Deloitte.

Think mobile first – mit dem Onboarding beginnt die Customer Journey

Medienbruchfrei mit der Online-Ausweisfunktion des Personalausweises und dem Smartphone eine Kontoeröffnung oder einen Kreditantrag legitimieren

Die fortschreitende Digitalisierung und das sich verändernde Konsumentenverhalten verlagern das Bankgeschäft immer stärker in Richtung Online-Services und einer kanalübergreifenden 24/7-Interaktion mit der Bank. Überweisungen lassen sich längst zeit- und ortsunabhängig mit wenigen Mausklicks oder von unterwegs mit dem Smartphone erledigen. Auch die Einbindung weiterer Konten in das Online-Banking ist in wenigen Minuten möglich. Doch spätestens die Identifikation (Legitimation) und die Vertragssignatur sorgen häufig noch für einen Bruch im digitalen Erlebnis der Kunden und verzögern eine voll automatisierte und schnelle Bearbeitung sowohl auf Kunden- als auch auf Bankenseite. Vor dem Hintergrund des KYC-Erfordernisses des Geldwäschegesetzes ist es beim Abschluss eines Verbraucherdarlehensvertrages von zentraler Bedeutung für die Bank, den Antragsteller als Neukunden zu legitimieren und zu authentifizieren. Dafür sind ein Gang zur Bankfiliale oder die Einbindung von Drittanbietern (Post- oder Video-Ident-Verfahren) notwendig. Für die Identitätsprüfung verschafft das Video-Ident-Verfahren als Alternative Abhilfe für den Gang zur Bank- oder Postfiliale. Bei diesem folgt der Nutzer den Anweisungen eines ausgebildeten Mitarbeiters per Videotelefonie. Eine neue, schnellere und benutzerfreundlichere Alternative zum Video-Ident-Verfahren stellt die Online-Ausweisfunktion des Personalausweises in Verbindung mit dem Smartphone dar. Zusätzlich lassen sich auf diese Weise auch Verträge rechtsgültig unterschreiben, was einen schnelleren, medienbruchfreien Abschluss ermöglicht.

Während das Geldwäschegesetz bei der Kontoeröffnung im Rahmen des KYC-Prozesses keine eigenhändige Unterschrift erfordert, ist dies für den Abschluss eines Verbraucherdarlehensvertrages notwendig. Nach § 492 BGB i.V.m. § 126 BGB ist der Vertrag in schriftlicher Form und seitens des Kunden mit eigenhändiger Unterschrift abzuschließen. Die schriftliche Form kann dabei jedoch gemäß § 126 Abs. 3 i.V.m. § 126a BGB durch die elektronische Form ersetzt werden. Bedingungen dafür sind jedoch, dass der Aussteller der Erklärung seinen Namen hinzufügt und beide Vertragsparteien das elektronische Dokument mit einer sogenannten qualifizierten elektronischen Signatur (QES) versehen.

> „Eine qualifizierte elektronische Signatur hat die gleiche Rechtswirkung wie eine handschriftliche Unterschrift."
>
> **Art. 25 Abs. 2 eIDAS-Verordnung**

Die QES bezieht sich dabei auf die Signaturart mit den höchsten Sicherheitsanforderungen im Hinblick auf die Identifizierung des Inhabers. Die Signaturarten werden dabei in der eIDAS-Verordnung (als Akronym für electronic IDentification, Authentication and trust Services, siehe: Rechtlicher Hintergrund) definiert. Die QES ist somit die einzige zulässige Art der digitalen Signatur, die für den Abschluss eines Verbraucherdarlehens rechtsgültig ist. Bis zum Zeitpunkt der Umsetzung der eIDAS-Verordnung war für die rechtsgültige elektronische Signaturerstellung die Anschaffung einer Signaturkarte sowie eines geeigneten Signaturkarten-Lesegeräts notwendig, um sich zu legitimieren und zu authentifizieren. Die Signatur ließ sich somit nur mit der Zuhilfenahme dieser externen Komponenten erstellen. Der Erwerb eben dieser sowie die daraus resultierende vergleichsweise geringe Benutzerfreundlichkeit sind jedoch Gründe für die geringe Nutzung im Privatgebrauch.

eIDAS eröffnet Möglichkeit der Fernsignatur

Mit der eIDAS-Verordnung ist nunmehr die sogenannte Fernsignatur möglich, bei der statt der Signaturkarte, dem Signaturkartenlesegerät und entsprechender Software nur noch folgende zwei Komponenten benötigt werden:

