RISIKOBASIERTE UND ADAPTIVE AUTHENTIFIKATION – EINE KARTENBASIERTE ZAHLUNGSDIENSTLEISTUNG FÜR BANKEN IM KONTEXT VON PSD2

Master Thesis

Zürcher Fachhochschule

HWZ Hochschule für Wirtschaft Zürich

eingereicht bei:

Ralph Hutter / Executive MBA

vorgelegt von: Santosh M. Ritter

Matrikelnummer: 02-594-547

Studiengang:

Ort, Datum: Zürich, 25. Oktober 2019

MANAGEMENT SUMMARY

Der Markt für kartengebundene elektronische Zahlungen befindet sich aufgrund der Digitalisierung von Produkten und Prozessen, neuen Informationstechnologien, dem Markteintritt von neuen Mitbewerbenden sowie neuen Gesetzen und Regulierungen im Umbruch. Die Entwicklungen bringen Chancen für neue Produkte und Geschäftsmodelle mit sich, gleichzeitig aber auch neue Risiken. Angriffe auf Zahlungssysteme sind für Kriminelle, trotz dem Einsatz von modernen Risikobewertungs- und Betrugsbekämpfungstechnologien, nach wie vor lukrativ. Im Stationärhandel konnte in den letzten Jahren durch die Einführung der mit einem Sicherheitschip ausgestatteten Zahlkarten die Anzahl Betrugsfälle signifikant reduziert werden. Gleichzeitig hat der Zahlkartenbetrug jedoch durch die steigende Anzahl von Betrugsfällen im Internet stark zugenommen.

Obwohl es mittlerweile eine grosse Anzahl an Angriffsvektoren gibt, welche technisch sehr ausgefeilt sind, spielt das Ausspähen und Stehlen von Benutzerinformationen und Passwörtern nach wie vor eine wichtige Rolle bei der Internetkriminalität. Banken stehen vor der Herausforderung, dass sie bei elektronischen Zahlungen im Internet, die Identitäten der Zahlungsdienstnutzenden nur schwer überprüfen können. Rund um die Identifizierung und Authentifizierung von Personen im Internet gibt es diverse neue Initiativen, Gesetze und Regelungen, welche alle das Ziel haben, die Sicherheit von elektronischen Vorgängen, wie beispielsweise eine Zahlung im Internet, sicherer zu machen.

Ein Ansatz ist dabei, die Anzahl der unsicheren digitalen Identitäten zu reduzieren, indem ein Rahmenwerk geschaffen wird, welches die Ausstellung eines staatlich anerkannten elektronischen Identifikationsmittels unterstützt. Eine E-ID ermöglicht der Inhaberin oder dem Inhaber einerseits, sich bei Behördengängen im Internet auszuweisen, andererseits kann die E-ID für die Anmeldung bei Internetplattformen und Internethändlern genutzt werden. Die überarbeitete Richtlinie für Zahlungsdienste (PSD2) verpflichtet europäische Finanzinstitute grundsätzlich, eine starke Kundenauthentifizierung durchzuführen, bevor der effektive Zahlprozess initiiert wird. Schweizer Banken sind durch PSD2 nicht reguliert. Da der Schweizer Finanzplatz im internationalen Wettbewerb steht und die meisten Finanzinstitute auch Kund/innen aus EU-Mitgliedstaaten betreuen, ist es wichtig, dass die Regelungen bezüglich starker Kundenauthentifizierung nach dem Best-Effort-Ansatz umgesetzt werden.

Im kartengebundenen elektronischen Zahlungsverkehr dient dazu das EMVCo-3D-Secure-Protokoll, womit Informationen von der Akzeptanzstelle zur Kartenherausgeberin übermittelt werden. Anhand der gelieferten Informationen kann die Kartenherausgeberin entscheiden, ob eine starke Kundenauthentifizierung erforderlich ist oder ob eine Zahlungstransaktion aufgrund einer tiefen Risikoeinschätzung ohne zusätzliche Kundeninteraktion abgewickelt werden kann. Entscheidend für die Kundenakzeptanz einer starken Authentifizierungsmethode sind einerseits Sicherheitsüberlegungen bezogen auf das Verfahren selber, andererseits auch auf den Schutz der Daten und die Privatsphäre.

Genauso wichtig ist aber das Kundenerlebnis; Methoden, welche bequem und gleichzeitig sicher sind, werden sich am Markt durchsetzen. Künftig werden neue biometrische Verfahren und Authentifizierungsmethoden eine noch wichtigere Rolle spielen. Entscheidend wird sein, dass es den Finanzinstituten rechtzeitig gelingt, ihren Kund/innen neue innovative Authentifizierungsmethoden zur Verfügung zu stellen, um so den Zahlungsverkehr im Internet noch sicherer und bequemer zu gestalten. Der risikobasierte und adaptive Authentifizierungsservice, welcher in dieser Arbeit vorgestellt wird, erfüllt alle der genannten Kriterien und Anforderungen und kann für eine Bank zu einem entscheidenden Wettbewerbsfaktor im Zahlungsverkehr werden.

INHALTSVERZEICHNIS

EHRENWÖRTLICHE ERKLÄRUNG

Ich bestätige hiermit, dass ich

- die vorliegende Thesis selbständig und ohne Benützung anderer als der angegebenen Quellen und Hilfsmittel anfertigte,
- die benutzten Quellen wörtlich oder inhaltlich als solche kenntlich machte,
- diese Arbeit in gleicher oder ähnlicher Form noch keiner Prüfungskommission vorlegte.

Ort, Datum

.....

(Unterschrift)

VORWORT

Die Zeit während des Masterstudiums in Banking & Finance an der Hochschule für Wirtschaft war sehr spannend, intensiv und lehrreich. Ich bedanke mich ganz herzlich bei all den Menschen, welche mich in den letzten zweieinhalb Jahren, insbesondere während der Entstehung meiner Masterarbeit, begleitet und unterstützt haben. Mein spezieller Dank gilt:

- Anna Storchenegger
- Constantino Lanni
- Daniel Anders
- Gaetano Mecenero
- Herbert Bucheli
- Kenan Calgin
- Magdalena Jaworski
- Manuel Villiger
- Ralph Hutter
- Stefan Leuthold
- Thomas Müller
- Thomas Weber
- Viton Vitanis

Der grösste Dank gebührt aber meiner Frau und meinen beiden Kindern, welche in den letzten beiden Jahren oft auf mich verzichten mussten. Danke für die grosse Unterstützung, ohne euch hätte ich es nicht geschafft! Ich freue mich darauf, künftig wieder mehr Zeit mit euch verbringen zu können.

Bezeichnungen, die Personen betreffen, sind in der vorliegenden Arbeit immer geschlechtergerecht in Form von Beidbenennungen oder geschlechtsneutralen Ausdrücken. Handelt es sich jedoch um Institute oder Unternehmen, wird nur die männliche (bspw. Händler) oder die weibliche Form (Kartenherausgeberin) verwendet. Englische Begriffe (bspw. Cardholder) für Personen gelten sowohl für das weibliche als auch das männliche Geschlecht.

Alle in dieser Arbeit angeführten englischen und deutschen Fachbegriffe werden innerhalb der Kapitel definiert und erläutert. Deshalb existiert kein separates Glossar.

1 EINLEITUNG

1.1 AUSGANGSLAGE, FORSCHUNGSPROBLEM UND -FRAGE

Die strategische Bedeutung des elektronischen Zahlungsverkehrs hat in den letzten Jahren stark zugenommen infolge stärkerer Serviceorientierung, der Entwicklungen in der Informationstechnologie und zunehmender Anforderungen bezüglich Sicherheit und Compliance. Der Markt für elektronische und mobile Zahlungen verändert sich aufgrund der Internationalisierung sowie Digitalisierung von Produkten und Prozessen rasch und unaufhaltsam. Durch das Aufkommen von neuen Zahlungsarten, Zahlungsdiensten, Mitbewerbenden und regulatorischen Vorschriften sind Banken gefordert, ihre Wertschöpfungsketten im Zahlungsverkehr zu optimieren. Dabei besteht oft ein Zielkonflikt zwischen der Serviceorientierung, welche eine Differenzierung und Individualisierung von Produkten und Dienstleistungen erfordert, und dem Druck, Produkte und Prozesse möglichst kosteneffizient zu gestalten und zu automatisieren, um sinkende Gewinnmargen zu verhindern.

Obwohl Bargeld in der Schweiz immer noch das meistgenutzte Zahlungsmittel ist, stieg die Zahl an kartenbasierten Zahlungstransaktionen in den letzten Jahren stark an. Beim bargeldlosen Zahlen gilt die Debitkarte als beliebtestes Zahlungsmittel. Mit den in der Schweiz am stärksten verbreiteten Debitprodukten wie Maestro (Mastercard) sowie V-Pay (Visa) können jedoch keine Online-Zahlungen im Internet getätigt werden. Für sogenannte Distanzzahlungen (E-Commerce) werden daher in der Schweiz häufig Kredit- oder Pre-Paid-Karten eingesetzt. Den Herausforderungen im Produktportfolio begegnen Banken zudem in letzter Zeit vermehrt mit dem Einstieg in Debitprodukte, welche Distanzzahlungen ermöglichen, wie beispielweise Mastercard Debit oder Visa Debit. Mobile Zahlverfahren wie Zahlungen mittels einer auf dem Mobiltelefon integrierten Applikation (In-App-Zahlungen) sowie die Anwendung von mobilen Zahlverfahren im Präsenzgeschäft (POS-Zahlungen) tragen durch immer häufigere Nutzung ebenfalls zum starken Wachstum des kartenbasierten Zahlungsverkehrs bei. Eine Weiterentwicklung der Zahlungsverfahren, welche auf der Vernetzung zwischen Menschen und Geräten basieren wie „Mobile Payment“, sind sogenannte Internet-of-Things-Zahlungen (IoT-Zahlungen), bei denen Maschinen untereinander Leistungen verrechnen, Zahlungen ausführen und Zahlungen annehmen (Machine-to-Machine Payment, M2M Payment).

Die neuen technologischen Möglichkeiten bergen jedoch auch Risiken. Die technischen und rechtlichen Herausforderungen, um das bargeldlose Zahlen einerseits sicher, andererseits auch so bequem wie möglich zu gestalten, sind enorm. Laut dem von Europol 2019 veröffentlichten Bericht „Internet Organised Crime Threat Assessment“ (IOCTA) gehört der sogenannte Card-Not-Present-Betrug (CNP-Betrug) nach wie vor zu den wichtigsten und häufigsten Bedrohungsszenarien im Cyber-Raum. Die Angriffsvektoren reichen dabei von sophistizierten Verfahren, welche auf Künstlicher Intelligenz (KI) und Machine Learning beruhen, bis hin zu einfachen Techniken, bei denen ahnungslose Opfer aufgrund eines „Phishing-E-Mails“ den Kriminellen Zugangsdaten zu ihren Zahlkonten gewähren. Durch CNP-Betrug werden unter anderem Aktivitäten rund um illegale Immigration, meist Menschenhandel und Menschenschmuggel finanziert, indem die Kriminellen mittels kompromittierter Kartendaten Flugtickets sowie Hotel- und Fahrzeugreservationen bezahlen. Banken fällt es aufgrund der technologischen Entwicklung zunehmend schwerer, ihre Kund/innen korrekt zu authentifizieren und mutmassliche Betrüger/innen zu entdecken. Trotzdem müssen sie

in der Lage sein, durch geeignete technische und organisatorische Massnahmen einen rechtssicheren Status von Transaktionen sicherzustellen sowie die Datensicherheit und den Datenschutz zu gewährleisten. Es erstaunt daher nicht, dass zahlreiche Schweizer Banken, trotz zunehmender strategischer Bedeutung, Teile des Zahlungsverkehrs an Zahlungsspezialisten ausgelagert haben.

In der Europäischen Union (EU) gilt seit Januar 2018 die zweite Zahlungsdiensterichtlinie, besser bekannt unter dem englischen Namen „Payment Services Directive 2“ (PSD2). Diese regelt unter anderem, welche Sicherheitsvorkehrungen bei Zugriffen auf ein Zahlungskonto sowie bei der Ausführung von Zahlungen getroffen werden müssen. Die Schweiz als Nichtmitglied der EU und des Europäischen Wirtschaftsraumes (EWR) ist durch die Regulierung nicht direkt betroffen und muss daher das Regelwerk nicht in geltendes Schweizer Recht umsetzen. Die Schweizer Banken befinden sich jedoch in einem internationalen Wettbewerb und betreuen häufig auch europäische Kund/innen. Bei einem allfälligen Rechtsstreit zwischen europäischen Kund/innen und einer Schweizer Bank dürfte künftig PSD2 zur Anwendung kommen. Daher hat die Richtlinie indirekt für den hiesigen Finanzplatz eine grosse Relevanz. Zudem ist es denkbar, dass internationale Kartennetzwerke wie Mastercard oder Visa künftig die Regeln bezüglich der starken Kundenauthentifizierung im gesamten europäischen Raum vereinheitlichen und die Schweiz hier ebenfalls indirekt angehalten ist, Teile der PSD2 zu übernehmen.

Die vorliegende Masterarbeit beschäftigt sich im Wesentlichen mit den folgenden Forschungsfragen:

- Wie könnte ein möglicher innovativer und PSD2-konformer Authentifizierungsservice aussehen, welcher es den Banken ermöglicht, ihre Kund/innen beim Zugriff auf Kartenzahlungskonten sowie bei der Auslösung von kartenbasierten Zahlungen auf eine bequeme und sichere Art zu authentifizieren?
- Welche Verfahren sind geeignet, um während der Authentifizierung ein möglichst gutes Kundenerlebnis zu schaffen bei einem möglichst hohen Sicherheitsniveau?

1.2 Zielsetzungen, inhaltliche Abgrenzung, Aufbau

Ziel dieser Arbeit ist es, einen digitalen PSD2-konformen Service zu entwickeln, welcher es den Banken oder ihren „Outsourcing-Partner/innen“ erlaubt, Kund/innen durch ein risikobasiertes und adaptives Verfahren zu authentifizieren. Das Risiko besteht grundsätzlich darin, dass sich Drittpersonen unbefugt Zutritt zu Zahlungskonten verschaffen und Zahlungen auslösen, welche nicht durch Kund/innen autorisiert wurden. Die risikobasierte und adaptive Authentifizierung verwendet die Wahrscheinlichkeit P(A) mit A = X hat R erstellt (Mass der Authentizität) als Eingabeparameter E für die dynamische Ermittlung der benötigten Verfahren zur ID-Verifikation und Authentifikation. Die Sicherheitsanforderungen an die auszuwählenden Verfahren sind proportional zur Gegenwahrscheinlichkeit von P, also $P(\bar{A})$ mit $\bar{A}$ = X hat R nicht erstellt (Riedel & Pohlmann, 2018, S. 362). Mögliche Eingabeparameter können unter anderem Transaktionsbetrag, Ort und Uhrzeit zum Zeitpunkt der Transaktion, Internet-Protokoll-Adressen (IP-Adressen) oder unbekannte Begünstigte sein.

Der Service basiert auf dem EMVCo-3-D-Secure-Protokoll und soll so konzipiert werden, dass bei einer tiefen Risikoeinschätzung keine zusätzliche Interaktion mit den Kund/innen notwendig ist, da sämtliche Authentifizierungsschritte im Hintergrund automatisch abgewickelt werden. Bei ei-

ner höheren Risikoeinschätzung wird eine Interaktion über eine benutzerfreundliche Methode angestrebt. Der Service soll zudem den hohen Identity- & Access-Governance-Anforderungen von Banken entsprechen.

Diese Arbeit fokussiert auf Vorgänge, welche bei einem Zugriff (Login) auf ein Zahlungskonto stattfinden, oder bei Vorgängen, welche im Zusammenhang mit der Zahlungsauslösung erfolgen. Sie ist aus der Sicht eines Dienstleisters verfasst, welcher im Auftrag der Schweizer Banken die Abwicklung von kartenbasierten Zahlungen vornimmt. Die effektive Zahlungsabwicklung (Autorisierung, Clearing und Settlement) steht aufgrund der zusätzlichen Komplexität des Themengebietes nicht im Fokus der vorliegenden Arbeit.

Nach der Einleitung (Kapitel 1) folgen in Kapitel 2 die theoretischen Grundlagen, um eine Basis für das Verständnis der Forschungsfragen sowie des empirischen Teils in Kapitel 4 zu schaffen. Kapitel 3 beschreibt die Methodik der vorliegenden Arbeit, insbesondere hinsichtlich der Befragung von acht Proband/innen. In den Schlussfolgerungen (Kapitel 5) werden die wichtigsten Erkenntnisse zusammengefasst, die Forschungsfragen beantwortet und Empfehlungen für die Praxis abgegeben.

2 THEORETISCHER TEIL

2.1 DIE RICHTLINIE ÜBER ZAHLUNGSDIENSTE IM EUROPÄISCHEN BINNENMARKT (PSD2)

Auf Vorschlag der Europäischen Kommission hat das Europäische Parlament und der Rat der Europäischen Union die Richtlinie (EU) 2015/2366 über Zahlungsdienste im Binnenmarkt erlassen und am 25. November 2015 im Amtsblatt der Europäischen Union publiziert. Mit dem Inkrafttreten der unter dem englischen Begriff „Revised Payment Services Directive (PSD2)“ bekannten Richtlinie am 13. Januar 2018 wurde gleichzeitig die erste Richtlinie zu Zahlungsdiensten 2007/64/EG aufgehoben. Sie ist innerhalb des Europäischen Wirtschaftsraumes (EWR), welcher die Europäischen Union (EU) und die Länder Norwegen, Lichtenstein und Island umfasst, anwendbar. Wie bereits in der Einleitung erwähnt, ist die Schweiz nicht Mitglied der EU und des EWR und somit nicht durch PSD2 reguliert.

