mit einem Pseudonym als Anmeldename bei einem ID-Provider verknüpft ist. Der Anmeldename kann als universelle Single-Sign-On Benutzerkennung für die Anmeldung an unterschiedlichen voneinander unabhängigen Online-Portalen dienen, sofern sie einheitlichen technischen Standards wie OpenID Connect oder OAuth2 für dieses Vorgehen folgen und die Verknüpfung des jeweiligen Nutzerkontos mit der universellen Kennung unterstützen.

Des Weiteren kann ein Anwender seine bei einem zentralen ID-Provider hinterlegten Daten an angeschlossene Portale weitergeben, um beispielsweise Altersnachweise zu führen, oder sogar verifizierte Identitäten an andere Anbieter weiterzureichen, sodass diese keine erneute Überprüfung der Person mehr durchführen müssen. Hierbei ist allerdings zu berücksichtigen, dass eine nach dem Geldwäschegesetzt (GwG) konforme Weitergabe von Identitäten bislang nur in engen Grenzen möglich ist. Andere Identitätsdienstleister bieten die Verknüpfung der Digitalen Identität mit eIDAS-konformen qualifizier-

Geldwäschegesetz setzt der Weitergabe von Identitäten enge Grenzen.

[1] GAFA: Google, Apple, Facebook, Amazon

ten Signaturen an, um rechtsverbindliche Geschäfte auch grenzübergreifend in der Online-Welt abzuschließen.

Herausforderungen

Es fehlt die kritische Masse

Trotz hoher Anforderungen der EU-DSGVO in Bezug auf Datensicherheit und der regulatorischen PSD2-Vorgaben für Kreditinstitute hinsichtlich der starken Kundenauthentifizierung, steigt nicht zwingend das Vertrauen der Verbraucher in die beschriebenen neuen ID-Initiativen.

Die Vielzahl der unterschiedlichen Initiativen und ID-Anbieter auf dem Markt führt nicht zu einem höheren Sicherheitsempfinden bezüglich der persönlichen Daten oder der eigenen Digitalen Identität. Im Gegenteil wachsen vielmehr Befürchtungen, dass diese Daten unkontrolliert weitergegeben werden könnten und die Kontrolle über die eigene Identität verloren geht – auch weil die vielen virtuellen Anmeldedaten, Sicherungs-PINs oder ähnliches nicht mehr beherrschbar sind. Ein Grund hierfür ist auch die Verwendung einer Digitalen ID als „Ganzes“, obwohl nur einzelne Attribute für den jeweiligen Geschäftsvorfall benötigt werden und die eigentliche personenbezogene Identität oftmals irrelevant ist. Beispiele hierfür sind etwa Altersnachweise für den Erwerb von Gütern, die an ein Mindestalter geknüpft sind. In diesem Fall ist nur das Attribut Alter der Person relevant und nicht deren Name oder Adresse. Oder die Vorlage und oft praktizierte Kopie eines Ausweisdokuments im Hotel, obwohl nur einzelne Attribute der Person für eine Übernachtung benötigt werden und nicht das gesamte Dokument inklusive aller personenbezogenen Daten.

Oftmals werden alle Bestandteile der Digitalen ID preisgegeben, obwohl eigentlich nur einzelne Attribute benötigt werden.

Die auf dem Markt befindlichen ID-Lösungen decken mal weniger, mal mehr Nutzungsfälle ab. Am Ende sind es aber alles Silos. Interoperabilität ist kaum vorhanden – und geschäftspolitisch auch oft nicht gewünscht. Kaum eine Lösung hat eine kritische Masse und sicher wird keine DAS universelle Identitätsverfahren darstellen. Also kann der Weg nach vorne nur siloübergreifende Interoperabilität sein.

Es ist nun absehbar, dass noch weitere Anwendungsfelder – und damit Silos – entstehen. Neben den klassischen Online-Diensten, deren Nutzer natürliche Personen sind, sorgt die zunehmende Vernetzung von Geräten und Maschinen im Zeitalter des Internet of Things für einen steigenden Bedarf an sicheren Authentifikationsmechanismen – nicht nur für Personen, sondern nun auch für den Zugriff und die sichere Identifikation von Geräten, Anwendungen und anderer automatisierter Prozesse ohne Benutzerinteraktion.

Das Internet of Things sorgt für steigenden Bedarf an sicheren Authentifikationsmechanismen.

Wie wir gesehen haben liegt der Fokus bezüglich der Frage „Bin ich berechtigt, auf eine bestimmte Ressource zuzugreifen?“ nicht unbedingt auf der Offenlegung einer kompletten Identität, sondern verschiebt sich in bestimmten Fällen in Richtung Rechte- und Attributeverwaltung, sowohl für Menschen als auch für Anwendungen und Geräte.