- **NFC-fähiges Smartphone** (bisher nur mit Android möglich)[1] als „Kartenleser" für den elektronischen Identitätsnachweis mit installierter Identitätsnachweis-App
- **Personalausweis** mit aktivierter Online-Ausweisfunktion („electronic Identity", eID) oder elektronischer Aufenthaltstitel

Eine QES wird dann im Auftrag des Unterzeichners durch einen qualifizierten Vertrauensdiensteanbieter (VDA bzw. Qualified Trust Service Provider, QTSP) erstellt. Dafür ist es erforderlich, dass der Nutzer einmalig ein Signaturzertifikat auf seinen elektronischen Personalausweis lädt, was sich in den Prozess einbinden lässt. VDAs weisen die Konformität der von ihnen erbrachten Vertrauensdienste nach, was bedeutet, dass sie für die Identität des Unterzeichnenden bürgen, sodass ein sicherer Rückschluss auf eben diesen gewährleistet ist. Der VDA bindet dabei einen kryptografischen Buchstaben- und Zahlencode über das zu signierende Dokument in das Protokoll der Online-Ausweisfunktion ein, welches der Nutzer durch seinen Ausweis verifiziert. Damit wird sichergestellt, dass das Dokument nach Unterzeichnung nicht mehr geändert wurde. Um die Erlaubnis zu erhalten, qualifizierte digitale Zertifikate bereitzustellen, müssen die Vertrauensdiensteanbieter vorab von einer staatlichen Aufsichtsbehörde geprüft und akkreditiert werden. Ohne in einer von der Europäischen Kommission geführten Vertrauensliste aufgeführt zu sein, sind VDA nicht berechtigt, qualifizierte Vertrauensdienste auszustellen.

Use Case: Identifikation und Signaturerstellung mittels Personalausweis und Smartphone

Um einen finanziellen Engpass kurzfristig zu überbrücken oder beispielsweise bevorstehende Investitionen in Haushaltsgeräte, Mobiliar oder technisches Equipment realisieren zu können, sind häufig Kleinkredite das bevorzugte Mittel. Bei diesen sind neben den Konditionen vor allen Dingen eine schnelle Beantragung und anschließende sofortige Auszahlung entscheidend. Nachdem sich der Nutzer für ein Produkt entschieden hat, gibt er zunächst Informationen zu seinem persönlichen Einkommen ein, um eine Kreditanfrage zu stellen. Nach positiver Prüfung übermittelt die Bank den Kreditvertrag an den Vertrauensdiensteanbieter, welcher ihn dem Kunden auf seinem mobilen Endgerät vorlegt. Im nächsten Schritt lädt sich der Kunde eine Legitimations-App auf sein Smartphone und seine Authentifizierungsanfrage wird an einen eID-Server weitergeleitet. Durch Auflegen seines NFC-Smartphones auf den Personalausweis wird zwischen seinem Personalausweis, seinem Smartphone und der dazugehörigen App ein sicherer Kanal aufgebaut. Das Smartphone fungiert dabei als Kartenlesegerät und die Smartphone-App als Middleware, die den Austausch zwischen Personalausweis, Smartphone und eID-Server herstellt. Um die gegenseitige Authentifizierung von Nutzer und Anbieter zu ermöglichen und dem Nutzer die Berechtigung nachzuweisen, die Ausweisdaten auslesen zu dürfen, wird ihm das vom Diensteanbieter erworbene Berechtigungszertifikat angezeigt. Um sicherzustellen, dass es sich nicht um einen Missbrauch eines gestohlenen Ausweises handelt, wird die Gültigkeit der

[1] Für die Online-Ausweisfunktion wird schreibender Zugriff auf die NFC-Schnittstelle gemäß dem in der ISO-Norm IEC 144443 / -4 definierten Protokoll benötigt, welche aktuell (Stand: März 2019) noch nicht vollständig von Apple freigegeben wurde.

eID-Funktion des Ausweises überprüft. Der Nutzer bestätigt dafür den Umfang und die Übermittlung der erforderlichen Daten durch die Eingabe seiner persönlichen sechsstelligen PIN. Zudem kann ein gestohlener Personalausweis mit einem individuellen Sperrkennwort gesperrt werden. Neben dem Besitz des Ausweises stellt die Eingabe der PIN (Wissen) den zweiten Faktor der Zwei-Faktor-Authentifizierung dar. Nach korrekter Eingabe legt der Nutzer seinen Ausweis auf das NFC-fähige Smartphone. Die Ausweisdaten sowie eine Authentifizierungsantwort werden innerhalb von wenigen Sekunden an den eID-Server über den RFID-Chip im Personalausweis übermittelt. Als ersten Teilprozess lässt sich die Identifikation somit vollständig durch die Verwendung des Personalausweises und des Smartphones durchführen.