Durch die Harmonisierung einer Vielzahl von unterschiedlichen Rechtsvorschriften der verschiedenen Mitgliedstaaten sowie die Aufhebung der Zahlungsverkehrsmärkte, die entlang nationaler Grenzen aufgeteilt sind, sollen Regulierungslücken entfernt und Rechtssicherheit geschaffen werden. Im Wesentlichen sind durch die revidierte Zahlungsdienstrichtlinie vier Hauptziele anzustreben:

- Der Schutz von Konsument/innen vor missbräuchlichen und betrügerischen Zahlungstransaktionen durch unbekannte Dritte
- Die kontinuierliche und effiziente Weiterentwicklung des integrierten Binnenmarktes für sichere elektronische Massenzahlungen
- Die Sicherstellung von Wettbewerbsgleichheit
- Die Förderungen von Innovation durch den geöffneten, kostenlosen Zugang zu Zahlungskonten für Drittparteien (auch Nicht-Banken), das sogenannte Access-to-Account-Prinzip (XS2A)

Artikel 98 über die technischen Regulierungsstandards (RTS) für die Authentifizierung und Kommunikation beauftragt die Europäische Bankenaufsichtsbehörde (EBA) in Zusammenarbeit mit der Europäischen Zentralbank (EZB), technische Regulierungsstandards auszuarbeiten, welche unter anderem Folgendes präzisieren:

- Anforderungen an die starke Kundenauthentifizierung gemäss Artikel 97
- Ausnahmen der Anwendung des Artikels 97
- Anforderungen, die Sicherheitsmassnahmen erfüllen müssen, um die Vertraulichkeit und Integrität der personalisierten Sicherheitsmerkmale der Zahlungsdienstnutzenden zu schützen
- Anforderungen an gemeinsame und sichere offene Standards für die Kommunikation zwischen den kontoführenden Zahlungsdienstleistern, Zahlungsauslösedienstleistern, Kontoinformationsdienstleistern, Zahler/innen und Zahlungsempfänger/innen zum Zwecke der Identifizierung und Authentifizierung
- Ermöglichung und Entwicklung benutzerfreundlicher, allgemein zugänglicher und innovativer Zahlungsmittel

Die Mitgliedstaaten wurden ausserdem verpflichtet, die Anforderungen aus PSD2 in nationales Recht umzusetzen und per 14.09.2019 anzuwenden. Aufgrund der fehlenden lückenlosen Umsetzung der Vorgaben durch die verschiedenen Marktteilnehmenden und den damit verbundenen Bedenken hinsichtlich der möglichen negativen Folgen für die Wirtschaft hat die Europäische Bankenaufsichtsbehörde (EBA) am 16. Oktober 2019 den zuständigen nationalen Behörden erlaubt, gewisse Umsetzungsfristen im Zusammenhang mit kartenbasierten E-Commerce-Transaktionen bis zum 31. Dezember 2020 zu verlängern. Dies umfasst unter anderem die Vorgaben, welche laut PSD2 (Artikel 97) eine starke Kundenauthentifizierung (Strong Customer Authentication, SCA) verlangt, wenn ein/e Zahler/in:

- online auf ihr/sein Konto zugreift,
- einen elektronischen Zahlungsvorgang auslöst oder
- über einen Fernzugang Handlungen vornimmt, die das Risiko eines Betrugs im Zahlungsverkehr oder anderen Missbrauchs birgt.

2.1.1 Marktteilnehmende und Rollen

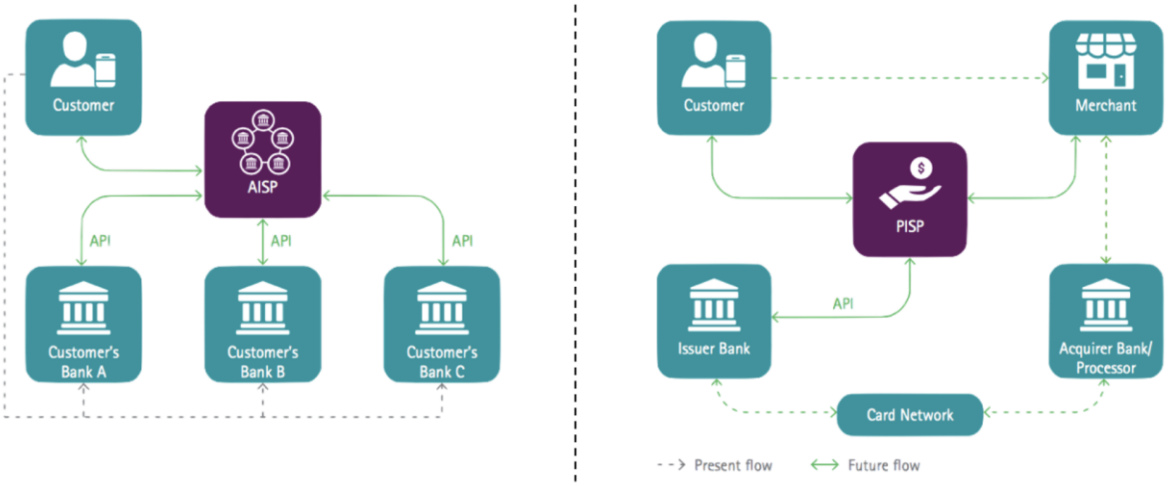
Die PSD2-Richtlinie definiert die Rechte und Pflichten der Marktteilnehmenden und beschreibt die Akteurinnen und Akteure und deren Begriffsbestimmungen wie folgt:

- Ein/e **Zahlungsdienstnutzer/in (Payment Service User, PSU)** ist laut PSD2 (Artikel 4, Ziffer 10) „eine natürliche oder juristische Person, die einen Zahlungsdienst als Zahler[in] oder Zahlungsempfänger[in] oder in beiden Eigenschaften in Anspruch nimmt“.
- Ein **kontoführender Zahlungsdienstleister (Account Servicing Payment Service Provider, ASPSP)** stellt laut PSD2 (Artikel 4, Ziffer 17) für eine Zahlerin oder einen Zahler ein Zahlungskonto bereit und führt es. Der kontoführende Zahlungsdienstleister stellt in der Regel die personalisierten Sicherheitsmerkmale für die sichere Kundenauthentifizierung zur Verfügung. Dies bedeutet auch, dass sich die Zahlungsauslösedienstleistenden (PISP) auf das Authentifizierungsverfahren des kontoführenden Zahlungsdienstleisters bei der Auslösung von Zahlungen verlassen können. Zudem muss jeder kontoführende Zahlungsdienstleister, auf dessen Zahlungskonten online zugegriffen werden kann, mindestens eine unentgeltliche Schnittstelle bieten, über die eine sichere Kommunikation mit anderen Drittparteien (Third Party Provider, TPP) möglich ist. Dabei kann der kontoführende Zahlungsdienstleister frei entscheiden, ob er für die Kommunikation mit Drittparteien eine neue Schnittstelle zur Verfügung stellt oder die für Identifizierung und Kommunikation mit den Zahlungsdienstnutzern bestehende Schnittstelle öffnet. Im Falle eines nicht autorisierten oder betrügerischen Zugangs sowie einer nicht autorisierten oder betrügerischen Zahlungsauslösung kann der kontoführende Zahlungsdienstleister laut PSD2 (Artikel 68, Ziffer 5) den Zugang zu einem Zahlungskonto verweigern.
- Ein **Kontoinformationsdienstleister (Account Information Service Provider, AISP)** stellt laut PSD2 (Artikel 4, Ziffer 16 und 17) dem Zahlungsdienstnutzer „einen Online-Dienst zur Mitteilung konsolidierter Informationen über ein oder mehrere Zahlungskonten zur Verfügung, welche der Zahlungsdienstnutzer bei einem oder mehreren Zahlungsdienstleistern hält“. Der Zahlungsdienstnutzer erhält somit in Echtzeit einen Gesamtüberblick über seine Kontostände sowie Zahlungstransaktionen. Die Kontodienstleistenden dürfen laut PSD2 (Artikel 67, Ziffer 2) die Dienstleistungen nur mit der ausdrücklichen Zustimmung der Zahlungsdienstnutzenden erbringen und müssen sicherstellen, dass die personalisierten Sicherheitsmerkmale der Zahlungsdienstnutzenden geschützt werden und über sichere

und effiziente Kanäle erfolgen. Kontoinformationsdienstleistende halten keine Gelder der Nutzenden.

- Ein **Zahlungsauslösedienstleister (Payment Initiation Service Provider, PISP)** stellt laut PSD2 (Artikel 4, Ziffer 15) einen Dienst bereit, „der auf Antrag des Zahlungsdienstnutzers einen Zahlungsauftrag in Bezug auf ein bei einem anderen Zahlungsdienstleister geführten Zahlungskonto auslöst“. Diese Zahlungsauslösedienste spielen laut PSD2 (Erwägungsgründe, Ziffer 27) „eine Rolle bei Zahlungen im elektronischen Geschäftsverkehr, indem sie eine Softwarebrücke zwischen der Webseite des Händlers und der Plattform des kontoführenden Zahlungsdienstleisters des Zahlers einrichten, um auf Überweisungen gestützte Zahlungen über das Internet auszulösen“. Laut PSD2 (Erwägungsgründe, Ziffer 31) ist der Zahlungsauslösedienstleister zu keinem Zeitpunkt der Zahlungskette im Besitz der Gelder der Nutzenden und tritt in aller Regel nicht in ein Vertragsverhältnis mit den kontenführenden Zahlungsdienstleistenden ein. Daher unterliegen diese neuen Marktteilnehmenden, sofern sie ausschliesslich Zahlungsauslösedienste anbieten, nicht den Eigenmittelanforderungen gemäss der Kapitaladäquanzverordnung (EU) Nr. 575/2013. Laut PSD2 (Artikel 65, Ziffer 1) müssen die Mitgliedstaaten sicherstellen, dass der kontenführende Zahlungsdienstleister bei einer Zahlungsauslösung „unverzüglich bestätigt, ob ein für die Ausführung eines kartengebundenen Zahlungsvorgangs erforderlicher Betrag auf dem Konto des Zahlers verfügbar ist“. Zahlungsauslösedienste müssen die Zahlungsempfänger/innen bei einer erfolgten Zahlungsauslösung unmittelbar informieren, so dass die entsprechende Ware freigegeben oder die Dienstleistung unverzüglich erbracht werden kann.

Abbildung 1: Beziehung zwischen den Marktteilnehmenden



Quelle: IBM Developer, 2019 abgerufen am 18. September 2019

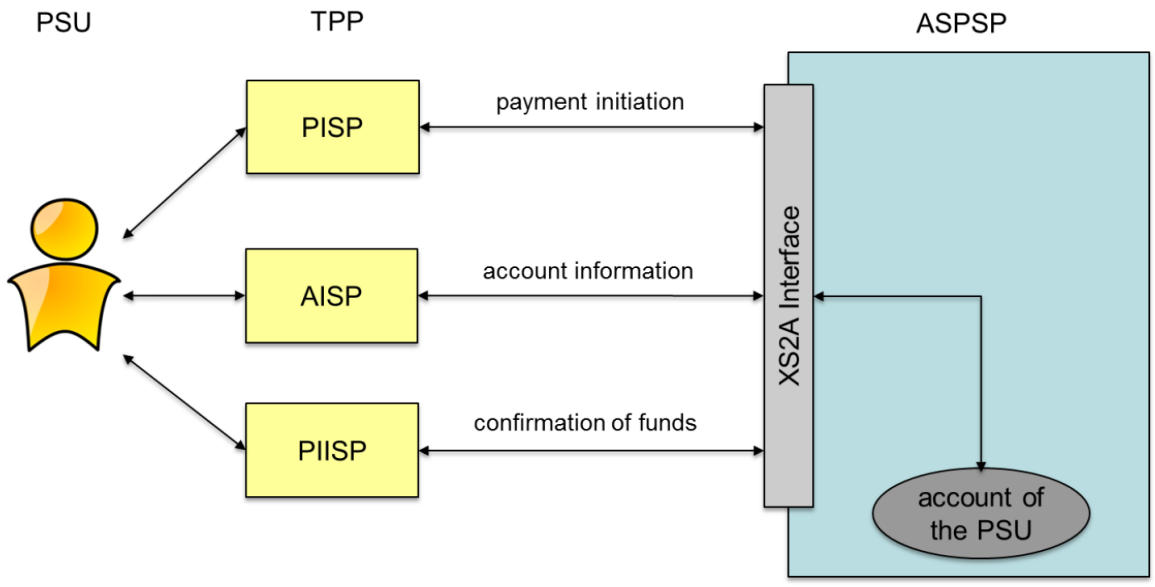
2.1.2 Gemeinsame und sichere Kommunikationsstandards

Laut PSD2 (Erwägungsgründe, Ziffer 49) muss jeder Zahlungsdienstleister unbedingt Zugang zu den technischen Infrastrukturdiensten der Zahlungssysteme haben: „Der Zugang sollte jedoch Anforderungen unterliegen, um die Integrität und Stabilität der Systeme zu gewährleisten.“ Die Best-

immungen über den Zugang gelten laut PSD2 (Erwägungsgründe, Ziffer 52) nicht für Zahlungssysteme, welche in einem Dreiparteien-System betrieben werden wie beispielsweise Drei-Parteien-Kartensysteme, in welchen der Zahlungsdienstleister sowohl die Rolle der Kartenherausgeberin (Issuer) als auch der Akzeptanzstelle (Acquiring) innehat. Die Rahmenbedingungen für den Zugang zu den Zahlungssystemen werden in den technischen Regulierungsstandards für die starke Kundenauthentifizierung und für sichere offene Standards für die Kommunikation (RTS) präzisiert, es wird jedoch kein Schnittstellenstandard definiert. Die Delegierte Verordnung (EU) 2018/389 hat die Europäische Kommission am 13. März 2018 im Amtsblatt der Europäischen Union veröffentlicht.

Die EBA verbietet ausserdem eine Technik namens „Screen-Scraping“, welche das Auslesen und Einfügen von Bildschirminformationen ermöglicht, mit dem Ziel der Informationsgewinnung und Extrahierung. FinTechs haben in der Vergangenheit diese Technologie genutzt, um den Bankkund/innen mit ihrer Einwilligung Informationen anzuzeigen. Durch das Verbot müssen Banken diesen direkten Zugriff auf Kontendaten nicht mehr gewähren, jedoch eine eigens für Drittanbietende eingerichtete Schnittstelle anbieten, welche die für Identifizierung und Kommunikation mit den Zahlungsdienstnutzenden bestehende Schnittstelle öffnen. Die finale Version der RTS sieht bezüglich Schnittstellen explizit Technologie-Neutralität vor. So wurden Anforderungen und Zielsetzungen zur Informationssicherheit wie ISO Standard 27001 sowie „Hypertext Transfer Protocol Secure (HTTPS) über Transport Security Layer (TLS)“ aus der Spezifikation entfernt. Zudem muss eine dedizierte Schnittstelle gemäss RTS (Erwägungsgründe, Ziffer 23) denselben Grad der Verfügbarkeit und Leistung aufweisen wie die von den Zahlungsdienstnutzenden verwendete Schnittstelle. Kontoführende Dienstleistende müssen diesbezüglich Leistungsindikatoren und Service-Level-Ziele definieren. Laut RTS (Erwägungsgründe, Ziffer 26) muss die Sicherheit von Kommunikationssitzungen zum Schutz der Vertraulichkeit und der Integrität der Daten gewährleistet sein.
Die „Berlin Group“ ist eine paneuropäische Interoperabilitäts- und Harmonisierungsinitiative, welche zum Ziel hat, offene zahlungsnetzwerk- und prozessorunabhängige Standards zu definieren zwischen Instituten, die Zahlungsinstrumente annehmen und abrechnen (Acquirer), und solchen, die Zahlungsinstrumente ausgeben (Issuer). Zudem hat die Berlin Group unter dem Namen „NextGenPSD2“ einen Standard bezüglich Kontozugängen anhand von Application Programming Interface (API) erarbeitet, wodurch TPP’s den Zugriff auf Bankkontoinformationen erhalten. Die API’s wurden im Architekturstil des Representational State Transfers (REST) definiert, welcher zur Umsetzung von REST-Webservices das HTTP-Protokoll verwendet. Dieser Standard wird bereits von zahlreichen Banken und Zahlungsdienstleistenden genutzt und verhindert damit, dass aufgrund der fehlenden Schnittstellenspezifikation in den RTS jedes Finanzinstitut eine proprietäre Schnittstelle entwickelt und zur Verfügung stellt.

Abbildung 2: Berlin Group – XS2A Framework



Quelle: Berlin Group, 2018, NextGenPSD2 XS2A Framework

2.1.3 Technische Regulierungsstandards zur starken Kundenauthentifizierung

Um die Sicherheit für Kartenzahlenden zu erhöhen, fallen grundsätzlich sämtliche Vorgänge, bei denen die Zahlenden online auf ihre Konten zugreifen oder einen elektronischen Zahlungsvorgang auslösen, in den Geltungsbereich der starken Kundenauthentifizierung (SCA). Bei der starken Kundenauthentifizierung prüft der Issuer die Identität der Karteninhabenden anhand von Authentisierungsfaktoren aus mindestens zwei unterschiedlichen Kategorien. Die Faktoren können Elemente aus den Kategorien Wissen, Besitz oder Inhärenz sein.
In bestimmten Fällen ist die starke Kundenauthentifizierung nicht erforderlich:

- wenn sich entweder der Zahlungdienstleister des Zahlers (Issuer) oder der Zahlungsdienstleister des Zahlungsempfängers (Acquirer) ausserhalb des EWR befindet (One-Leg-Out-Transaktionen, OLO)
- Bei Versandhandels- und Telefonbestellungen („Mail Order/Telephone Order“, MOTO), da diese nicht als elektronische Zahlungen gelten
- wenn Zahlungen mittels anonymen Pre-Paid-Karten vorgenommen werden
- bei Kartenzahlungen, bei denen die Karteninhabenden mittels Unterschrift verifiziert werden
- wenn die Zahlung durch den Zahlungsempfänger ausgelöst wird („Merchant Initiated Transactions“, MIT), beispielsweise bei Lastschriften

Grundsätzlich gilt, dass bei Distanzzahlungen mit jeder starken Authentifizierung der Authentifizierungscode mit einem Zahlungsempfänger sowie einem Betrag und einer Währung verknüpft sein muss (sogenanntes Dynamic Linking) (RTS, Ziffer 3). Insbesondere in der Reise- und Gastgewerbebranche sind häufig die effektiv abzurechnenden Zahlungsbeträge zum Zeitpunkt der Authentisierung nicht bekannt, wie beispielsweise bei der Reservation eines Hotelzimmers. Im

Grundsatz gilt jedoch, dass der Autorisierungsbetrag maximal gleich hoch oder tiefer als der Authentifizierungsbetrag sein muss.