Begleitend dazu entsteht ein Bedarf nach intelligenten und risikobasierten Authentifikationsmechanismen, um eine sichere und nutzerfreundliche Authentifikation der Akteure und somit den Zugriff auf Attribute einer Identität sicherzustellen. Dazu zählen nicht althergebrachte Benutzernamen/Passwort-Kombinationen und auch nicht strenge 2-Faktor-Verfahren, wie sie beispielsweise die PSD2 vorschreibt. Die ersten sind zu unsicher oder leicht zu umgehen. Die zweite Lösung wird vom Nutzer oftmals als umständlich angesehen, was in vielen Fällen zum Abbruch eines Vorgangs führt und daraus resultierend zu einer niedrigen Konversionsrate. Gefragt für diesen Einsatzzweck sind vielmehr moderne Varianten wie etwa Verhaltensmustererkennung oder biometrische Verfahren und auch Kombinationen der genannten, gegebenenfalls unter Einbindung weiterer Faktoren wie beispielsweise der Geolokation.

Verhaltensmustererkennung und biometrische Verfahren werden die althergebrachten Authentifikationsmechanismen ablösen.

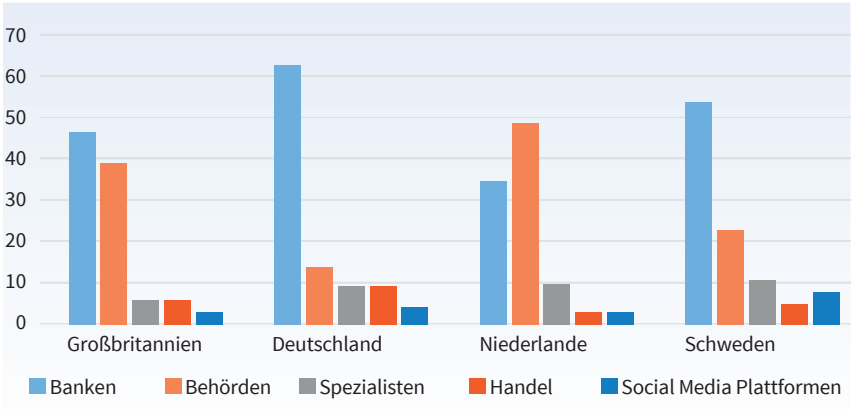
Darüber hinaus spielt der zugrunde liegende Geschäftsvorfall bei der Ermittlung des damit verbundenen Risikos eine Rolle: Eine Altersverifikation, die nur feststellt, ob eine Person volljährig ist, erfordert ein niedrigeres Sicherheitsniveau als eine Kontoeröffnung, bei der eine Vielzahl personenbezogener Daten erhoben werden.

Neben einer hohen Nutzerfreundlichkeit und einem hohen Sicherheitsniveau für zugrundeliegende Geschäftsvorfälle, kommt auch der

Vertrauenswürdigkeit eines Identitätsdiensteanbieters eine wichtige Bedeutung zu. Cyber-Attacken, Datenschutzverstöße, Phishing oder Social Engineering sind keine Ausnahmeerscheinungen, sondern stellen eine alltägliche Bedrohungslage für sämtliche Wirtschaftsbereiche und auch die einzelne Person dar. Kreditinstitute genießen trotz Negativpresse in den vergangenen Jahren in diesem Zusammenhang einen guten Ruf innerhalb der Bevölkerung, der nicht zuletzt auf ein robustes Zahlungsnetzwerk und hohe IT-Sicherheitsmaßnahmen zurückzuführen ist. Ferner gelten für Kreditinstitute hohe Anforderungen, was die Identifikation von Personen betrifft – sowohl vor Aufnahme der Geschäftsbeziehung als auch währenddessen. Hierzu trägt besonders ein strenger KYC-Prozess bei, der auf Grundlage gesetzlicher Regelungen eine Legitimation sämtlicher Kontoinhaber und Bevollmächtigten auf Basis eines amtlichen Ausweisdokuments vorsieht.

Kreditinstitute genießen aufgrund ihres robusten Zahlungsnetzwerks und ihrer hohen IT-Sicherheit einen guten Ruf.

Wen würden Sie als Anbieter Ihrer elektronische Identität (eID) bevorzugen?



Quelle: On-Boarding Report - The Battle to On-board II[2]

[2] https://www.signicat.com/wp-content/whitepapers/signicat-battle-to-onboard-II-v6.pdf

Chancen und Lösungsansätze für Banken

Das Potenzial ist vorhanden

Der KYC-Prozess des Einholens personenbezogener Daten, Verarbeitens, Speicherns und letztlich Aktualisierens in regelmäßigen Abständen ist für Finanzdienstleister zeit- und kostenintensiv. Aber er führt zu einem qualitativ hochwertigen Bestand an Personendaten, der den meisten Kreditinstituten heute nur einem Zweck dient: Erfüllung regulatorischer und gesetzlicher Vorgaben.