Sofern die Identitätsprüfung erfolgreich abgeschlossen ist, beginnt der eigentliche Signaturprozess. Hierfür wird zunächst das vom Vertrauensdiensteanbieter bereitgestellte Zertifikat mit einem persönlichen vergebenen Passwort heruntergeladen und per SMS-TAN aktiviert. Die Identifizierung im Signaturprozess erfolgt durch die Eingabe einer weiteren abschließenden SMS-TAN. Der Vertrag wird so mit einer rechtsgültigen qualifizierten elektronischen Signatur medienbruchfrei unterzeichnet und der Prozess kundenseitig abgeschlossen. Anschließend kann der Kleinkredit aufgrund der geringen Summe automatisch ausgezahlt werden. Sowohl Kunde als auch Bank erhalten nach Abschluss des Kreditvertrages ein signiertes Exemplar per E-Mail. Der gesamte Vorgang dauert nur wenige Minuten und ist unabhängig von den Bearbeitungszeiten des Video-Ident-Callcenters und möglichen Wartezeiten zu Stoßzeiten.

Im beschriebenen Verfahren werden also die Identifizierung des Nutzers (zur Ausstellung eines qualifizierten elektronischen Signatur-Zertifikates) sowie die Authentifizierung (zur Autorisierung der Signaturerstellung durch den Vertrauensdiensteanbieter) miteinander verknüpft, womit sichergestellt wird, dass die identifizierte Person identisch mit der Person ist, welche ihre Zustimmung zum Unterzeichnen gegeben hat. In anderen Verfahren werden diese Vorgänge noch getrennt umgesetzt, indem die Identifikation über Post- oder Video-Ident durchgeführt wird. Dies führt zu Medienbrüchen und ist zeitaufwendig. Zudem erhöht diese Art der Identifizierung vor dem Hintergrund der in der Regel einmaligen bzw. nur seltenen Kreditanfrage die Benutzerfreundlichkeit gegenüber der bisher notwendigen Anschaffung der nun nicht mehr benötigten Komponenten.

Rechtlicher Hintergrund

Mit dem Ziel, einen einheitlichen EU-Rahmen für vertrauenswürdige elektronische Geschäftsprozesse und eine Nachvollziehbarkeit von elektronischen Transaktionen zwischen Bürgern, Unternehmen und Behörden zu ermöglichen, hat der Rat der Europäischen Union die eIDAS-Verordnung erlassen. Als unmittelbar geltendes Unionsrecht bedarf die eIDAS-Verordnung hinsichtlich ihrer materiellen Vorschriften keiner Umsetzung in nationales Recht, wird in Deutschland jedoch durch das Vertrauensdienstegesetz ergänzt und präzisiert. Dieses löste das bis 29.07.2017 geltende Signaturgesetz ab. Mit der eIDAS-Verordnung kam es zu einer EU-weiten Harmonisierung und Standardisierung der elektronischen Signaturen.

Die eIDAS-Verordnung definiert in Art. 3 Nr. 10–12 folgende Formen von elektronischen Signaturen:

- Bei der (einfachen) elektronischen Signatur handelt es sich um Daten in elektronischer Form, die anderen elektronischen Daten beigefügt oder logisch mit ihnen verbunden werden und die der Unterzeichner zum Unterzeichnen verwendet. Sie dient dabei jedoch nicht der Identifikation einer Person.
- Die fortgeschrittene elektronische Signatur ist eine Signaturart, die unter anderem eindeutig dem Unterzeichner zugeordnet werden kann und die Identifizierung des Unterzeichners ermöglicht.
- Die qualifizierte elektronische Signatur (QES) ist eine fortgeschrittene elektronische Signatur, die von einer qualifizierten elektronischen Signaturerstellungseinheit erstellt wurde und auf einem qualifizierten Zertifikat für elektronische Signaturen beruht.

Die Gleichstellung der handschriftlichen mit der qualifizierten elektronischen Signatur schafft dabei die rechtliche Grundlage für benutzerfreundliche, medienbruchfreie Signaturprozesse.