Um eine Disruption des kartengebundenen Zahlungsverkehrs aufgrund der SCA-Vorgaben zu verhindern, wurden zahlreiche SCA-Befreiungen, sogenannte „Exemptions", definiert. Eine Transaktion kann mehrere Exemptionskriterien erfüllen. Diese Befreiungen von der starken Kundenauthentifizierung werden in den RTS im Kapitel III in den Artikeln 10–18 definiert und haben zum Ziel, die zu erwarteten Zahlungsabbrüche aufgrund der starken Kundenauthentifizierung zu verringern. Gleichwohl gilt, dass SCA die Regel ist und Exemptions als optional zu betrachten sind. Nachfolgend sind die wichtigsten Befreiungen aufgelistet:

- **Befreiung bei kontaktlosen Zahlungen an der Verkaufsstelle (RTS, Artikel 11)**
  Eine kontaktlose Zahlung erfolgt über den Nearfield-Communication-Funkstandard (NFC-Funkstandard) zur drahtlosen Datenübertragung, welcher auf der Technologie der Radio-Frequenz-Identifikation (RFID) beruht. Dabei wird die Zahlkarte oder ein Kundengerät wie ein Smartphone an das POS-Zahlterminal gehalten, um den Zahlvorgang zu initiieren. Eine kontaktlose Zahlung bis EUR 50 muss dabei nicht stark authentifiziert werden, solange die Anzahl Transaktionen ohne starke Kundenauthentifizierung 5 oder der kumulative Betrag EUR 150 nicht übersteigt. Die Kartenherausgebenden haben die Möglichkeit, zu bestimmen, ob die Anzahl Transaktionen oder der Maximalbetrag bezüglich der Ausnahme von der starken Kundenauthentifizierung zur Anwendung kommt. Da der Händler diese Informationen nicht vorliegen hat, kann die Ausnahme nur durch die Kartenherausgeberin oder das Zahlungsnetzwerk wie beispielsweise Mastercard oder Visa angewendet werden.
- **Befreiung bei unbeaufsichtigten Terminals für Nutzungsentgelte und Parkgebühren (RTS, Artikel 12)**
  Dies gilt für eine vom Zahlungsdienstnutzer initiierte Zahlung, um an einem unbeaufsichtigten Zahlterminal Beförderungsentgelte oder Parkgebühren zu entrichten.
- **Befreiung bei vertrauenswürdigen Zahlungsempfänger/innen (RTS, Artikel 13)**
  Falls die Kartenherausgeberin es anbietet, haben die Karteninhabenden die Möglichkeit, Zahlungsempfänger wie beispielsweise einen Online-Händler, bei dem sie regelmässig einkaufen, auf eine Liste mit vertrauenswürdigen Zahlungsempfängern (Whitelist) zu setzen. Ein Zahlungsempfänger kann sich nicht selber auf eine Whitelist setzen, zudem behält die Kartenherausgeberin so die Möglichkeit, dass die Karteninhabenden sich auch bei Transaktionen bei vertrauenswürdigen Zahlungsempfängern stark authentifizieren lassen müssen.
- **Befreiung bei wiederkehrenden Zahlungsvorgängen (RTS, Artikel 14)**
  Bei wiederkehrenden Zahlungsvorgängen mit gleichem Betrag und dem gleichem Zahlungsempfänger muss lediglich beim erstmaligen Erstellen, Auslösen oder bei einer Änderung eine starke Kundenauthentifizierung verlangt werden. In allen anderen Fällen kann von einer starken Kundenauthentifizierung abgesehen werden.
- **Befreiung bei Überweisungen zwischen Konten, die von derselben Person gehalten werden (RTS, Artikel 15)**
  Falls es sich beim Zahler bzw. der Zahlerin und Empfänger bzw. Empfängerin um die gleiche natürliche oder juristische Person handelt und beide Zahlungskonten vom gleichen kontoführenden Zahlungsdienstleister unterhalten werden, kann von einer starken Kundenauthentifizierung abgesehen werden.
- **Befreiung bei Kleinbetragszahlungen (RTS Artikel 16)**

Bei E-Commerce-Zahlungsvorgängen mit Beträgen unter EUR 30 kann von einer starken Kundenauthentifizierung abgesehen werden, falls entweder die Summe der Zahlungsvorgänge seit der letzten starken Kundenauthentifizierung EUR 100 nicht oder die Anzahl an Zahlungsvorgängen ohne starke Kundenauthentifizierung 5 nicht übersteigt.

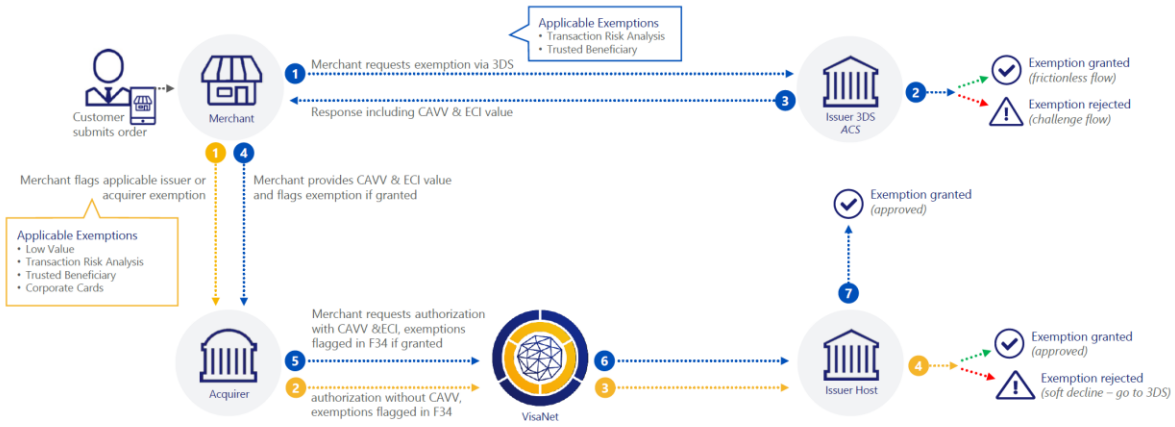
- **Befreiung aufgrund einer Transaktionsrisikoanalyse (RTS Artikel 18)**
  Die wohl wichtigste Befreiung von der starken Kundenauthentifizierung bei kartengebundenen E-Commerce-Zahlungen ist, wenn aufgrund von Transaktionsüberwachungsmechanismen in Echtzeit eine Transaktion als risikogering eingeschätzt wird. Die Kartenherausgeberin kann dabei keines der folgenden Szenarien feststellen:
  i) Eine ungewöhnliche Ausgabe oder ein irritierendes Verhaltensmuster der Zahlenden, beispielsweise bezüglich Ort, Datum und Uhrzeit der Transaktion oder des Transaktionsbetrags
  ii) Ungewöhnliche Informationen über den Zugriff auf das Zugangsgerät oder die Zugangssoftware der Zahlenden, beispielsweise bezüglich des Orts des Zugriffes, der IP-Adresse oder wenn in ungewöhnlicher Weise eine „Passwort vergessen"-Funktion aktiviert wird
  iii) Eine Malware-Infektion in einer Phase des Authentifizierungsverfahrens
  Das Entdecken einer Malware-Infektion auf einem Gerät im Authentifizierungsverfahren ist in der Realität schwierig, meist lückenhaft und ohne Zustimmung (Consent) der Zahlenden rechtlich nicht zugelassen. Das Android-Betriebssystem lässt es technisch zu, dass eine Liste sämtlicher auf einem Mobiltelefon installierter Apps ausgelesen und mit einer Liste von allen bekannten schadhaften Apps verglichen wird. Das Entdecken einer Malware bei einer browserbasierten Authentifizierung z.B. über einen Desktop-Computer ist noch schwieriger. Technisch ist es möglich, festzustellen, welche Plug-Ins in einem Browser installiert wurden, um so eine triviale „Man-in-the-Browser"-Attacke (MITB-Attacke) zu erkennen. Bei einer MITB-Attacke infiziert eine Trojaner-Schadsoftware den Browser der Zahlerin oder des Zahlers, um bei einer Transaktion, von den Zahlenden unbemerkt, Änderungen (z.B. Betrag und Begünstigte/r) vorzunehmen.
  iv) Bekanntes Betrugsszenario bei der Erbringung von Zahlungsdienstleistungen
  v) Ungewöhnlicher Ort der Zahlenden (sie waren vorher noch nie an diesem Ort)
  vi) Ort der Zahlenden mit hohem Risiko

Der ungefähre Aufenthaltsort der Zahlenden kann meistens nur indirekt bestimmt werden, indem beispielsweise bei browserbasierten Authentifizierungen die Internet-Protokoll-Adresse (IP-Adresse) geprüft wird und so aufgrund des entsprechenden lokalen Internetregisters (häufig auch der Internet Service Provider, ISP) das Land oder die Region bestimmt werden kann. Betrüger/innen nutzen jedoch meistens Verfahren, um die tatsächliche IP-Adresse zu verschleiern, beispielsweise durch die Nutzung von Virtuellen Privaten Netzwerken (VPN), TOR-Browsern oder Proxyservern. Der Browser Opera wirbt beispielsweise mit folgender Eigenschaft (Feature): „Opera ist der erste und noch immer der einzige der gängigen Browser, in den ein kostenloser, unbeschränkter VPN-Dienst integriert ist. Dank des VPN können Sie sich auf die Ihnen wichtigen Inhalte konzentrieren, ohne Angst vor der Verletzung Ihrer Privatsphäre zu haben" (Opera, 2019, o.S.). Bei auf einer App basierten Authentifizierungsverfahren können von Roaminginformationen des entsprechenden Telekommunikationsanbieters Informationen über den ungefähren Aufenthaltsort der

Zahlenden abgeleitet werden. Das exakte Bestimmen des Ortes der Transaktion über Global-Positioning-System-Daten (GPS-Daten) ist aufgrund von Datenschutzbestimmungen als heikel zu betrachten und in der Praxis unüblich.

Eine weitere Möglichkeit für die Kartenherausgeberin ist, die Kundenauthentifizierung an den Händler zu delegieren. Transaktionen, bei denen die Karteninhaberin oder der Karteninhaber vorgängig durch eine sogenannte „Delegated Authentication" authentifiziert wurde, müssen im 3D-Secure-Protokoll entsprechend markiert sein. Der Händler hat zudem die Möglichkeit, aufgrund der durchgeführten delegierten Authentifizierung eine sogenannte „Acquirer Exemption" zu beantragen, so dass der Issuer nicht nochmals eine starke Authentifizierung verlangt.

Abbildung 3: Acquirer Exemption – Transaktionsfluss



Quelle: Visa, 2019, Visa Risk & Authentication Forum in Frankfurt

Um die Befreiung von der Transaktionsrisikoanalyse (TRA) geltend machen zu können, darf die Gesamtbetrugsrate die in der Tabelle 1 abgebildeten Schwellenwerte nicht übersteigen.

Tabelle 1: Berechnung der Betrugsraten für kartengebundene E-Commerce-Zahlungen

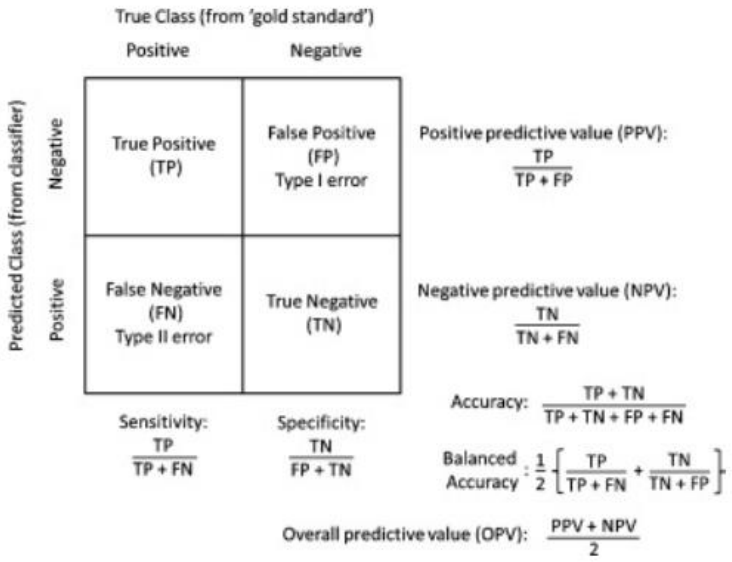
Befreiungsschwellenwert	Referenzbetrugsrate
500 EUR	0.01% = 1 Basispunkt
250 EUR	0.06% = 6 Basispunkte
100 EUR	0.13% = 13 Basispunkte

Quelle: Eigene Darstellung in Anlehnung an RTS, Anhang

Die Gesamtbetrugsrate errechnet sich als Gesamtwert der nicht autorisierten betrügerischen E-Commerce-Transaktionen dividiert durch den Gesamtwert sämtlicher E-Commerce-Zahlungen.

Die Berechnung basiert somit auf der Brutto-Betrugsbetrag. Die Zahlungsnetzwerke haben für kartenbasierte Zahlungen umfangreiche Regelwerke erlassen, welche definieren, ob in einem Betrugsfall der Acquirer oder Issuer haftet. Die Haftungsfrage oder Haftungsumkehr (Liability Shift) ist davon abhängig, wie eine Zahlungstransaktion vorgängig authentifiziert wurde. Falls im Grundsatz keine Haftungsumkehr zur Anwendung kommt, haftet der Acquirer. Der Issuer hat somit das Recht, eine Transaktion, welche durch die Karteninhaberin oder den Karteninhaber als Betrugstransaktion gemeldet wurde, zu beanstanden (Dispute/Chargeback). Falls der Händler nicht belegen kann, dass es sich um eine durch die Karteninhaberin oder den Karteninhaber legitimierte und autorisierte Transaktion handelt, trägt der Acquirer den Schaden. In der Praxis wird der Acquirer den Betrugsschaden in aller Regel dem Händler weiterverrechnen. Laut dem Kartennetzwerk Visa werden über 80% der beanstandeten Transaktionen als vermeintliche Betrugstransaktionen gemeldet. Dies ist häufig darauf zurückzuführen, dass die Karteninhaberin oder der Karteninhaber eine Transaktion aufgrund unklarer Transaktionsdetails wie beispielweise kryptisch klingender Händlernamen nicht erkennt. Es ist im Interesse des gesamten Zahlungs-Ökosystems, die Anzahl der zu Unrecht als Betrug gemeldeten Transaktionen mit geeigneten Massnahmen zu reduzieren. So gibt es technische Lösungen, welche es möglich machen, der Karteninhaberin oder dem Karteninhaber Warenkorbinformationen des Händlers anzuzeigen, um somit die Transaktionserkennungsrate zu steigern. Eine Kartenherausgeberin hat zudem die Möglichkeit, auf einfache Art und Weise ihre Betrugsraten zu senken, indem sie beispielsweise seine Transaktionsautorisierungsstrategie so restriktiv aufsetzt, dass mehr Betrugstransaktionen gefunden werden. Dies wird im Regelfall jedoch die Konsequenz nach sich ziehen, dass auch mehr legitime Transaktionen zu Unrecht als Betrugstransaktionen klassifiziert und abgelehnt werden, sogenannte „False Positives“. Die Herausforderung besteht also darin, ein holistisches Risiko-Management-System zu implementieren, welches sämtliche relevanten Kennzahlen optimiert, sowohl bezüglich Sensitivität, Spezifizität als auch hinsichtlich der Trennschärfe.

Abbildung 4: Konfusions-Matrix mit Kennzahlenberechnung



Quelle: Research Gate, 2019

2.2 Identifikation und Authentifikation

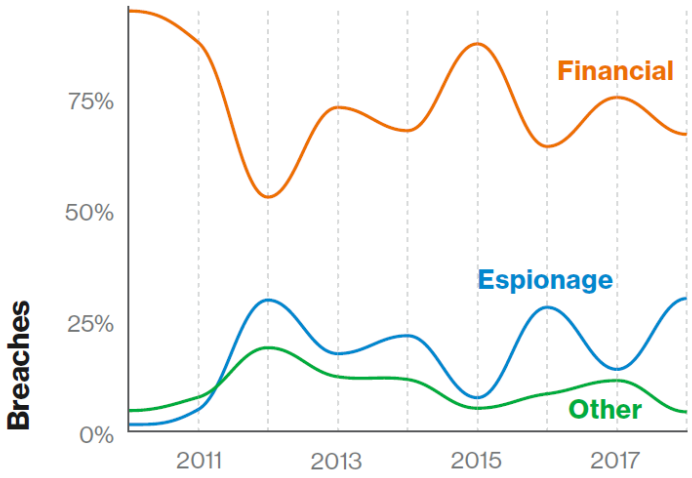
Der Begriff der Identität wird in unterschiedlicher Weise verwendet. Diese Arbeit orientiert sich an der Definition des Rechtschreibewörterbuchs von Duden und lautet: „Echtheit einer Person […]; völlige Übereinstimmung mit dem, was sie ist […]“ (Duden, 2019).

Die Authentifikation umfasst zwei Vorgänge: die Authentisierung sowie die Authentifizierung. „Die Authentisierung stellt den Nachweis einer Person dar, dass sie tatsächlich die Person ist, die sie vorgibt zu sein, um damit ihre Identität zu bestätigen.“ (Datenschutzbeauftragter, 2019)
Die Authentifizierung stellt die Prüfung der behaupteten Authentisierung dar, das heisst, die gemachten Angaben werden auf ihre Echtheit überprüft. Eine korrekte Authentifizierung einer Person erfordert deren eindeutige Charakterisierung durch wohldefinierte Eigenschaften, so dass über diese zweifelsfrei eine eindeutige Identifizierung möglich ist (Eckert, 2018). In der englischen Sprache wird mit dem Wort „Authentication“ sowohl der Authentisierungs- als auch Authentifizierungsvorgang bezeichnet.

2.2.1 Elektronische Identität

In der physischen Welt besitzt jede natürliche Person lediglich eine Identität und der Nachweis erfolgt in der Regel mit einem Pass oder einer Identitätskarte. Im Internet haben natürliche Personen mehrere digitale Identitäten, da man sich auf vielen Webseiten registrieren oder identifizieren muss, um Waren oder Dienstleistungen zu erhalten. Obwohl viele Nutzende bei der Registrierung für ein Online-Konto oft die gleiche E-Mail-Adresse sowie das gleiche Passwort verwenden, handelt es sich um unterschiedliche Identitäten. Der Einsatz des gleichen Nutzernamens und Passwortes bei unterschiedlichen Registrierungen ist heikel, da es Betrüger/innen immer wieder gelingt, Lücken in den Sicherheitssystemen und Netzwerken zu finden und grosse Datenmengen zu stehlen (Data Breaches). Aus der 2019er-Ausgabe des jährlich erscheinenden „Data Breach Investigations Reports (DBIR)“ des US-amerikanischen Telekommunikationsunternehmens Verizon geht hervor, dass in über 70% der untersuchten Ereignisse die Cyber-Angriffe finanziell motiviert sind.

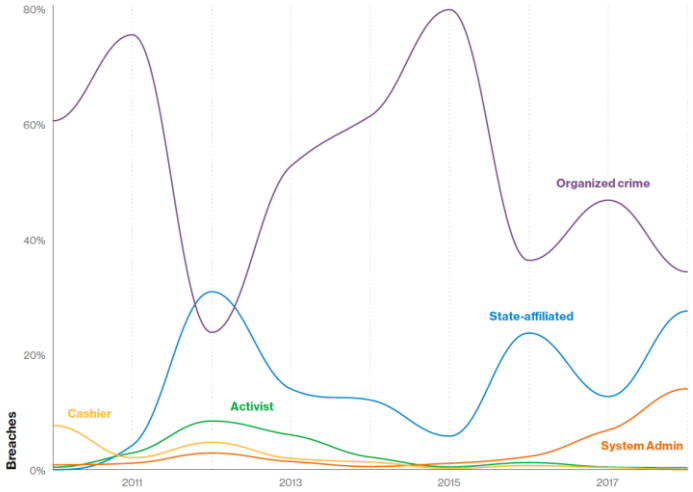
Abbildung 5: Motivationstreiber der Cyber-Kriminellen



Quelle: 2019, Verizon – Data Breach Investigations Report, S. 6

Der Bericht zeigt ebenfalls auf, dass in den letzten Jahren der grösste Anteil an Angriffen von Mitgliedern der organisierten Kriminalität ausgeführt wurde, jedoch die Anzahl Angriffe ausgeführt durch staatliche oder staatsnahe Akteurinnen und Akteure deutlich zugenommen hat:

Abbildung 6: Verteilung nach Angriffsgruppen



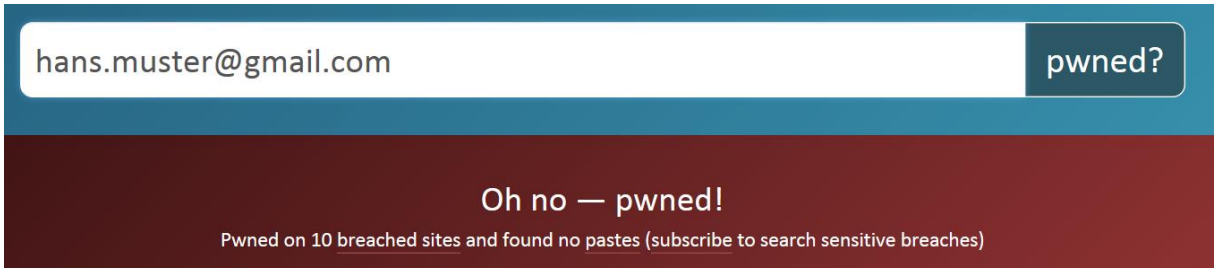
Quelle: 2019, Verizon – Data Breach Investigations Report, S. 7

Im September 2018 meldete British Airways, dass persönliche Daten von über 500‘000 Kund/innen gestohlen wurden. Aufgrund des Verstosses gegen das Europäische Datenschutzgesetz (GDPR) wird British Airways dafür eine Busse von ca. 183 Millionen Britische Pfund bezahlen müssen. Im November 2018 wurden bei der Hotelgruppe Mariott 339 Millionen Datensätze gestohlen, welche Kreditkartennummern, Passnummern sowie Geburtsdaten enthielten. Bekannte Data Breaches wurden 2019 unter anderem bei dem Online-Spiel „Fortnite“ verzeichnet, bei dem über

eine Cross-Site-Scripting-Attacke (XSS-Attacke) Daten von über 200 Millionen Nutzenden gestohlen wurden. „Bei einem XSS-Angriff wird eine Webanwendung mit einem Skript gesendet, dieses wird aktiviert, wenn sie vom Browser eines ahnungslosen Benutzers oder von einer Anwendung gelesen wird, die sich nicht gegen Cross-Site-Scripting geschützt hat. Je nach Schwere des Angriffs können Benutzerkonten gefährdet, Trojanerprogramme aktiviert und Seiteninhalte geändert werden, was viele Benutzer dazu verleitet, ihre persönlichen Daten freiwillig preiszugeben. Schliesslich konnten Session-Cookies aufgedeckt werden, die es einem Täter ermöglichen, sich als gültiger Benutzer auszugeben und seine privaten Konten zu missbrauchen“ (IT Talents, 2019). Ebenfalls 2019 wurde der Data Breach einer mobilen Applikation (App) der Medienunternehmung Cultura Colectiva sowie der App „At the Pool“ bekannt, bei der über 540 Millionen Facebook Datensätze inklusive Facebook ID’s gestohlen wurden (Handelsblatt, 2019).