Kreditinstitute nutzen ihren qualitativ hochwertigen Bestand an Personendaten nicht konsequent aus.

Insbesondere in der Zeit zunehmender Regulierung ist dies ein großer Ausgabenblock und bietet auf den ersten Blick wenige Chancen, die entstandenen Kosten zu kompensieren oder sogar ein neues Geschäftsfeld zu erschließen. Einige innovative Banken haben aber bereits erkannt, dass der Bestand an GwG-konformen Kundendaten ein großes Potenzial bietet, hieraus einen neuen Geschäftsansatz zu entwickeln, und beteiligen sich, wie in der Einleitung beschrieben, an den ersten ID-Initiativen auf dem Markt. Da bei diesen Initiativen noch ein Silodenken vorherrscht und kein übergreifender Datenaustausch stattfindet, bleibt der Aktionsradius jedoch auf die eigene Sphäre beschränkt. Abhilfe schafft in diesem Zusammenhang nur ein föderiertes System von ID-Providern, das grenzüberschreitend sämtliche Akteure miteinander vernetzt.

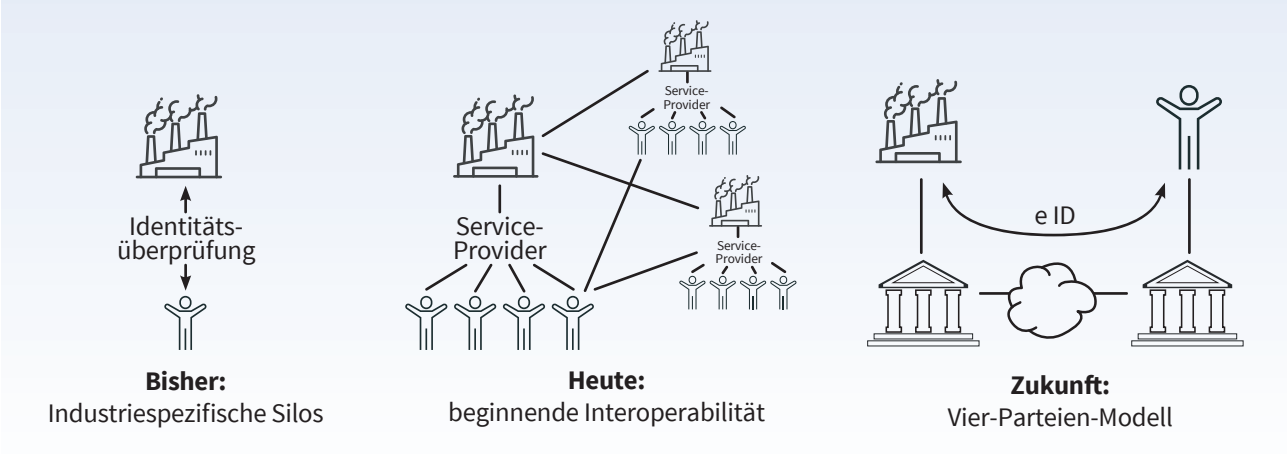
Föderierten Systemen gehört die Zukunft.

Banken erfüllen alle notwendigen Voraussetzungen, ein solches System aufzubauen:

- Legitimierte Personendaten
- Ein robustes, sicheres, internationales Kommunikationsnetzwerk für den Austausch der relevanten Daten
- Modelle zur Zusammenführung aller Akteure (zum Beispiel Broker, 4-Corner)
- Existierende, siloübergreifende Verbindungen zu praktisch allen Personen und Unternehmen

Insbesondere in einem, im ACH-Bereich bewährten Vier-Parteien-Modell können alle an einem ID-Austausch beteiligten Partner profitieren. Personen, die Attribute ihrer Identität bereitstellen möchten, können dies mittels eines Services ihrer Bank vornehmen. Banken erschließen ein neues Geschäftsfeld als ID-Provider, die innerhalb eines etablierten Kommunikationsnetzwerkes ID-Informationen austauschen und sich gegenseitig vertrauen. Zuletzt vertraut eine Attribut anfragende Partei auf die Rückmeldung durch ihre Bank und kann das Geschäft abschließen.