Vorteile für Kunden und die Bank

Als schnelle und sichere Alternative zum Video-Ident-Verfahren bietet die Identitätsfeststellung mittels eID und Smartphone-App somit folgende Vorteile:

- **Rechtskonformität:** Das Verfahren ist Geldwäschegesetz-, Zahlungsdienste-aufsichtsgesetz- und eIDAS-konform sowie BSI-zertifiziert.
- **Grundsatz der Datensparsamkeit:** Vor dem Grundsatz der Datenminimierung personenbezogener Daten, wie ihn die DSGVO fordert, können die relevanten Datenfelder aus dem Personalausweis spezifisch definiert werden.
- **Zeit- und Ortsunabhängigkeit:** 24/7-Verfügbarkeit, keine Bindung an die Öffnungszeiten der Post- oder Bankfiliale oder des Video-Ident-Callcenters.
- **Schnelligkeit:** Die Daten werden per NFC in Sekundenschnelle übertragen, weshalb die eID-Legitimation schneller als das Video-Ident-Verfahren funktioniert. Auf Endkundenseite kann durch die Vermeidung von Stoßzeiten mit langen Wartezeiten der gesamte Onboarding-Prozess in wenigen Minuten durchgeführt werden. Für die Bank lassen sich damit Prozessdurchlaufzeiten massiv reduzieren und automatisieren.
- **Skalierbarkeit:** Da der Prozess ohne menschliche Interaktion eines Mitarbeiters stattfindet, ist diese Art der Identifikation nahezu unendlich skalierbar.
- **Kosteneinsparung:** Die Gebührenmodelle, die für die Nutzung eines VDA in Rechnung gestellt werden, sind deutlich geringer als die von externen Video-Ident-Callcentern. Darüber hinaus lassen sich im Vergleich zum klassischen Verfahren mit Gang zur Bank oder Postfiliale oder dem Postident-Verfahren Papier-, Porto- und Verwaltungskosten verringern. Für den Endkunden ist das Verfahren kostenlos.
- **Unabhängigkeit von Video-Ident-Callcentern:** Hier ist zum einen keine Ausbildung von eigenen Mitarbeitern in internen Callcentern zu Ident-Spezialisten notwendig. Zum anderen ist der Service unabhängig von Öffnungszeiten und Preisanpassungen des Callcenters.
- **Sicherheit:** Durch die Akkreditierung der Vertrauensdiensteanbieter wird eine hohe Sicherheit gewährleistet. Zudem findet eine Zwei-Faktor-Authentifizierung, wie sie die PSD2 mit dem Ziel der höheren Sicherheit für Endanwender fordert, statt.
- **Medienbruchfreiheit:** Die vollständig digitale Prozessdurchführung erhöht zum einen die Customer Experience und verhilft der Bank zum anderen bei ihren Digitalisierungszielen.

Die genannten Vorteile führen in der Summe zu geringeren Eintrittsbarrieren, einer niedrigeren Absprungrate im Onboarding-Prozess sowie zu einer gesteigerten Conversion Rate und erhöhten Kundenzufriedenheit.

Ausblick

Durch die intuitive Customer Experience und die einfache Bedienung ist das E-Ident-Verfahren 24/7 und für alle Vertragsabschlüsse und Prozesse mit Identifikationsnotwendigkeit einsetzbar und beschleunigt die Durchführung. Auch am Point of Sale kann das Kreditinstitut den Onboarding-Prozess durch vollautomatisiertes Auslesen der Ausweisdaten im Vergleich zur manuellen Anlage der Kundenstammdaten beschleunigen. Das Onboarding via eID und Smartphone-App lässt die digitale und physische Welt somit weiter zusammenwachsen und stellt einen weiteren Meilenstein für eine vollständig automatisierte Prozessbearbeitung dar. Schon heute sind über 56 Mio. neue Personalausweise und 8 Mio. elektronische Aufenthaltstitel mit neuester Technologie im Umlauf. Bei Behörden lässt sich die Online-Ausweisfunktion bereits für zahlreiche Bürgerservices nutzen, wie beim Onlineabruf der Rentenauskunft, der Registrierung bei ELSTER, beim Beantragen eines Führungszeugnisses oder der Fahrzeugzulassung. Zudem hat die Bundesregierung bereits 2017 einen Gesetzesentwurf zur Förderung des elektronischen Identitätsnachweises angenommen, sodass seitdem jeder neue Personalausweis künftig mit einer einsatzbereiten Funktion zum elektronischen Identitätsnachweis ausgegeben wird. Für alle Geldwäschegesetz-regulierten Märkte wie Banken, Zahlungsdienstleister und Versicherer sind weitere Einsatzfelder denkbar, wie z.B. bei der Konto- oder Depoteröffnung oder dem Abschluss einer Versicherung. Deshalb ist zu erwarten, dass auch die Zahl der Banken und Finanzdienstleister, die diese Lösungen einsetzen, steigen wird und es zu einer höheren Breitenwirkung und Marktdurchdringung kommt.