Um herauszufinden, ob man Opfer eines Data Breaches geworden ist, besteht auf der Website https://haveibeenpwned.com die Möglichkeit, anhand der E-Mail-Adresse zu überprüfen, ob ein Online-Konto durch Betrüger/innen kompromittiert wurde.

Abbildung 7: Data Breach – Prüfung eines Kontos



Quelle: Eigenes Beispiel, abgerufen am 14.9.2019 auf https://haveibeenpwned.com

In dem gewählten Beispiel ist ersichtlich, dass der Account von „Hans Muster“ mit der E-Mail-Adresse hans.muster@gmail.com bereits bei 10 Data Breaches kompromittiert wurde. Ein Blick auf die Detailliste zeigt, dass bei drei bekannten Online-Diensten sowohl E-Mail-Adressen als auch Passwörter kompromittiert wurden; bei Adobe sind 153 Millionen Konten betroffen, bei Dropbox 68 Millionen und bei LinkedIn über 164 Millionen.

Wie sicher ein Passwort ist, kann man auf der Webseite www.passwortcheck.ch des Zürcher Datenschutzbeauftragten prüfen. Diese zeigt an, wie viel Rechenzeit benötigt wird, um ein spezifisches Passwort zu hacken:

Abbildung 8: Passwortüberprüfung beim Zürcher Datenschutzbeauftragten

Quelle: Eigenes Beispiel, abgerufen am 6. 9.2019 auf https://www.passwortcheck.ch/passwort-check/passwortcheck

Obwohl heutzutage Passwörter meistens nicht im Klartext, sondern als Hashwerte gespeichert werden, welche grundsätzlich nicht zurückgerechnet werden können, gelingt es den Betrüger/innen, Passwörter herauszufinden. Eine Hashfunktion (Algorithmus) wandelt ein Passwort mit beliebiger Anzahl von Zeichen in eine Zeichenfolge mit fester Länge um. Oft werden die Hashwerte als hexadezimale Zeichenfolge codiert, also mit Werten von 0–9 und A–F (Ersatz der Zahlen 10–15). Der weitverbreitete Hashfunktion-Message-Digest-Algorithmus 5 (MD5) erzeugt beispielsweise einen 128 Bit-Hashwert. Über sogenannte Regenbogentabellen (Rainbow Tables) lassen sich Passwörter mit geringem Rechenaufwand knacken. Für die Erstellung einer Regenbogentabelle wird am Anfang ein zufälliges Passwort gewählt, welches dann durch den MD5-Algorithmus in einen 32 Zeichen langen (32*4 Bit = 128 Bit) Hexadezimal-Fingerprint verschlüsselt wird. Wird beispielsweise das Passwort „Passwort“ gewählt, wird der MD5-Hash „3e45af4ca27ea2b03fc6183af40ea112“ generiert. Nun wird über eine Reduktionsfunktion, welche nicht die inverse Funktion der Hashfunktion ist, der Hexadezimalwert wieder in ein Klartextpasswort umgewandelt, in diesem Beispiel ergibt es das Passwort „1(e4%99#“ (Stackoverlow, 2019). Dieses Passwort wird nun als Inputvariable für den nächsten Hashing-Vorgang verwendet und dann mittels Reduktionsfunktion wieder in ein neues Klartextpasswort umgewandelt. Bei einer Million Wiederholungen erhält man somit je nach Rechenleistung in wenigen Sekunden bis Minuten 1 Million Passwörter, welche die Betrüger/innen nutzen, um sich in Kombination mit den gestohlenen E-Mail-Adressen Zugang zu Online-Nutzerkonten zu erhalten (Decademic, 2019).

Ein möglicher Lösungsansatz, um die Anzahl an unsicheren digitalen Identitäten im Internet zu reduzieren, ist die Zentralisierung der Identitäten durch sogenannte „Identity Provider“ (IdP). Grosse Unternehmungen wie Google, Facebook und Amazon ermöglichen bereits heute die Nutzung ihrer Kontoinformationen für die Authentifizierung bei Drittparteien. Die Qualität der Registrierung (QoR) solcher digitalen Identitäten ist niedrig, da bei der Selbstdeklaration keine persönliche Vorsprache (physische Anwesenheit) oder das Vorweisen und die Überprüfung eines Ausweisdokumentes erforderlich sind.

Abbildung 9: Anonymität im Internet

"On the Internet, nobody knows you're a dog."

Quelle: Peter Steiner, 1993 in „The New Yorker"

Um dem Mangel an Vertrauen gegenüber solchen digitalen Identitäten etwas entgegenzusetzen, bieten zahlreiche Länder staatlich anerkannte elektronische Identitäten an. In der Schweiz hat das eidgenössische Justiz- und Polizeidepartement (EJPD) eine Botschaft für ein Bundesgesetz über elektronische Identifizierungsdienste ausgearbeitet, welche im Juni 2018 vom Bundesrat verabschiedet wurde. In der Herbstsession 2019 einigten sich National- und Ständerat auf Regeln für den elektronischen Ausweis und verabschiedeten das Bundesgesetz über anerkannte elektronische Identifizierungseinheiten (E-ID-Gesetz). Die E-ID wird vom EJPD definiert als „digitales Identifizierungsmittel, das im Cyberaum den Beweis erbringt, dass ich ein bestimmter Mensch mit einem bestimmten Geburtsdatum bin". Zugleich wird die Abgrenzung vorgenommen, dass die E-ID kein Reisedokument wie eine Identitätskarte oder ein Pass ist und in der realen Welt nicht zur Identifikation genutzt werden kann und keine digitale Signatur darstellt. Das Gesetz hat laut BGEID, Artikel 1 zum Zweck:

- den sicheren und einfachen elektronischen Geschäftsverkehr unter Privaten und mit Behörden zu vereinfachen
- den Schutz der Persönlichkeit und der Grundrechte von Personen, über die Daten bearbeitet werden, zu gewährleisten
- die Standardisierung und die Interoperabilität der E-ID sicherzustellen

Für Kontroversen sorgte im Vorfeld der Verabschiedung des E-ID-Gesetzes die Aufgabenteilung zwischen Staat und Markt, wobei der Betrieb der Identifizierungsdienste sowie die Ausstellung der elektronischen Identität in die Hände von privatwirtschaftlichen Unternehmen, sogenannten Identity Provider (IdP), gelegt werden. Das Zusammenspiel zwischen Staat und privaten Unternehmen soll laut dem E-ID-Gesetz die notwendige Akzeptanz für die E-ID durch das Verbinden von

vertrauenswürdigen rechtlichen und organisatorischen Rahmenbedingungen mit der Leistungsfähigkeit und Dynamik des Marktes erreicht werden (E-ID-Gesetz, Artikel 1.2.2). Der Beitrag des Staates beschränkt sich im Wesentlichen auf:

- die Erarbeitung und Pflege der Rechtsgrundlagen
- die Definition von Standards, Sicherheits- und Interoperabilitätsanforderungen
- das Betreiben einer elektronischen Schnittstelle über welche anerkannte IdP staatlich geführte Personenidentifizierungsdaten beziehen können
- Anerkennung und Beaufsichtigung von IdP und E-ID Systeme

Dass eine Aufteilung der Rollen zwischen Staat und Markt erfolgreich sein kann, zeigen diverse europäische Länder sowie Kanada.

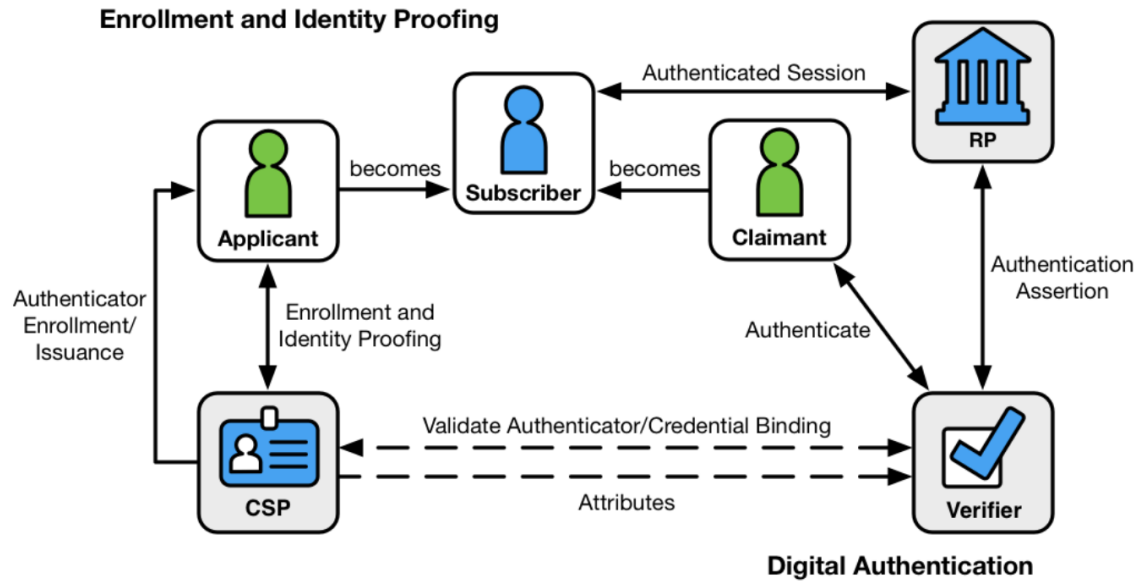
Abbildung 10: Erfolgreiche E-ID-Lösungen von Staaten und Privaten

Land	Lösung (seit)	durchschnittliche Nutzung / Bevölkerung	Herausgeber	Initiatoren	Nutzung möglich bei
Dänemark	NEM ID (2010)	4,7 Mio. Nutzer 83 % der Bev.	Staat	Banken und Staat	öffentlichen und privaten Stellen
Schweden	BankID (2003)	7,5 Mio. Nutzer 76 % der Bev.	Banken	Banken	öffentlichen und privaten Stellen
Norwegen	BankID (2000)	3,6 Mio. Nutzer 69 % der Bev.	Banken	Banken und Staat	öffentlichen und privaten Stellen
Estland	ID-Card (2002) Mobiil ID (2007) Smart-ID (2016)	0,7 Mio. Nutzer 53 % der Bev. (Verbreitung bei mehr als 90 % der Bev.)	Staat	Banken, Telekommunikations-Unternehmen und Staat	öffentlichen und privaten Stellen
Kanada	SecureKey concierge (2012)	7 Mio. Nutzer 20 % der Bev.	Banken	Banken und Staat	öffentlichen und privaten Stellen
Belgien	Itsme (2017)	seit Mai 2017 verfügbar keine Zahlen	Aussteller in Besitz von Banken und Telekommunikations-Unternehmen	Banken und Telekommunikations-Unternehmen	öffentlichen und privaten Stellen
Holland	iDIN (2016)	seit November 2016 verfügbar keine Zahlen	Banken	Banken	öffentlichen und privaten Stellen
	DigiD (2003)	12 Mio. Nutzer 70 % der Bev.	Staat	Staat	öffentliche Stellen
Deutschland	Elektronischer Personalausweis (2010)	2,5 Mio. Nutzer 3 % der Bev.	Staat	Staat	öffentlichen und privaten Stellen

Quelle: EJPD, 2017, Eine staatlich anerkannte elektronische Identität für die Schweiz

Diverse Elemente des E-ID-Gesetzes orientieren sich an den „Digital Identity Guidelines“, welche 2019 vom US-amerikanischen National Institute of Standards and Technology (NIST) publiziert wurden. So gibt es sowohl ähnliche Rollen und Verantwortlichkeiten, die Begrifflichkeiten und Aufgaben sind jedoch teilweise unterschiedlich. Der IdP heisst in der NIST-Spezifikation beispielsweise Credential Service Provider (CSP) und übernimmt zugleich auch die Funktion und Aufgaben des Verifiers. Ein Online-Dienstleister, welcher beim IdP eine Identifizierung des E-ID-Inhabers verlangt, heisst Relying Party (RP), da er sich auf die Authentifizierungsbestätigung des CSP/Verifiers verlässt.

Abbildung 11: NIST-Identity-Modell – Registrierung und Authentifizierung



Quelle: NIST, 2017, Digital Identity Guidelines, S. 22

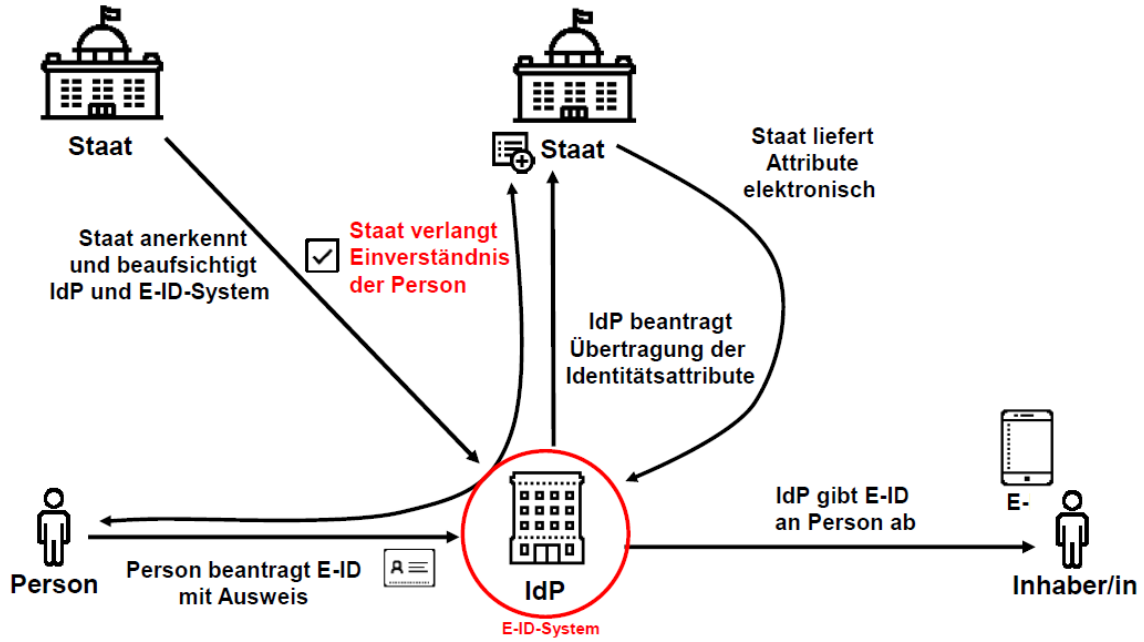
Zudem gibt es ähnlich definierte Sicherheitsniveaus (Level of Assurance, LOA), welche im Schweizer E-ID-Gesetz die Merkmalsausprägungen „niedrig“, „substanziell“ und „hoch“ haben. Das Sicherheitsniveau ergibt sich bei beiden aus der Kombination der Qualität der Registrierung (Identity Assurance Level, IAL), wie beispielsweise persönliche Vorsprache oder Videoidentifikation, der Qualität der Authentifizierungsmittel (Authenticator Assurance Level, AAL) sowie deren Übergabe an einen Antragssteller.

Beim Sicherheitsniveau „niedrig“ kann laut E-ID-Gesetz Artikel 1.2.5 die Registrierung online, gestützt auf einen staatlichen Ausweis, durchgeführt werden. Bei diesem Sicherheitsniveau werden nur die Daten Name, Vorname, Geburtsdatum und die E-ID-Registrierungsnummer zugeordnet. Für den Einsatz der E-ID ist eine Ein-Faktor-Authentifizierung ausreichend. Der Gesetzgeber vergleicht den Vorgang dabei mit kontaktlosen Zahlungen von Kleinbeträgen.

Die E-ID mit Sicherheitsniveau „substanziell“ soll laut E-ID-Gesetz, Artikel 1.2.5 „die Gefahr eines Identitätsmissbrauchs oder der Identitätsveränderung erheblich vermindern“. Die Registrierung erfolgt durch persönliche Vorsprache oder durch eine gleichwertige virtuelle Präsenz wie beispielsweise eine Videoidentifikation, gestützt auf einen staatlichen Ausweis. Zusätzlich zu den Daten, welche im Sicherheitsniveau „niedrig“ enthalten sind, werden Geschlecht, Geburtsort und Zivilstand zugeordnet. Der Einsatz verlangt eine 2-Faktor-Authentifizierung, wie es bei Anwendungen im Finanzsektor üblich ist.

Die E-ID mit Sicherheitsniveau „hoch“ soll gemäss E-ID-Gesetz, Artikel 1.2.5 ebenfalls „die Gefahr eines Identitätsmissbrauchs oder der Identitätsveränderung erheblich vermindern“. Zusätzlich zur persönlichen Vorsprache oder Videoidentifikation, gestützt auf einen staatlichen Ausweis, wird bei der Registrierung die Echtheit des Ausweises und mindestens ein biometrisches Merkmal, gestützt auf eine behördliche Quelle, überprüft. Der Einsatz verlangt eine 2-Faktor-Authentifizierung, wobei gemäss der eIDAS-Durchführungsrechtsakte mindestens ein Faktor biometrisch sein muss.