Evolution der ID-Architektur



Quelle: Dr. Michael Salmony, Rethinking digital identity JPSS Journal of Payments Strategy & Systems, Volume 12, Number 1, Spring 2018, pp40-57, Henry Steward Publications

Auf dieser Basis ist eine Integration des bankeigenen ID-Services als optionaler Dienst im Rahmen der Öffnung der Banken für Drittanbieter interessant. Da die PSD2 die Einrichtung einer Schnittstelle für andere Marktteilnehmer vorsieht, können Banken hiervon profitieren und die jeweilige XS2A-Schnittstelle kostenpflichtig im Rahmen ihrer API-Strategie für spätere ID-Services nutzen. Ferner wirkt eine Integration des ID-Services in das Kunden-Frontend einer Bank-Website dem Verlust der Kundenschnittstelle entgegen, da sich Kunden durch die Nutzung von ID-Services enger an ihre Hausbank binden.

Banken können sich Drittdiensteanbietern öffnen und gleichzeitig die eigenen Kunden enger an sich binden.

Die Vorteile eines solchen Ansatzes sind:

- Gewinnbringende Verwertung der eigenen GwG-konformen Identitäten
- Bessere Auslastung des Interbanken-Netzwerkes
- Kompensierende Maßnahme zum Verlust der Kundenschnittstelle
- Banken können einen Gegenpol zu den Internetgiganten[3] schaffen
- Eigene Positionierung als Innovator
- Gute Ausgangsposition für Kreditinstitute durch:
  - Wegfall des Aufbaus eines Kundenstamms
  - Vorhandenes internationales Kommunikationsnetzwerk
  - Hohes Ansehen gegenüber anderen Wirtschaftszweigen in puncto Datensicherheit

Diese vom Leser möglicherweise als recht revolutionäre anzusehende Vorgehensweise ist in manchen Ländern schon gelebte Praxis. In den Nordischen Ländern bietet beispielsweise BankID – ein föderiertes System, das auf Bank-Authentifizierung basiert – die Möglichkeit, für alle anderen Industrien von Handel bis E-Government, Attribute der Nutzer sicher und im Interesse aller zu verifizieren. The future is here.

[3] GAFA (Google, Apple, Facebook, Amazon) und chinesische Anbieter

Fazit

Einen neuen Ansatz wagen

Banken besitzen eine sehr gute Ausgangsbasis, um das Feld der Digitalen Identitäten nicht dem Wettbewerb zu überlassen und ihre Positionen am Markt zu sichern. Sie erfüllen alle notwendigen Voraussetzungen, sich langfristig am Markt mit einem innovativen, sicheren und einheitlichen Identitätskonzept zu etablieren. Allerdings erfordert eine erfolgreiche bankenbasierte ID-Lösung ein gemeinsames, unter den Banken und Kreditinstituten sowie beteiligten Technologiepartnern verbindlich abgestimmtes Vorgehen, um eine zeitnahe Umsetzung zu gewährleisten.

Solch eine Initiative ist kurzfristig anzugehen, da bereits mehrere Initiativen existieren, die mit fertigen Lösungen am Markt sind und zunehmend Marktanteile gewinnen. Fehler bei der Einführung gemeinsamer Projekte aus der Vergangenheit, deren Absicht es war, einen Gegenpol zu einem globalen Bezahlverfahren einzuführen, sollten bei diesem Ansatz ebenfalls eine kritische Würdigung finden, um eine Wiederholung zu vermeiden.

Eine weitere Bedrohung entstammt dem Lager der modernen Bezahlsysteme wie etwa AliPay, WeChat oder Google-/ApplePay, die mehr und mehr die klassischen Bezahlverfahren der Banken ablösen und in den Bereich der Digital Identity Services einsteigen.

Die Zeit ist reif für einen neuen Ansatz. Wagen wir diesen.

Die PPI AG

PPI ist spezialisiert auf Softwareprodukte sowie Consulting im Bereich Zahlungsverkehr und Marktführer für EBICS- und FinTS-Lösungen. Die PPI AG bietet mit ihren Produkten die komplette ZV-Verarbeitungskette für Banken aus einer Hand, angefangen von der Kunde-Bank-Kommunikation, der ZV-Kernverarbeitung bis zur Interbankenkommunikation. Das Consulting-Angebot erstreckt sich von der strategischen sowie der bankfachlichen bis zur IT-Beratung mit ZV-Bezug. PPI berät seine Kunden unter anderem zu den Themen Regulierung (z. B. PSD II), Instant Payments, Individual-, SEPA und kartengestützter Zahlungsverkehr.

Ansprechpartner



René Keller
Senior Consutant
PPI AG
T +49 (0)40 2274331565
M +49 (0)170 4480515
rene.keller@ppi.de

PPI AG
Wilhelm-Leuschner-Straße 79
60329 Frankfurt am Main



Dr. Michael Salmony
Executive Adviser
equensWorldline SE
M +49 (0)172 6867163
michael.salmony@equensworldline.com

equensWorldline SE
Hahnstrasse 25
60528 Frankfurt am Main