Abb. 1 – Schematischer Kreditprozess mittels Fernsignatur

Da es sich beim Verwendung der eID-um ein sicheres Verfahren handelt, was im Vergleich zum bereits etablierten Video-Ident-Verfahren entscheidende Vorteile bezüglich der Skalierbarkeit, Zeitunabhängigkeit und Geschwindigkeit bietet, ist davon auszugehen, dass Breitenwirkung und Nutzerzahlen weiter steigen werden. Durch eine nachhaltig effiziente Einführung der Legitimation und Authentifizierung via eID und Smartphone wird ein weiterer Schritt für eine End-to-End-Automatisierung ermöglicht, wodurch auch die Kundenzufriedenheit maßgeblich gesteigert werden kann. Doch hierbei ist vor allem ein intuitiver Anmeldeprozess entscheidend, um Neukunden zu gewinnen und Onboarding-Abbrüche zu reduzieren.

Wie kann Deloitte dabei unterstützen?

Damit eine besonders anwenderfreundliche Integration der eID und der QES in Ihre Geschäftsprozesse gelingt, empfehlen wir ein dreistufiges Verfahren: Eine umfassende Ist-Analyse, mit der es uns gelingt, den Reifegrad der ausgewählten Prozesse zu ermitteln und etwaige Optimierungspotenziale zu identifizieren, die Ableitung und Bewertung von Maßnahmen sowie die vollumfängliche Begleitung im Rahmen der Umsetzungsphase bis hin zum Go-Live.

1. Ist-Analyse

Für eine möglichst effiziente Implementierung der Identifizierung via eID und der qualifizierten elektronischen Signatur in der bestehenden Prozesslandschaft, bedarf es eines initialen ganzheitlichen Open Banking Readiness Assessment. Dabei werden in Form von Prozessanalysen und Workshops der Aufwand und etwaige Maßnahmen untersucht, die für eine Implementierung notwendig sind. Die Ergebnisse des Open Banking Readiness Assessment werden hierbei für die nächsten Projektphasen zusammengefasst und aufbereitet. In der Konzeptionierungsphase wird dann ermittelt, an welcher Stelle die Daten aus dem elektronischen Personalausweis ausgelesen werden und wie mit diesen Daten umgegangen wird (z.B. bei politisch exponierten Personen vor dem Hintergrund des GWG). Zudem wird evaluiert, ob die Einbindung eines Drittanbieters, das Outsourcen des Verifikationsprozesses oder der eigene Aufbau der Infrastruktur empfehlenswerter sind, um die Dienstleistung Wettbewerbern kostenpflichtig anzubieten.

2. Ableitung und Bewertung von Maßnahmen

In der zweiten Phase werden die gewonnenen Erkenntnisse genutzt, um daraus Maßnahmen abzuleiten und diese anschließend zu priorisieren. Gerne unterstützen wir Sie bei der Make-or-Buy-Entscheidung, ob die notwendige Infrastruktur selbst aufgebaut werden soll, um diesen Service als ID-Verification-as-a-Service-Modell entgeltpflichtig auch anderen Unternehmen bereitzustellen oder auf einen bereits etablierten Anbieter zurückgegriffen werden sollte. Im Fall des Fremdbezugs unterstützen wir Sie bei der bei der Auswahl eines geeigneten Integrationspartners.

3. Umsetzung und Go-Live

Nachdem sich für ein Modell entschieden wurde, begleiten wir Sie bei der gesamten Umsetzungsphase bis hin zur technischen Implementierung bzw. dem Go-Live. Dabei wird sichergestellt, dass die Implementierung einen nachhaltigen Mehrwert in Form von Kosteneinsparungen, Prozessautomatisierungen und Unabhängigkeit von Callcentern generiert.

Unser Ansatz ist agil und multidisziplinär: Neben einer effizienten und ressourcenschonenden Methodik und Vorgehensweise bringen wir die notwendige regulatorische, prozessuale und technologische Kompetenz ein. Lessons learned aus zahlreichen Projektdurchführungen unterstreichen die größtmögliche Umsetzungskompetenz von Deloitte.

Wir sind gerne Ihr kompetenter Sparringspartner.

Ihre Ansprechpartner

Frank Thiele
Partner
Financial Services Solutions
Tel: +49 (0)511 3023 3306
Mobil: +49 (0)173 6114 657
fthiele@deloitte.de

Jano Koslowski
Director
Financial Services Solutions
Tel: +49 (0)211 8772 3127
Mobil: +49 (0)173 6163 339
jkoslowski@deloitte.de

Wolfgang Raudaschl
Senior Manager
Financial Services Solutions
Tel: +49 (0)89 29036 7986
Mobil: +49 (0)151 5800 4416
wraudaschl@deloitte.de

Deloitte.

Stand 07/2019