Abbildung 12: Ausstellung einer schweizerischen E-ID



Quelle: EJPD, 2017, E-ID: Eine staatlich anerkannte elektronische Identität für die Schweiz

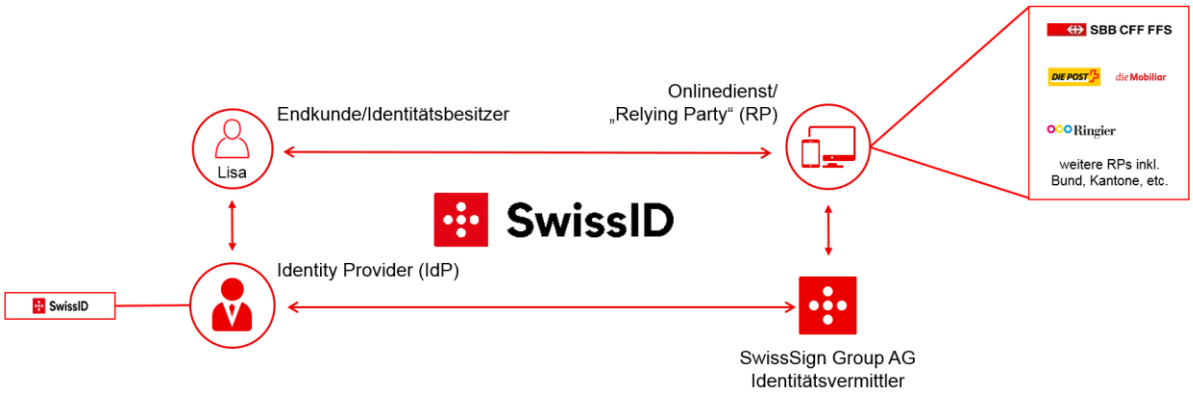
Laut E-ID-Gesetz läuft die Ausstellung einer E-ID in folgenden 7 Schritten ab:

- Schritt 1: Die antragsstellende Person beantragt eine E-ID bei einem (oder mehreren) Identity Providern (IdP) mit einem Ausweis (Pass, Identitätskarte oder Ausländerausweis).
- Schritt 2: Der IdP überprüft den vorgelegten Ausweis und macht bei der Schweizerischen Stelle für elektronische Identität (Identitätsstelle), welche vom Bundesamt für Polizei (fedpol) geführt wird, eine elektronische Anfrage, um die Angaben des Ausweises bestätigen zu lassen, und beantragt die Übermittlung der Identitätsattribute.
- Schritt 3: Die Identitätsstelle überprüft die Daten des Ausweises mit den Personenregisterdaten.
- Schritt 4: Die antragsstellende Person bestätigt über einen digitalen Kanal (z.B. Smartphone), dass sie damit einverstanden ist, dass ihre Personenidentifizierungsdaten einer E-ID zugeordnet und dem IdP übermittelt werden.
- Schritt 5: Die Identitätsstelle übermittelt die E-ID-Registrierungsnummer mit den bestätigten Daten an den IdP.
- Schritt 6: Der IdP ordnet der antragsstellenden Person ein Authentifizierungsmittel (Trägermittel der E-ID) zu, womit sie sich online identifizieren kann. Dieses kann auf einem physischen Träger wie eine Chipkarte, USB-Stick oder auf dem Mobiltelefon der antragstellenden Person gespeichert werden. Zur Speicherung auf dem Mobiltelefon wird ein kryptographisches Verfahren angewendet mittels einer App, welche an das Gerät der antragstellenden Person gekoppelt ist.
- Schritt 7: Der IdP sorgt für die richtige Zuordnung der E-ID-Registrierungsnummer zur E-ID mit dem Authentifizierungsmittel und aktiviert die E-ID für den Gebrauch durch die Inhaberin oder den Inhaber.

In der Schweiz ist die SwissID auf gutem Weg, die erste staatlich anerkannte E-ID zu werden.

Die SwissID ist eine kostenlose Dienstleistung der SwissSign Group, eines Joint Ventures aus staatsnahen Betrieben, Finanzunternehmen, Versicherungsgesellschaften und Krankenkassen und registrierte am 8. Oktober 2019 die 1-millionste Kundin (Swissid, 2019). Das Konsortium besteht aus folgenden Unternehmungen: SBB, Schweizerische Post, Swisscom, Banque Cantonale de Genève, Credit Suisse, Entris Banking, Luzerner Kantonalbank, Raiffeisen, Six Group, UBS, Zürcher Kantonalbank, Axa, Baloise, CSS, Helvetia, Mobiliar, SWICA, Swiss Life, Vaudoise und Zürich.

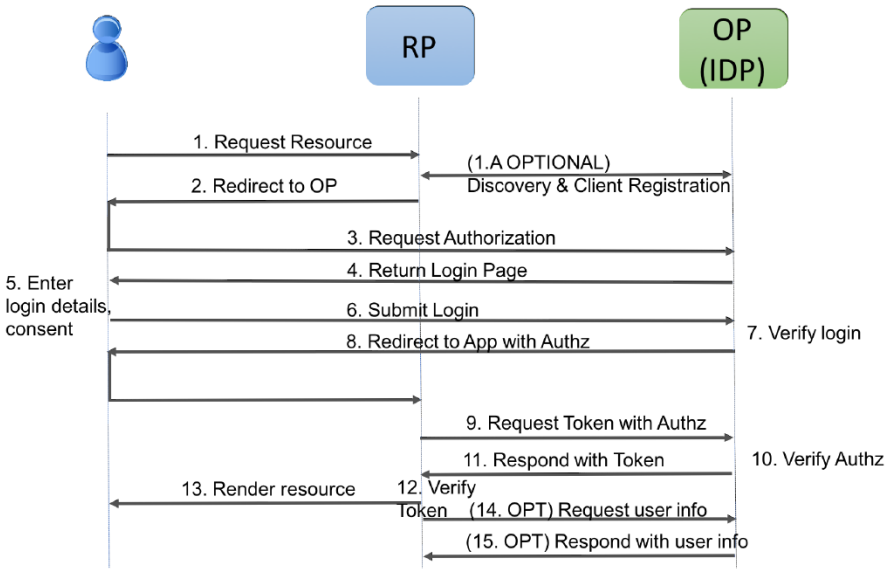
Abbildung 13: SwissID-Ökosyste



Quelle: Präsentation der Swiss Sign Group an Swiss Payment Association, Januar 2019

Eine Person hat grundsätzlich die Möglichkeit, bei mehreren IdP's eine E-ID zu beantragen und kann diese bei den unterschiedlichen Onlinediensten (Relying Parties) nutzen. Die Interoperabilitätsfähigkeit der verschiedenen technischen Lösungen ist zentral für das Funktionieren des gesamten E-ID-Ökosystems. Die SwissID basiert auf dem dezentralen Authentifizierungssystem OpenIDConnect. 2018 haben die beiden Forschenden Dr. Jan Camenisch und Dr. Maria Dubovitskaya von IBM Research einen Evaluationsbericht zum Thema Interoperabilität verfasst. Der gemäss Evaluationsreport beste Lösungsansatz ist derjenige mit direkter Interoperabilität, basierend auf dem „Open-Source“-Protokoll OpenID Connect. OpenID Connect ist eine Erweiterung von OpenID und basiert auf dem OAuth-2.0-Protokoll, welches sichere API-Autorisierungen für Desktop, Web- und Mobileanwendungen zur Verfügung stellt. Nach der Registrierung einer OpenID bei einem OpenID-Provider können sich die Nutzenden bei allen im Ökosystem befindlichen Websites mit dem „Identifier“ (OpenID) anmelden.

Abbildung 14: High-Level-Nachrichtenfluss mit OpenID Connect



Quelle: Camenisch & Dubovitskaya, 2017, Proof of Concept Interoperabilität E-ID, S. 6

2.2.2 2-Faktor-Authentifizierung

Die Zwei-Faktoren-Authentifizierung (2FA) beschreibt den Prozess, bei welchem eine Person zwei unterschiedliche Merkmale aus unterschiedlichen Kategorien bereitstellt, um den Nachweis zu erbringen, dass sie tatsächlich die behauptete Person ist. Die sogenannten Authentifizierungsfaktoren werden dabei in Elemente der drei Kategorien Wissen, Besitz und Inhärenz aufgeteilt. Sie hat zum Ziel, die Sicherheit z.B. beim Zugriff auf ein Online-Konto oder bei einer elektronischen Zahlung zu erhöhen und gleichzeitig das Risiko von Betrug möglichst zu verhindern.

Für die starke Kundenauthentifizierung wird in der Zahlungsdiensterichtlinie unter den Begriffsbestimmungen in Artikel 4 (30) definiert, dass mindestens zwei unabhängige Elemente der Kategorien Wissen, Besitz oder Inhärenz erforderlich sind, und zwar so, dass die Nichterfüllung eines Kriteriums die Zuverlässigkeit der anderen nicht in Frage stellt und die Vertraulichkeit der Authentifizierungsdaten geschützt sind. Die technischen Regulierungsstandards schreiben Sicherheitsanforderungen vor, insbesondere für Mehrzweckgeräte wie Mobiltelefone oder Tablet Computer, welche sowohl für die Erteilung der Anweisung zur Ausführung von Zahlungen als auch für den Authentifizierungsprozess verwendet werden können.

Aufgrund zahlreicher Unklarheiten und Rückfragen von Marktteilnehmenden zu den am 13. Mai 2018 publizierten finalen RTS veröffentlichte die EBA am 21. Juni 2019 ein, nach eigenen Angaben, abschliessendes Positionspapier zur starken Kundenauthentifizierung. „Das Papier richtet sich primär an die national zuständigen Behörden (CAs), soll aber angesichts der damit verbundenen aufsichtsrechtlichen Erwartungen auch für Zahlungsdienstleister (PSPs), Zahlungssysteme und Zahlungsdienstnutzer (PSUs) einschließlich Händlern als Orientierung dienen“ (Core, 2019).

Die EBA beantwortet dabei insbesondere die Frage, welche Verfahren oder Kombinationen von Authentifizierungselementen die Anforderungen von PSD2/SCA erfüllen. Das Papier stellt zudem

klar, dass Elemente, welcher der gleichen Kategorie angehören wie z.B. ein SMS-Einmalpasswort (OTP) und ein dynamischer Kartensicherheitscode, nicht PSD2-konform sind.

Elemente der Kategorie Wissen:

Der PSD2-Artikel 4(30) definiert Wissen als „etwas, was nur [die Nutzerin oder] der Nutzer weiss". Das Wissen soll gemäss EBA bereits vor der Initiierung des Authentifizierungsprozess vorhanden sein. Das bedeutet, dass beispielsweise Informationen, welche man im Rahmen des Authentifizierungsprozesses erhält, nicht als Wissenselemente zugelassen sind.

Die EBA ist der Meinung, dass folgende Elemente zu der Kategorie Wissen gehören könnten:

- Ein Passwort
- Eine Passphrase
- Eine Persönliche Identifikationsnummer (PIN)
- Wissensbasierte Antworten auf eine Herausforderung
- Die Wischsequenz auf einem Mobiltelefon oder Tabletcomputer, um das Gerät zu entsperren („memorized swiping path")

Folgende Elemente gehören laut EBA nicht zu der Kategorie Wissen:

- Karteninformationen, welche auf der Karte aufgedruckt sind, inklusive Sicherheitscode
- Falls der Sicherheitscode nicht auf der Karte aufgedruckt ist und separat von der Karte (analog PIN-Versand) an die Karteninhaberin oder den Karteninhaber zugestellt wird, kann der Sicherheitscode zu der Kategorie Wissen gehören
- Ein Benutzername oder eine Benutzer-ID
- Eine E-Mail-Adresse
- Ein Einmalpasswort (OTP), da es die Bedingung nicht erfüllt, dass es schon vor dem Authentifizierungsprozess bekannt sein muss

Elemente der Kategorie Besitz:

Der PSD2-Artikel 4(30) definiert Besitz als „etwas, was nur [die Nutzerin oder] der Nutzer besitzt". Damit ist nicht nur der physische Besitz gemeint, sondern auch nicht-physische Elemente wie beispielsweise eine mobile Applikation (App) auf einem mobilen Gerät. Der Besitz eines Gerätes kann unter anderem durch den Erhalt eines dynamischen Validierungselementes auf dem Gerät (z.B. OTP oder Push Notification) belegt werden.

Die EBA ist der Meinung, dass folgende Elemente zu der Kategorie Besitz gehören könnten:

- Besitz eines Gerätes (respektive Teilnehmer-Identitätsmodul / SIM-Karte), welches durch den Empfang eines OTP belegt wird
- Besitz eines Gerätes, welches durch eine Signatur belegt wird (Hardware oder Software Token)
- Besitz einer Karte oder Gerätes, welches durch das Scannen eines Quick Response (QR) oder Photo TAN mittels eines externen Gerätes belegt wird
- Besitz eines Gerätes mit Hardware-Sicherheitsmodul (z.B. Trusted-Platform-Module (TPM), Secure Element) oder durch Koppelung einer App mittels eines privaten Schlüssels an ein bestimmtes Gerät oder der Registrierung eines technischen Browser Fingerprints mit gerätespezifischen Merkmalen
- Besitz einer Karte, welche mit einem Kartenlesegerät (Terminal) gelesen wird (kontaktlos und kontaktbehaftet)

- Besitz einer Karte mit einem dynamischen Sicherheitscode

Die EBA ist der Meinung, dass folgende Elemente nicht zu der Kategorie Besitz gehören:

- Auf der Karte aufgedruckte Informationen wie Name, Kartennummer, Verfalldatum und Sicherheitszahl
- Eine gedruckte Liste (oft Streichliste) mit Einmalpasswörtern (OTP)

Elemente der Kategorie Inhärenz:

Der PSD2-Artikel 4(30) definiert Inhärenz als „etwas, was [die Nutzerin oder] der Nutzer ist". In der vorliegenden Arbeit wird der Begriff mit „etwas, was [der Nutzerin oder] dem Nutzer anhaftet" erweitert. Die EBA ist der Auffassung, dass sowohl biologische als verhaltensbiometrische Elemente in die Kategorie Inhärenz gehören könnten. Sie misst der Verwendung von Elementen aus der Kategorie Inhärenz am meisten Innovationspotential bezogen auf reibungslose Authentifizierung zu.

Gemäss der EBA gehören folgende Elemente zu der Kategorie Inhärenz:

- Fingerabdruck
- Stimmerkennung
- Venenerkennung
- Hand- und Gesichtsgeometrie
- Augenhintergrund (Retina) und Iris (Regenbogenhaut)-Scanning
- Tastaturanschlags-Dynamik
- Herzfrequenz (welche beispielsweise von „Waerables" gemessen werden kann)
- Winkel, wie ein mobiles Gerät gehalten wird

Hingegen zählen folgende Elemente nicht zu der Kategorie Inhärenz:

- Informationen, welche über ein Kommunikationsprotokoll wie EMVCo 3D Secure übermittelt werden, da es noch keine Datenelemente für biometrische Informationen in den Versionen 3D Secure 2.1 und 2.2 gibt
- Die Wischsequenz auf einem Mobiltelefon oder Tabletcomputer, um das Gerät zu entsperren („memorized swiping path"), da dies zu der Kategorie Wissen gehört

2.2.3 Biometrische Authentifizierung

Die Biometrie, auch Biometrik, wird als „automatisierte Messung von natürlichen, charakteristischen, physiologischen oder verhaltenstypischen Merkmalen von Menschen zum Zweck der Unterscheidung von anderen Personen" (Privatim, 2006, S. 6) definiert, mit dem Ziel, mittels eines automatisierten Verfahrens Personen aufgrund ihrer Merkmale zu erkennen. Die biometrischen Merkmale sollen folgende Voraussetzungen erfüllen:

- Messbarkeit mittels Sensoren
- Möglichst viele Personen besitzen dieses Merkmal.
- Der Messwert ist möglichst für alle Personen einmalig unterschiedlich.
- Das Alter der Person oder der Zeitpunkt der Messung ist nicht relevant für den Messwert.
- Das Merkmal lässt sich nur sehr schwer und mit viel Aufwand verändern (z.B. durch chirurgische Eingriffe).

Als biometrische Authentifizierungsmerkmale werden unter anderem verwendet:

- Iris (Regenbogenhaut)
- Retina (Augenhintergrund)
- Fingerabdruck
- Gesichtsgeometrie
- Venenstruktur
- Handlinienstruktur
- Stimme (nicht zu verwechseln mit Spracherkennung)
- Unterschrift
- Tastaturanschlagsdynamik
- Computer-Mausbewegungen

Grundsätzliche Funktionsweise und Verfahren

Bei physiologischen Merkmalen erfolgt die Messwertaufnahme über einen Sensor wie beispielsweise eine Kamera oder Fingerabdruckscanner, bei verhaltenstypischen Merkmalen beispielsweise über eine Tastatur und liefert ein biometrisches „Sample". „Im biometrischen Verfahren wird ein spezielles Mustergenerierungs- oder Mustererkennungsverfahren eingesetzt und aus dem Merkmal ein Muster (Template) des Abdrucks des personengebundenen Merkmals generiert (Feature Extraction)" (Privatim, 2006, S. 7). Um den Zugriff auf Mobilgeräte zu bestätigen oder verweigern, werden verschiedene biometrische Authentifizierungsverfahren angewendet. Auf Consumergeräten sind heutzutage Gesichtserkennungstechnologien State-of-the-Art, z.B. FaceID bei Apple-Geräten oder Face Unlock bei Samsung-Geräten. Die Gesichtserkennung besteht aus einem Sensor, der ein Raster von tausenden von Infrarotpunkte auf das Gesicht eines Benutzers projiziert, welche anschliessend von einer Infrarotkamera gelesen werden (Apple, 2019).
Eine mathematische Darstellung des 3D-Rasters wird dann durch ein „Deep Convolutional Neural Network" zugeführt und ein sogenanntes Embedding (Vektor mit n Elementen) wird berechnet. Das neuronale Netzwerk wird so trainiert, dass Embeddings vom gleichen Benutzenden sehr nah zueinander im euklidischen Raum sind und Embeddings von unterschiedlichen Benutzenden weit weg von einander. Die Verlustfunktion, die während des Trainings minimiert wird, wird oft als „triplet loss" bezeichnet. Gemäss Apple ist dieses Verfahren so genau, dass die Wahrscheinlichkeit, dass eine zufällige Person das Gerät einer anderen entsperrt, 1:1000000 ist.

Aus Rohdaten lassen sich über den eigentlichen Verwendungszweck hinaus, Rückschlüsse auf Merkmale ziehen. Beispielsweise kann über ein Gesichtserkennungsverfahren auf das Alter, das Geschlecht oder ein Gesundheitszustand geschlossen werden. Daher werden über komplexe Algorithmen sämtliche für die Erstellung des Templates nicht notwendigen Merkmalen extrahiert. Die Rohdaten sollten, falls sie nicht mehr verwendet werden, sofort gelöscht werden. Wird nun über einen Sensor ein neues Sample erfasst, so kann über einen Merkmalsvergleich ein Vergleichswert (Similarity Score) gegenüber dem Template berechnet werden. Die Verifikationsfunktion macht einen 1:1-Abgleich zwischen den Eingangsdaten und den Referenzdaten (Template) derjenigen Person, als die sich die Nutzerin oder der Nutzer ausgibt, mit dem Ziel, die Identität zu bestätigen oder nicht zu bestätigen. Bei der Identifikation gibt die Nutzerin oder der Nutzer keine Identität an, das System versucht, sie lediglich anhand der biometrischen Eingangsdaten aus der Grundgesamtheit der gespeicherten Referenzdaten zu erkennen.

Die Sicherheit von biometrischen Verfahren hängt von verschiedenen Faktoren ab. Biometrische Verfahren arbeiten mit Wahrscheinlichkeiten, eine 100%-Wahrscheinlichkeit gibt es nicht. So hängen die Leistungskriterien und Fehleranteile unter anderem von der Qualität des Sensors ab, jedoch auch von den aktuellen Umständen wie Temperaturen, Stimmungen, Alterung etc.

Tabelle 2: Leistungskennzahlen von biometrischen Verfahren

False Rejection Rate (FRR)	Anteil der falsch zurückgewiesenen Nutzenden
False Acceptance Rate (FAR)	Anteil der fälschlich vom System zugelassenen Personen
Equal Error Rate (ERR)	FRR und FAR sind voneinander abhängig: steigt die eine, sinkt die andere
Threshold	Grenzwert, ab dem ein Ereignis als akzeptabel klassifiziert werden kann
Failure to enrol rate (FER)	Prozentsatz der Personen, welche vom System nicht erfasst werden können, weil sie nicht über das biometrische Merkmal verfügen oder Schwierigkeiten bei der Erfassung des Merkmals haben (z.B. bei Verätzungen des Fingerabdruckes)

Quelle: Eigene Darstellung in Anlehnung an Privatim, 2006, S. 8

Datensicherheit und Datenschutz

Datensicherheit und Datenschutz sind zentrale Kriterien für die Marktakzeptanz eines biometrischen Authentifizierungsservices. Der Datenschutz konzentriert sich auf den Schutz von personenbezogenen Daten. „Der Begriff Datenschutz ist somit juristischer Natur, da die Begrifflichkeit sämtliche rechtliche Vorschriften, die personenbezogene Daten schützen sollen, erfasst. Beim Datenschutz geht es somit um die rechtlichen Fragen, unter welchen Voraussetzungen personenbezogene Daten erhoben, verarbeitet oder genutzt werden“ (Brands Consulting, 2011).

Für den im Datenschutzrecht geforderten Schutz bietet die Datensicherheit den technischen Schutz dieser Daten durch technische und organisatorische Massnahmen (TOM-Massnahmen), mit dem Ziel, die Vertraulichkeit, Integrität und Verfügbarkeit sicherzustellen. Vertraulichkeit ist die Eigenschaft, dass nur dafür autorisierte Personen und Systeme auf die Daten Zugriff haben, während die Wahrung der Integrität das Ziel hat, dass die Daten nicht verändert oder ungewollt gelöscht werden können. Insbesondere der fremde Zugriff auf Daten aufgrund von technischen Mängeln stellt bezüglich Datensicherheit im Internet eine grosse Herausforderung für sämtliche Unternehmen dar, welche Daten verarbeiten.

In der EU wurde im Mai 2018 die neue Datenschutz-Grundverordnung (DSGVO), im Englischen bekannt als General Data Protection Regulation (GDPR), in Kraft gesetzt. Da es sich im Gegensatz zu PSD2 nicht um eine Richtlinie handelt, muss die Verordnung in den Mitgliedstaaten nicht in nationales Recht umgesetzt werden, sondern sie ist unmittelbar für den gesamten EU-Raum gültig. Die DSGVO regelt die Verarbeitung von personenbezogenen Daten durch private Unternehmen sowie staatliche Akteurinnen und Akteure. „Das Hauptziel des neuen Datenschutzgesetzes

ist die Kontrollmöglichkeit der Daten von betroffenen Personen und die Erkennbarkeit zu erhöhen“ (Snowflake, 2019).

Der extraterritoriale Anwendungsbereich umfasst, im Gegensatz zur bisher gültigen Datenschutzrichtlinie, beispielsweise auch ausserhalb der EU ansässige Unternehmen, da der Wohnort der betroffenen Personen massgeblich ist und nicht wie bisher der Ort der Datenverarbeitung. Dies bedeutet, dass auch in der Schweiz ansässige Unternehmen durch das Marktortprinzip und das Anbieten von Produkten und Dienstleistungen an EU-Bürger/innen neu unter den Anwendungsbereich der DSGVO fallen.

Zur Aufrechterhaltung des Schutzniveaus des schweizerischen Datenschutzgesetzes mit der DGSVO hat der Bundesrat bereits 2011 beschlossen, dass aus dem Jahr 1992 stammende Bundesgesetz über den Datenschutz (DSG) zu überarbeiten und den rasanten technologischen Entwicklungen anzupassen sowie den Entwicklungen auf europäischer Ebene Rechnung zu tragen. Das Gesetz soll 2020 in Kraft treten und sämtliche Schweizer Unternehmen betreffen, welche personenbezogene Daten verarbeiten. Als Verarbeitung gilt das Beschaffen, Speichern, Aufbewahren, Verwenden, Verändern, Bekanntgeben, Archivieren, Löschen oder Vernichten von Daten (Snowflake, 2019).

Die Revision orientiert sich dabei an sieben Leitlinien; risikobasierter Ansatz, Technologieneutralität, Modernisierung der Terminologie, Verbesserung des grenzüberschreitenden Datenverkehrs, Stärkung der Rechte der betroffenen Personen, verbesserter Schutz der betroffenen Personen durch Präzisierung von Verantwortlichkeiten und Pflichten sowie der Stärkung der Kontrolle. Unter der Modernisierung der Terminologie werden Begriffe aus der DSGVO übernommen, so wird beispielsweise der Begriff „Persönlichkeitsprofil“ durch den Begriff „Profiling“ abgelöst.

Zudem umfasst der Begriff besonders schützenswerte Personendaten neu auch genetische und biometrische Daten. „Unter biometrischen Daten sind hier Personendaten zu verstehen, die durch ein spezifisches technisches Verfahren zu den physischen, physiologischen oder verhaltenstypischen Merkmalen eines Individuums gewonnen werden und die eine eindeutige Identifizierung der betreffenden Person ermöglichen oder bestätigen. Es handelt sich dabei beispielsweise um einen digitalen Fingerabdruck, Gesichtsbilder, Bilder der Iris oder Aufnahmen der Stimme. Diese Daten müssen zwingend auf einem spezifischen technischen Verfahren beruhen, das die eindeutige Identifizierung oder Authentifizierung einer Person erlaubt“ (Schweizerische Eidgenossenschaft,2017).

Biometrische Verfahren verstossen nicht grundsätzlich gegen verfassungsrechtliche Rahmenbedingungen und Grundrechte wie die Menschenwürde, Schutz vor Missbrauch der persönlichen Daten, Diskriminierungsverbot oder das Recht auf persönliche Freiheit und Achtung des Privat- und Familienlebens. Grundsätzlich unterliegt die Bearbeitung personenbezogener Daten zur biometrischen Erkennung keinem datenschutzrechtlichen Verbot. Vielmehr ist als Rechtfertigungsgrund die Einwilligung der betroffenen Person einzuholen. Zudem ist auf die Zweck- und Verhältnismässigkeit abzustellen. Die oder der Verantwortliche sollte deshalb stets abwägen, wessen schutzwürdigen Interessen im Einzelfall überwiegen. Trotz der Tatsache, dass die Nutzenden anonym sind, kann man ihr Verhalten mit biometrischen Daten sehr genau analysieren, z.B. anhand der Geschwindigkeit der Tastatureingabe oder der Mausgeschwindigkeit. Aus derartigen Informationen lässt sich z.B. ableiten, ob jemand Rechts- oder Linkshänder ist. Die durch biometrische Verfahren gewonnenen Daten müssen durch technische und organisatorische Sicherheitsmass-

nahmen wie beispielsweise Verschlüsselung bei der Übertragung und Speicherung, Manipulationsverhinderung oder Zutritts- und Zugriffskontrollen geschützt werden. Personendaten dürfen bereits heute schon nur zu dem Zweck bearbeitet werden, der bei der Erhebung der Daten oder Beschaffung angegeben wurde, aus den Umständen ersichtlich oder in einem Gesetz oder einer Verordnung vorgesehen ist (DSG, Art. 4, Abs. 4).

Sofern es möglich ist, sind Personendaten zu anonymisieren oder zu pseudonymisieren. Anonymisierung beschreibt den Vorgang, dass personenbezogene Daten so verändert werden, dass keine Rückschlüsse mehr auf die natürliche Person gezogen werden können und somit endgültig sind, ausser man würde unverhältnismässig viel Aufwand (Kosten) betreiben. Die Pseudonymisierung ersetzt wesentliche Identifikationsmerkmale (z.B. Name und Vorname) durch einen neutralen Datensatz (Pseudonym), so dass die Bestimmung der natürlichen Person ausgeschlossen werden. Verhaltensbiometrische Analysen von Inhärenzfaktoren, wie beispielsweise Tastaturanschlagsaufzeichnungen oder Mausbewegungen, eignen sich für die Pseudonymisierung der Daten, da die effektive Identität der Person für das Authentifizierungsverfahren selbst nicht relevant ist, sondern lediglich eine Verifikation stattfindet zwischen den Eingangsdaten und den Referenzdaten des Zahlungsdienstnutzenden (Karteninhaberin oder Karteninhaber). Durch Pseudonymisierung der Daten untersteht die Bearbeitung von biometrischen Daten einer weniger strengen Datenschutzregelung, da der Bearbeitungszweck nicht personenbezogen ist.

2.3 DAS 3-D-SECURE-PROTOKOLL

Das 3-D-Secure-Protokoll 1.0 ist ein XML-basiertes Kommunikationsprotokoll, welches durch das US-amerikanische Kartenzahlungsnetzwerk Visa entwickelt und im Jahr 2006 unter der Marke „Verified by Visa“ veröffentlicht wurde. Mastercard folgte später mit SecureCode, JCB mit JSecure, Discover mit ProtectBuy sowie American Express mit Safe Key. Ziel der zusätzlichen Sicherheitsvorkehrung war, browserbasierte Online-Zahlungen von Kredit-und Debitkarten im Internet, sogenannte „Card-Not-Present-Zahlungen“, so sicher zu machen wie Zahlungen im Stationärhandel, bei welchen die Karteninhaberin oder der Karteninhaber und die Karte („Card-present“) jeweils beim Zahlvorgang physisch präsent sind, der elektronische Prozessorchip der Karte gelesen wird und die Karteninhaberverifikation mittels PIN erfolgt. Die zusätzliche Sicherheitsschicht soll verhindern, dass beispielsweise mit gestohlenen Kreditkartendaten Online-Zahlungen durchgeführt werden können, da der Prozess eine Authentifizierung der Karteninhabenden gegenüber den Kartenherausgebenden erfordert. Um diesen Vorgang ausführen zu können, ist eine Umleitung an eine Internet-URL des Access Control Servers (ACS) der Kartenherausgeberin notwendig. Das 3-D-Secure-Protokoll 1.0 basiert auf einem 3-Domänen-Modell, in welchem die Acquirer-Domäne und Issuer-Domäne durch die Interoperabilitäts-Domäne verbunden sind, mit dem Zweck, dass sich die Karteninhabenden bei einem elektronischen Kartenzahlungsvorgang gegenüber der Kartenherausgeberin (Issuer) authentifizieren kann. „Bei der Interoperabilität handelt es sich um die Fertigkeit eines Programms oder Systems, wobei die Schnittstellen vollständig offengelegt sind, um eine Integration mit anderen gegenwärtigen oder zukünftigen Produkten oder Systemen ohne Einschränkungen hinsichtlich Zugriff oder Implementierung zu schaffen.“ (Gründerszene, 2019). Das Protokoll 1.0 wurde in einer Zeit entwickelt, in welcher noch keine Smartphones mit entsprechenden Apps existierten. Das Protokoll 1.0 unterstützt lediglich browser-basierte Authentifizierungsprozesse bei Zahlungsvorgängen. „Unter einem […] Wallet wird ein elektronischer Speicher für […] hinterlegte Zahlungsinstrumente verstanden“ (Stengel & Weber, 2016, S. 48).

Um den technologischen Entwicklungen und Ansprüchen gerecht zu werden, wurde am 25. Oktober 2016 durch EMVCo die finale Version des EMVCo-3-Secure-Protokolls veröffentlicht, welches zuvor unter dem Namen 3-D Secure 2.0 bekannt war. EMV bezeichnet den 1994 von **E**uropay, **M**astercard und **V**isa entwickelten Standard für Zahlkarten, welche mit einem Prozessorchip ausgestattet sind und bei einem Zahlvorgang von einem Chipkartenlesegerät wie einem POS-Terminal sowie von Geldautomaten, beispielsweise bei einem Bargeldbezug, elektronisch verarbeitet werden kann. Der Standard für chip-basierte Zahlungsinstrumente liegt aktuell in der Version 4.3 vor. In der Zwischenzeit wurden durch EMVCo nebst 3-D Secure weitere Standards wie beispielsweise Mobile Payment, Tokenisierung, QR-Code oder Secure Remote Commerce veröffentlicht. EMVCo mit Sitz in Delaware (USA) ist durch die sechs Mitgliederorganisationen von American Express, Discover, JCB, Unionpay, Mastercard, Visa sowie zahlreiche Banken, Händler, Prozessoren und anderen Industrievertreter konstituiert. Mit der Migration auf das EMVCo-3-D-Secure-Protokoll wird die Marke „Verified by Visa" ab September 2019 in „Visa Secure" sowie „Mastercard Secure Code" in „Mastercard Identity Check" umbenannt.

2.3.1 Protokoll und Kernfunktionen

Das EMVCo-3-DS-Protokoll und die Kernfunktionsspezifikation wurden im Jahr 2016 in der Version 2.0 veröffentlicht. In der Zwischenzeit folgten diverse Erweiterungen, welche im Protokoll 2.1 am 30. Oktober 2017 sowie in der Version 2.2 am 13. Dezember 2018 publiziert wruden. Das EMVCo-3-DS-Protokoll unterstützt nebst der Zahlungsauthentifizierung neu auch die Nachrichtenkategorie der Nicht-Zahlungsauthentifizierung, wie beispielsweise das Hinzufügen einer Karte in eine digitale Wallet oder das Abfragen eines Kartenkonto-Status. „Des Weiteren unterstützt die neue Version 3-DS 2 die Authentifizierung für In-App-Käufe, Mobile Payments und Wallets (bspw. durch den Einsatz biometrischer Verfahren wie der Fingerabdruck-Authentifizierung) sowie die Nutzung von Transaktionsdaten für die Authentifizierung, was mit der Vorgängerversion 3-DS 1 nicht möglich und auf browser-basierte Transaktionen begrenzt war" (Ingenico, 2019).

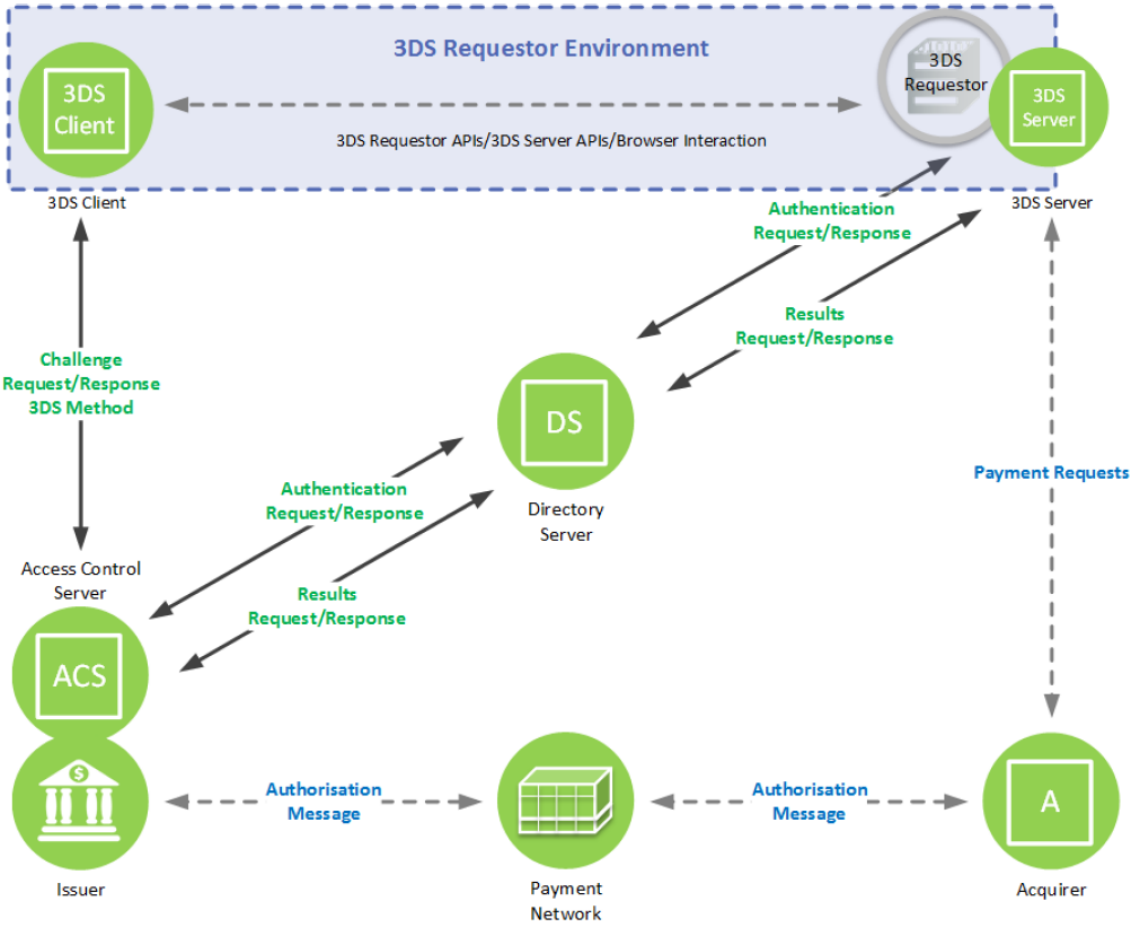
Die Initiierung des 3-DS-Prozesses erfolgt entweder über den Browser der Zahlungsdienstnutzenden oder über eine Händler-App auf einem Smartphone oder Tablet. Die Version 2.2 hat gegenüber der Version 2.1 insbesondere bessere PSD2-SCA-Exemption-Möglichkeiten für eine möglichst friktionslose Authentifizierung und enthält neue Datenelemente hinsichtlich Pre-checkout-Events. Zusätzlich wurden neue Features für Offline-Authentifizierungsanwendungen geschaffen. Die sogenannten Merchant Initiated Transactions (MIT) sind Transaktionen, welche durch den Händler ausgelöst werden. MIT's sind teilweise vom Geltungsbereich der PSD2 ausgenommen und könnten grundsätzlich direkt in den Autorisierungsprozess („direct-to-authorisation") geschickt werden, das Protokoll erlaubt jedoch die Initiierung von sogenannten 3DS-Requestor-Initiated-Zahlungen (3RI-Zahlungen):

- Periodisch wiederkehrende Transaktionen (Recurring) wie beispielsweise Abonnemente
- Ratenzahlungen (Installments)
- Unregelmässige Zahlungen mit gespeicherten Kartendaten (Unscheduled Credential-on-File-Payment, UCoF) wie beispielsweise das Aufladen einer Mobiltelefonkarte beim Unterschreiten eines bestimmten Schwellwertes
- Entkoppelte Authentifizierung (Decoupled Authentication) ist eine Authentifizierungsmethode, bei welcher die Karteninhaberin oder der Karteninhaber nicht zwingend „in-session" sein muss. Das bedeutet, dass die Authentifizierung zu einem späteren Zeitpunkt stattfinden kann.

2.3.2 KOMPONENTEN

Das 3-DS-Modell enthält zahlreiche Komponenten, welche in den Authentifizierungsfluss involviert sind. Die nachfolgende Darstellung und Beschreibung der Komponenten ist direkt der EMVCo-3-DS-Spezifikation 2.2 entnommen. Zugunsten der besseren Lesbarkeit wird bei der Beschreibung der Komponenten nicht jedes Mal einzeln auf die Quelle EMVCo-3-DS-Spezifikation 2.2 verwiesen.

Abbildung 15: 3D-Secure-Domänen und -Komponenten



Quelle: EMVCo 3-DS Spezifikation 2.2

Die **Acquirer Domain** enthält folgende Komponenten:

- 3DS Requestor
- 3DS Client
- 3DS Server
- 3DS Integrator
- Acquirer für Zahlungsautorisierung

3DS Requestor
Die 3DS-Requestor-Komponente leitet die 3-DS-Daten vom dem Gerät, das die Kund/innen nutzen, in den 3-DS-Authentifizierungskanal und initiiert damit den Prozess. Bei einem Zahlungsvorgang repräsentiert die 3DS-Requestor-Komponente typischerweise einen Händler-Webshop. Der 3DS Requestor ist entweder über die 3DS Requestor App oder den Browser mit dem 3DS Client verbunden. Ausserdem hat der 3DS Requestor einen Link zum 3DS Server oder ist direkt in den 3DS Server integriert.

- Bei der app-basierten Variante wird das 3DS SDK in die 3DS Requestor App integriert und zeigt den Karteninhabenden bei der Transaktionsabwicklung das entsprechende User Interface (UI) an.
- Bei der Browser-basierten Variante wird die 3DS Methode genutzt, um Informationen zum Browser oder Consumer Device zu sammeln, damit der ACS dem Browser, im Falle einer Challenge, den Hypertext Markup Language (HTML) Content zur Verfügung stellen kann.

3DS Client
Der 3DS Client ist die Komponente auf dem Kundengerät, welche eine 3-D-Secure-Transaktion initiiert. Die Implementierung kann dabei entweder über eine Händler-App (folgend Merchant App genannt) oder über den Browser erfolgen.

- Bei der App Version ist der 3DS Client das 3DS SDK, welches in der 3DS Requestor App (Merchant App) intergriert ist. Das 3DS SKD sammelt Informationen über das Kundengerät und unterstützt die Authentifizierung auf dem Access Control Server (ACS).
- Bei der browser-basierten Version ist der 3DS Client die 3DS-Methode, welche in die 3DS Requestor Website integriert ist und über den Browser des Consumer Device aufgerufen wird. Durch die 3DS-Methode können zusätzliche Browser Informationen gesammelt werden, welche für risikobasierte Entscheidungen genutzt werden können.

3DS Server
Der 3DS Server stellt die funktionale Schnittstelle zwischen 3DS Requestor Environment und dem Directory Server (DS) dar. Der 3DS Server ist verantwortlich für:

- Sammeln der Datenelemente, welche für die 3DS Nachrichten notwendig sind
- Authentifizierung des Directory Server
- Validierung des Directory Server, des 3DS SDK sowie des 3DS Requestors
- Sicherstellung, dass der Nachrichteninhalt geschützt ist

3DS Integrator (3DS Server und 3DS Client)
Die 3DS-Integrator-Rolle ist im Authentifizierungsprozess zentral, da sie den 3DS Server sowie den 3DS Client funktional verbindet und die Schnittstelle zum Directory Server und ACS bereitstellt.

Acquirer
Der Acquirer ist ein Finanzdienstleister oder eine Bank, welche für folgende Aufgaben zuständig ist:

- Sicherstellen der Kartenzahlungsakzeptanz
- Empfangen von Autorisierungsanfragen vom Händler
- Senden von Autorisierungsanfragen an das Autorisationssystem
- Senden von Autorisierungsantworten an den Händler
- Einreichen von komplettierten Transaktionen in das Settlement-System

Die **Interoperabilitätsdomäne** enthält folgende Komponenten:

- Directory Server (DS)
- Directory Server Certificate Authority (DS CA)
- Autorisationssystem

Directory Server

Der Directory Server ist unter anderem für folgende Funktionen verantwortlich:

- Authentifizierung des 3DS Servers und des ACS
- Routing der Nachrichten zwischen 3DS Server und ACS
- Validierung des 3DS Servers, 3DS SDK und 3DS Requestor
- Definition von spezifischen Programmregeln wie z.B. Logos, Time-out-Werte etc.

Directory Server Certificate Authority

Die Directory Server Certificate Authority generiert den öffentlichen Directory-Server-Schlüssel (Public Key) für das 3DS SDK und generiert die Transport-Layer-Security-Zertifikate (TLS-Zertifikate) für die 3-D-Secure-Komponenten.

Autorisierungssystem

Das Autorisierungssystem ist nicht Teil der 3-D-Secure-Spezifikation, da die Autorisierung grundsätzlich nach der Authentifizierung, aber vor dem Clearing und Settlement durchgeführt wird. Das Autorisierungssystem ist verantwortlich für:

- Empfangen von Autorisierungsanfragen vom Acquirer
- Senden der Autorisierungsanfragen an den Issuer
- Senden der Autorisierungsantwort an den Acquirer
- Bereitstellen von Clearing und Settlement Services für Acquirer und Issuer

Die **Issuer Domäne** enthält folgende Komponenten:

- Karteninhaber/in
- Consumer Device (Kundengerät)
- Issuer
- Access Control Server (ACS)

Karteninhaber/in

Die Karteninhaberin oder der Karteninhaber stellt Kontoinformationen über ein von ihr oder ihm genutztes Gerät (Consumer Device) zur Verfügung. Falls notwendig, wird die Karteninhaberin oder der Karteninhaber dazu aufgefordert, zusätzliche Daten für die Authentifizierung bereitzustellen.

Consumer Device

Das Consumer Device ist in der Lage, eine 3DS Requestor App zu betreiben oder über einen Browser eine Website für die 3-D Secure-Authentifizierung anzuzeigen.

Issuer

Der Issuer ist ein Finanzdienstleister oder eine Bank, welche für folgende Funktionen zuständig ist:

- Ausgabe von Zahlkarten wie Kredit- oder Debitkarten
- Definition der Kartennummernbereiche, welche für die Teilnahme am 3-D Secure-Verfahren zugelassen sind
- Übermitteln der zugelassenen Kartennummernbereiche an den Directory Server

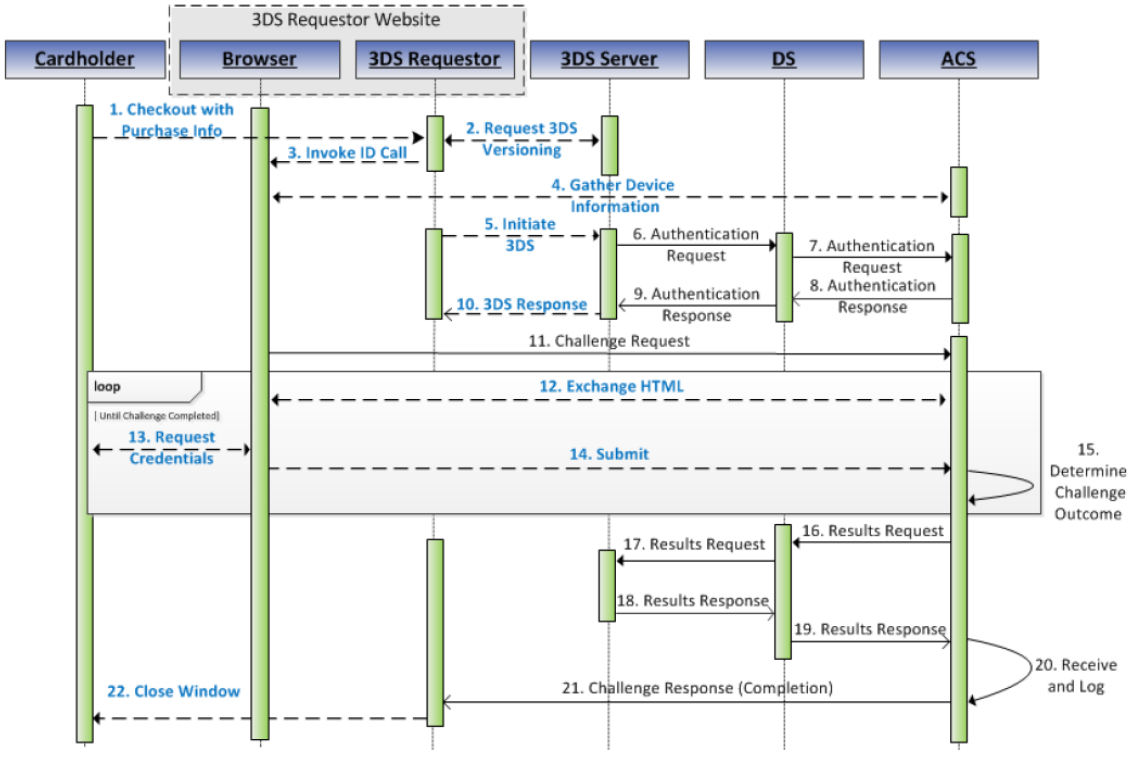
Access Control Server
Der ACS enthält die issuer-spezifischen Authentifizierungsregeln und ist für folgende Funktionen zuständig:

- Überprüfung, ob ein Consumer Device für die 3-D-Secure-Authentifizierung zugelassen ist
- Authentifizierung der Karteninhaberin oder des Karteninhabers oder Bestätigen von Kontoinformationen

2.3.3 AUTHENTIFIZIERUNGSFLUSS

Der Authentifizierungsfluss kann entweder durch die Karteninhaberin oder den Karteninhaber über eine Merchant App, einen Browser oder direkt durch den Händler (ohne Beteiligung der Karteninhabenden) initiiert werden. Sogenannte 3DS-Requestor-Initiated-Transaktionen (3RI-Transaktionen), werden für die Bestätigung eines Kontos verwendet, beispielsweise bei E-Commerce-Händler, welche Abonnementsdienstleistungen (z.B. TV-Abonnemente) anbieten oder bei entkoppelten (decoupled) Authentifizierungen. In dieser Arbeit wird der browserbasierte Ansatz beschrieben, da dieser für die Basis-Produkte-Vision „risikobasierter und adaptiver Authentifizierungsservices“ relevant ist. Beim Frictionless Flow kann die Authentifizierung ohne zusätzliche Kundeninteraktion durchgeführt werden. Falls der ACS aufgrund der Risikoeinschätzung einer Transaktion bestimmt, dass zusätzliche Authentifizierungsfaktoren notwendig sind, wird der Challenge Flow genutzt. Die nachfolgende Darstellung und Beschreibung des Authentifizierungsflusses ist direkt der EMVCo-3-DS-Spezifikation 2.2 entnommen und beschränkt sich auf die für diese Arbeit relevanten Daten und Inhalte. Zugunsten der besseren Lesbarkeit wird bei der Beschreibung des Authentifizierungsflusses nicht jedes Mal einzeln auf die Quelle EMVCo-3-DS-Spezifikation 2.2 verwiesen.

Abbildung 16: Browserbasierter 3-D-Secure-Authentifizierungsfluss



Quelle: EMVCo 3-DS Spezifikation 2.2

Schritt 1:
Die Zahlungsdienstnutzerin oder der Zahlungsdienstnutzer (Cardholder) möchte einen Einkauf auf der Website eines E-Commerce-Händlers mit der Karte bezahlen. Falls die Zahlkartendaten beim Händler nicht hinterlegt sind (Credential-on-File, COF), erfasst die Karteninhaberin oder der Karteninhaber in der Regel ihre bzw. seine Kartennummer, Kartenverfalldatum sowie die dreistellige Kartenprüfnummer (CVV2/CVC2). Dabei interagiert sie oder er durch den Browser auf dem Consumer Device mit dem 3DS Requestor.

Schritt 2:
Der 3DS Requestor liefert die von den Zahlungsdienstnutzenden erfassten Kartendaten an den 3DS Server, um damit die Karteninhaberauthentifizierung zu starten. Die Anfrage beinhaltet die Protokoll-Versionen des Directory Server und ACS und, falls vorhanden, die 3DS Method URL für den spezifische Bankidentifikationsnummer-Bereich (BIN-Bereich). Der 3DS Server liefert die vorgängig vom Directory Server erhaltenen Informationen aus der Preparation Response Message (PRes) sowie die generierte 3DS Server Transaction ID an den 3DS Requestor.

Schritt 3:
Der 3DS Server stellt sicher, dass die 3DS-Methode auf der 3DS Requestor Website ausgeführt wird.

Schritt 4:
Falls im Schritt 2 eine 3DS Method URL an den 3DS Requestor übermittelt wurde, stellt der Browser eine Verbindung über einen sicheren Link mit dem ACS oder einer anderen für die Risikoprüfung vorgesehene Instanz her. Der Issuer hat beim Aufruf der 3DS Method URL die Möglichkeit, durch den Browser der Zahlungsdienstnutzerin oder des Zahlungsdienstnutzers (Cardholder) mittels des eigenen Java Scripts Informationen zum Browser und Kundengerät (Consumer Device) zu sammeln. Die Methode, wie diese Daten abgerufen werden, ist nicht Teil der 3DS-Spezifikation, es muss jedoch sichergestellt werden, dass die 3DS Server Transaction ID Informationen zur Verfügung stellt für einen späteren Abgleich mit dem Browser.

Schritt 5:
Das 3D Requestor Environment sammelt die notwendigen Informationen, welche der 3DS Server für die Erstellung der Authentifizierungsanfrage (AReq) benötigt. Folgende Informationen können in der Anfrage enthalten sein:

- Kontoinformationen
- Risikoeinschätzung des Händlers
- Authentifizierungsinformationen des Händlers
- Informationen zum Vorauthentifizierungsprozess
- Zahlungsinformationen
- Nicht-Zahlungsinformationen

Schritt 1 – 5 sind nicht Teil der EMVCo-3DS-2.2-Spezifikation. Dies ist in der Abbildung 16 mittels gestrichelter Linien dargestellt.

Schritt 6:
Der 3DS Server erstellt die Authentifizierungsanfrage und sendet diesen an den Directory Server.

Der AReq enthält über 100 Datenelemente, welche in verschiedene Kategorien aufgeteilt werden können und relevant für die Issuer-Transaktionsrisikoanalyse sind:

- 3DS-Requestor-Daten
- Kontoinformationen
- Karteninhaberinformation
- Einkaufsinformationen
- Browserinformationen
- Geräteinformationen

Abbildung 17: AReq-Ausschnitt im Java-Script-Object-Notation-Format:


```
{
      "threeDSCompInd":"Y",
      "threeDSRequestorID":"az0123456789",
      "threeDSRequestorName":"Example Requestor name",
      "threeDSRequestorURL":"https://threedsrequestor.adomainname.net",
      "acquirerBIN":"868491",
      "acquirerMerchantID":"mGm6AJZ1YotkJJmOk0fx",
      "addrMatch":"N",
      "cardExpiryDate":"1910",
      "acctNumber":"8944988785642183",
      "billAddrCity":"Bill City Name",
      "billAddrCountry":"840",
      "billAddrLine1":"Bill Address Line 1",
      "billAddrLine2":"Bill Address Line 2",
      "billAddrLine3":"Bill Address Line 3",
      "billAddrPostCode":"Bill Post Code",
      "billAddrState":"CO",
      "email":"example@example.com",
      "homePhone":{
            "cc":"123",
            "subscriber":"123456789"
      },
      "mobilePhone":{
                  "cc":"123",
                  "subscriber":"123456789"
      },
```


Quelle: EMV 3-D Secure JSON Message Samples Version 2.1.0

3DS Requestor: Daten

Unter anderem enthält ein 3D Requestor Daten bezüglich des Device Channels (App, Browser oder 3RI), womit die Transaktion initiiert wurde, und darüber, ob es sich um eine Zahlungstransaktion handelt oder nicht. Bei einer Zahlungstransaktion wird zwischen Einmalzahlung, wiederkehrender Zahlungen (gleicher Händler mit gleichem Betrag) und Teilzahlung unterschieden. Optional kann der 3DS Requestor mitteilen, ob und wie die Karteninhaberin oder der Karteninhaber vor oder während der Transaktion authentifiziert wurde und ob die Authentifizierung erfolgreich war. Folgende Authentifizierungsmethoden stehen zur Verfügung:

- Keine Authentifizierung durchgeführt (z.B. eingeloggt als „Gast“)
- Login Karteninhaber/in Konto durch 3DS Requestor eigene Zugangsdaten
- Login Karteninhaber/in Konto durch Federated ID
- Login Karteninhaber/in Konto durch Issuer-Zugangsdaten
- Login Karteninhaber/in Konto durch Drittparteien-Zugangsdaten
- Login Karteninhaber/in Konto durch FIDO Authentifizierung
- Login Karteninhaber/in Konto durch FIDO Assurance Data signed

- Secure Remote Commerce Assurance Data

Der 3DS Requestor kann sowohl für Zahlungs- als auch Nichtzahlungstransaktionen seine Präferenz bezüglich Challenge angeben. Hat ein Händler beispielsweise bei einer Zahlungstransaktion Zweifel bezüglich der Legitimität der Zahlung, kann er eine Challenge vorschlagen oder verlangen. Wird eine Karte einer digitalen Wallet hinzugefügt, kann ebenfalls eine Challenge notwendig sein. Der 3DS Requestor kann aber auch angeben, dass er keine Challenge erwartet, da beispielsweise bereits eine Transaktionsrisikoanalyse gemacht oder eine starke Kundenauthentifizierung durchgeführt wurde, oder weil die Kundin oder der Kunde den Händler auf eine Whitelist gesetzt hat. „Kund[/innen] können Unternehmen einer Whitelist (‚Positivliste') von ‚vertrauenswürdigen Empfänger[/innen]' zuordnen, die von ihrer Bank oder dem kartenherausgebenden Institut (Issuer) geführt wird. Whitelist-Händler sind von 3D Secure ausgenommen. So können Kund[/innen], die regelmäßig bei einem bestimmten Unternehmen einkaufen, SCA von diesem Zeitpunkt an vermeiden" (Ingenico, 2019).

Zudem kann der 3DS Requestor Informationen mitliefern, wie und wann die Karteninhaberin oder der Karteninhaber in der Vergangenheit bei diesem Händler authentifiziert wurde. Diese Informationen können dem ACS helfen bei der Entscheidungsfindung, ob eine Transaktion stark authentifiziert werden muss oder nicht, wie beispielswiese bei wiederkehrenden Zahlungen, bei denen grundsätzlich nur bei der ersten Transaktion eine starke Authentifizierung verlangt wird.

Konto- und Karteninhaberinformationen
Die Datenelemente zum Karteninhaberkonto enthalten Information, ob es sich um ein Kredit-, Debit- oder Pre-Paid-Konto handelt und welches Verfalldatum die Karte hat. Es stehen ebenfalls Informationen zur Verfügung, wie lange das Konto bereits existiert, wie viele Einkäufe über das Konto getätigt wurden, ob und wann Kontoinformationen wie z.B. Liefer- oder Rechnungsadresse oder das Passwort geändert wurden. Zudem können die Händler angeben, ob mit diesem Konto in der Vergangenheit verdächtige Aktivitäten festgestellt oder Betrugstransaktionen durchgeführt wurden. Die Anzahl der der Einkäufe über dieses Konto können die Händler ebenfalls optional befüllen. Das Konto enthält auch Informationen zu der Rechnungs- und Lieferanschrift wie beispielsweise Adressdaten, aber auch, ob bei diesem Konto eine Lieferadresse bereits früher genutzt wurde.

Einkaufsinformationen
Ein 3DS Requestor hat die Möglichkeit, dem Issuer seine Einschätzung hinsichtlich des Betrugsrisikos bei der spezifischen Transaktion mitzuteilen. Ein wichtiger Indikator ist dabei, welche Liefermethode gewählt wurde.

- Lieferung an die Rechnungsadresse der Karteninhabenden
- Lieferung an eine andere verifizierte Adresse, welche bei den Händlern registriert ist
- Lieferung an eine von der Rechnungsadresse abweichende Lieferadresse
- Lieferung an eine „Pick-up"-Adresse
- Digitale Güter (z.B. Online-Dienstleistungen, elektronische Geschenkkarten etc.)
- Reise- und Veranstaltungsticket, welche nicht verschickt werden

Browserinformationen

- Browser-IP-Adresse
- Java-Aktivierung
- JavaScript-Aktivierung
- Browserspracheinstellung

- Browserfarbtiefe
- Bildschirmhöhe und Bildschirmweite
- Zeitzone
- Browsertyp und Version (UserAgent)
- Challenge Fenstergrösse in Pixels (Breite * Höhe)

Device Informationen
Das 3DS SDK sammelt Device-Informationen, welche verschlüsselt an den ACS übertragen werden.

Abbildung 18: JSON-Beispiel verschlüsselte Device Informationen


```
"},
      "deviceInfo":"ew0KCSJEViI6ICIxLjAiLA0KCSJERCI6IHsNCgkJIkMwMDEiOiAiQW5kc
m9pZCIsDQoJCSJDMDAyIjogIkhUQyBPbmVfTTgiLA0KCQkiQzAwNCI6ICI1LjAuMSIsDQoJCSJDMD
A1IjogImVuX1VTIiwNCgkJIkMwMDYiOiAiRWFzdGVybiBTdGFuZGFyZCBUaW1lIiwNCgkJIkMwMDc
iOiAiMDY3OTc5MDMtZmI2MS00MWVkLTk0YzItNGQyYjc0ZTI3ZDE4IiwNCgkJIkMwMDkiOiAiSm9o
bidzIEFuZHJvaWQgRGV2aWNlIg0KCX0sDQoJIkRQTkEiOiB7DQoJCSJDMDEwIjogIlJFMDEiLA0KC
QkiQzAxMSI6ICJSRTAzIg0KCX0sDQoJIlNXIjogWyJTVzAxIiwgIlNXMDQiXQ0KfQ0K"
}
```


Quelle: EMV 3-D Secure JSON Message Samples Version 2.1.0

Schritt 7:
Der Directory Server empfängt den AReq, führt diverse Validierungen durch und leitet bei erfolgreicher Validierung den AReq an den ACS weiter. Falls die Validierung nicht erfolgreich ist, beendet der DS den Authentifizierungsprozess mit einer Authentication Response (ARes) oder einer Fehlermeldung an den 3DS Server.

Schritt 8:
Der ACS empfängt den AReq und führt diverse Validierungen durch. Er nutzt die Informationen, welche er über die AReq-Nachricht und die 3DS-Methode erhalten hat, um einen Abgleich vorzunehmen. Basierend auf dem Abgleich führt er in Echtzeit eine Transaktionsrisikoanalyse durch und entscheidet, ob er die Authentifizierung vornehmen kann.

In der Praxis ist es häufig der Fall, dass die Transaktionsrisikoanalyse mittels eines Risikobeurteilungs- und Risikoentscheidungssystems erfolgt und nicht anhand des Kern-ACS selbst. Dieses System ist entweder mit dem ACS verbunden oder in den ACS integriert. Beim Frictionless Flow ist keine Interaktion mit der Karteninhaberin oder dem Karteninhaber erforderlich respektive vorgesehen. Der ACS schickt die Authentifizierungsantwort (Authentication Respons, ARes) an den Directory Server.

Abbildung 19: Ausschnitt aus app-basiertem Frictionless-ARes im JSON-Format


```
{
      "threeDSServerTransID":"8a880dc0-d2d2-4067-bcb1-b08d1690b26e",
      "dsReferenceNumber":"DS_LOA_DIS_PPFU_020100_00010",
      "dsTransID":"f25084f0-5b16-4c0a-ae5d-b24808a95e4b",
      "messageVersion":"2.1.0",
      "sdkTransID":"b2385523-a66c-4907-ac3c-91848e8c0067",
      "messageType":"ARes",
      "transStatus":"Y",
      "acsOperatorID":"AcsOpId 4138359541",
      "acsReferenceNumber":"3DS_LOA_ACS_PPFU_020100_00009",
      "acsTransID":"d7c1ee99-9478-44a6-b1f2-391e29c6b340",
      "authenticationValue":"MTIzNDU2Nzg5MDA5ODc2NTQzMjE=",
      "eci":"05"
}
```


Quelle: EMV 3-D Secure JSON Message Samples Version 2.1.0

Bei einer erfolgreichen Frictionless Authentifizierung wird im ARes der Transaktionsstatus auf Y = Authentication Verification Sucessful gesetzt. Weitere mögliche Werte für Transaktionsstatus sind:

Tabelle 3: ARes – Übersicht Transaktionsstatus

Werte	Beschreibung
C	Eine Cardholder Challenge ist notwendig, um die Authentifizierung abzuschliessen.
D	Eine Cardholder Challenge ist notwendig, um die entkoppelte Authentifizierung (Decoupled Authentication) abzuschliessen.
N	Nicht authentifiziert
A	Nicht authentifiziert (3DS von den Händler/-innen angeboten, aber vom Issuer nicht genutzt, da Karte beispielsweise nicht für 3D-Secure registriert ist)
U	Nicht authentifiziert aufgrund von technischen oder anderen Problemen
R	Authentifizierung abgelehnt durch den Issuer mit der Aufforderung, die Transaktion nicht in den Autorisierungsprozess zu schicken
I	Keine Authentifizierung ist notwendig, da die Daten lediglich für Informationszwecke geschickt wurden.

Quelle: eigene Darstellung, angelehnt an EMV 3-D Secure JSON Message Samples Version 2.1.0

Zudem generiert der ACS unter anderem die zahlungsnetzwerkabhängigen Authentifizierungstoken (Authentication Value) sowie den Electronic Commerce Indicator (ECI) und sendet den ARes an den Directory Server.

Tabelle 4: ECI Übersicht bei Mastercard und Visa

Zahlungsnetzwerk	Master-card	Visa
Authentifizierung erfolgreich	02	05
Authentifizierung angeboten, aber nicht genutzt, weil Karte oder Issuer nicht für 3-D Secure registriert ist	01	06
Authentifizierung nicht erfolgreich oder nicht versucht, weil Karte oder Issuer nicht für 3-D Secure registriert ist, technischer Fehler oder falsche Konfiguration	00	07

Quelle: Eigene Darstellung

Schritt 9:
Der Directory Server empfängt den ARes und führt diverse Validierungen durch. Sind die Validierungen erfolgreich, sendet der Directory Server den ARes an den 3DS Server.

Schritt 10:
Der 3DS Server empfängt den ARes und prüft bei einer Zahlungstransaktion, ob der ECI- und Authentication Value für den Autorisierungsprozess vorhanden sind. Der 3DS Server sendet die notwendigen Informationen aus dem ARes an den 3DS Requestor und schliesst bei einem Frictionless Flow den Authentifizierungsprozess ab (Schritt 22 in Abbildung 16).

Falls der ACS eine Challenge verlangt und der 3DS Requestor diese akzeptiert, generiert der 3DS Server den Challenge Request (CReq) und sendet diese über einen serverseitig authentifizierten TLS Link vom Cardholder Browser mittels http POST an die im ARes enthaltene ACS URL.

Abbildung 20: Ausschnitt aus browser-basiertem Challenge-ARes im JSON-Format


```
{
      "messageVersion":"2.1.0",
      "dsTransID":"f25084f0-5b16-4c0a-ae5d-b24808a95e4b",
      "messageType":"ARes",
      "threeDSServerTransID":"8a880dc0-d2d2-4067-bcb1-b08d1690b26e",
      "acsTransID":"d7c1ee99-9478-44a6-b1f2-391e29c6b340",
      "acsReferenceNumber":"3DS_LOA_ACS_PPFU_020100_00009",
      "acsOperatorID":"AcsOpId 4138359541",
      "dsReferenceNumber":"DS_LOA_DIS_PPFU_020100_00010",
      "transStatus":"C",
      "acsChallengeMandated":"Y",
      "acsURL":"https://test.com",
      "authenticationType":"01"
}
```


Quelle: EMV 3-D Secure JSON Message Samples Version 2.1.0

Der Transaktionsstatus wird vom ACS auf = „C“ gesetzt. Falls die Challenge beispielsweise durch eine Regulierung wie PSD2 mandatiert ist, wird das entsprechende Feld vom ACS auf „Y“ gesetzt. Der Authentication Type gibt an, welche Authentifizierungsmethode der Issuer für die Cardholder Challenge nutzen wird. Der Wert „01“ steht für statische Authentifizierung. Die Authentifizierung mittels eines statischen Passwortes wurde durch PSD2 aufgehoben und die Zahlungsnetzwerke

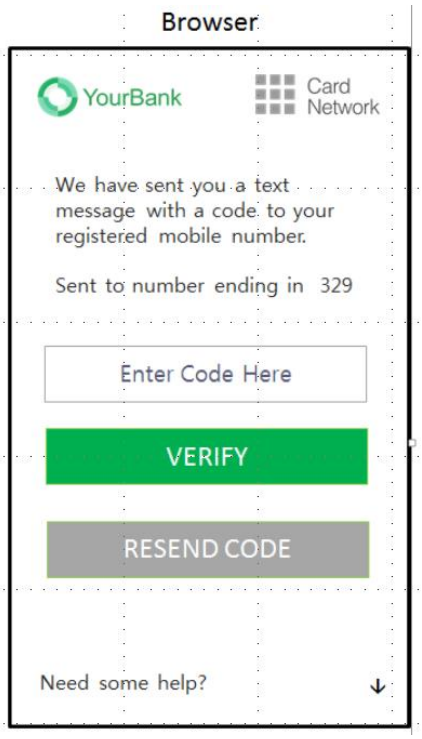
sind seit 1. April 2019 nicht mehr zugelassen. Anerkannt sind dynamische Verfahren, welche eine einmalig gültige und dynamisch erzeugte Authentifizierungsnummer (TAN) generieren, sowie sogenannte Out-of-Band-Authentifizierungsstypen. „Die Out-of-Band-Authentifizierung (OOB) ist eine Form der starken Authentifizierung, bei der neben dem Hauptkanal ein weiterer Kommunikationskanal genutzt wird, um einen zweiten Authentifizierungsfaktor zu schaffen (etwas, das jemand besitzt). Beispiele für Out-of-Band-Kommunikationskanäle sind Datenverbindungen über E-Mail, Smartphone und mobile Geräte, um Einmalpasswörter zu übertragen“ (Safenet, 2019).

Schritt 11:
Der ACS empfängt den CReq vom Browser und führt diverse Validierung durch.

Schritt 12:
Der ACS schickt das ACS UI an den Browser, und dieser zeigt das ACS UI entsprechend dem Cardholder an.

Schritt 13:
Der Cardholder gibt die Authentifizierungsdaten ein, welche vom ACS UI verlangt werden.

Abbildung 21: Browser UI Template für die Eingabe von Authentisierungsdaten



Quelle: EMVCo 3-DS Spezifikation 2.0

Schritt 14:
Der Browser sendet die Daten zur Authentifizierung mittels HTTP POST über den sicheren Kanal (siehe Schritt 10) an den ACS.
Schritt 12 – 14 sind nicht Teil der EMVCo-3DS-Spezifikation.

Schritt 15:
Der ACS prüft die von den Karteninhabenden eingegebenen Authentisierungsdaten. Falls diese korrekt sind, setzt der ACS unter anderem den Transaktionsstatus auf „Y“ und generiert den DS-spezifischen ECI- sowie Authentifizierungswert.

Schritt 16:
Der ACS generiert die Results-Request-Nachricht (RReq) und sendet diese über eine sichere Verbindung an den Directory Server.

Schritt 17:
Der Directory Server empfängt den RReq und sendet diesen über eine sichere Verbindung an den 3DS Server.

Schritt 18:
Der 3DS Server empfängt den RReq, generiert die Result Response (RRes) und schickt diese über eine sichere Verbindung an den Directory Server.

Schritt 19:
Der Directory Server empfängt die RRes und sendet diese mit einer sicheren Verbindung an den ACS.

Schritt 20:
Der ACS empfängt den RRes.

Schritt 21:
Der ACS geniert als Antwort auf den CReq (Schritt 11) die finale Challenge Response Message (CReq) und schickt diese via HTTP POST (z.B. über JavaScript) durch den Browser an die in der AReq angegebene Notification URL.

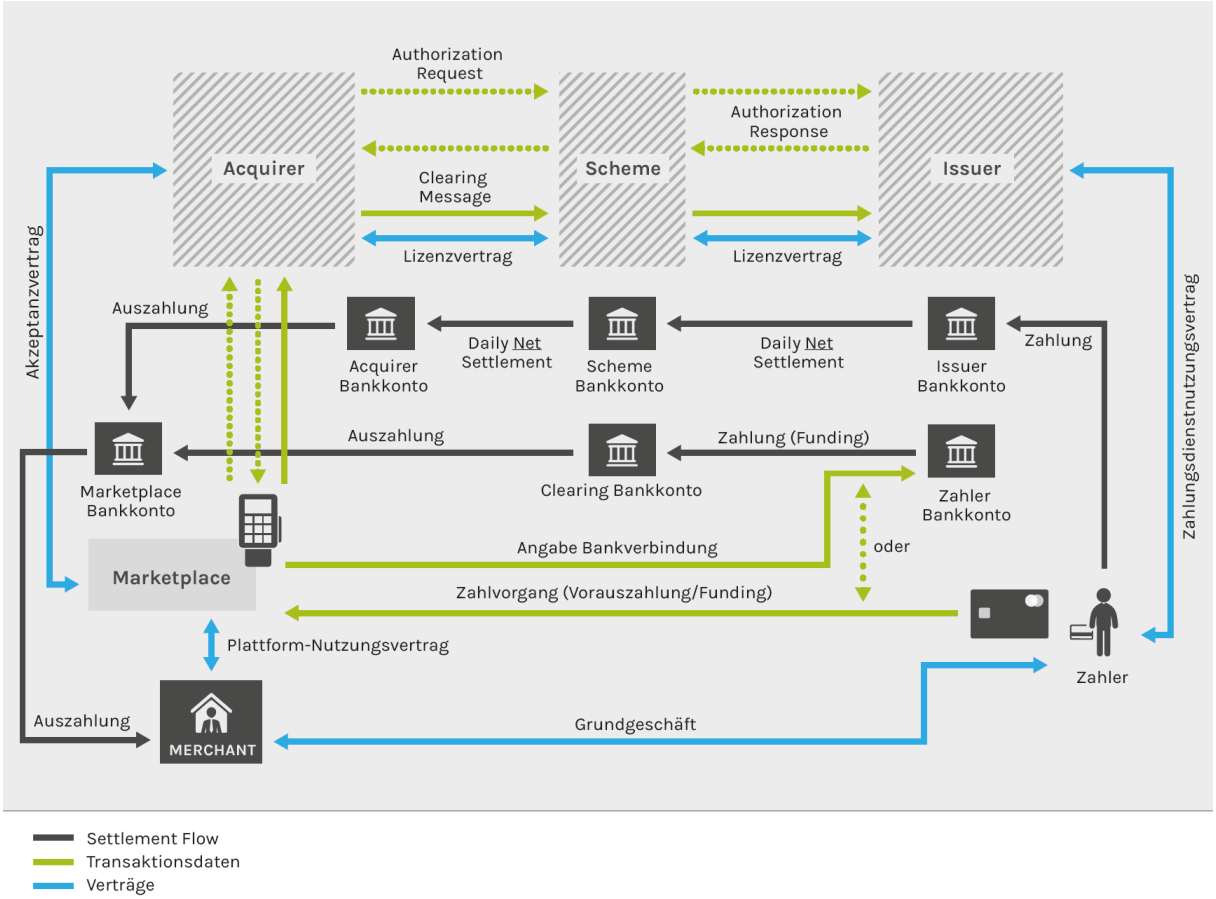
Schritt 22:
Das 3DS Requestor Environment fährt mit dem Checkout-Prozess weiter und schliesst das Authentifizierungsfenster.

Bei einer „Out-of-Band (OOB)“-Challenge-Flow-Authentifizierung sind folgende Schritte unterschiedlich:
Schritt 7: Der ACS erkennt, dass eine OOB-Interaktion mit den Karteninhabenden notwendig ist.

Schritt 12 – 15: Die Karteninhaberin oder der Karteninhaber authentifiziert sich gegenüber dem ACS, Issuer oder einem sonstigen Service Provider durch die Interaktion mit dem ACS. Eine OOB-Kommunikation kann beispielsweise über eine Push Notification in einer Banking App erfolgen. Die Banking App komplettiert die Authentifizierung und sendet das Resultat an den ACS.

Nach einer erfolgreichen Authentifizierung sendet der Händler die Zahlungsanfrage an den Acquirer, damit dieser mit der Autorisierung den Zahlungsabwicklungsprozess starten kann. Der kartenbasierte Zahlungsprozess wird im Rahmen dieser Masterarbeit nicht näher beschrieben. Abbildung 20 gibt eine Übersicht bezüglich der vertraglichen Beziehungen der involvierten Parteien, der Transaktionsflüsse (Autorisierung und Clearing) sowie des Geldflusses (Settlement).

Abbildung 22: Vertragssicht und Zahlungstransaktionsfluss bei einem „Marketplace-Händler“



Quelle: Stengel & Weber, 2016, S. 71

3 METHODISCHE VORGEHENSWEISE

- **Theoretischer Teil**

  Die unter Kapitel 2 angeführten theoretischen Ausführungen stützen sich, unter Berücksichtigung der Forschungsfrage, primär auf Literatur- und Onlinerecherchen sowie auf das bereits vor der Ausarbeitung der Masterarbeit erworbene Fachwissen des Autors, insbesondere im Bereich der Abwicklung von kartenbasierten Zahlungsvorgängen. Alle Informationen ohne Quellenangaben beruhen auf den Kenntnissen des Autors.

- **Empirischer Teil**

  Im empirischen Teil entwickelt der Autor mit dem risikobasierten und adaptiven Authentifizierungsservice ein neues Produkt durch die Kombination von innovativen Verfahren. Um ein tieferes Verständnis von Wirkungszusammenhängen zu gewinnen, kommt in dieser Arbeit mit der Fokusgruppe eine qualitative Methode der Marktforschung zum Einsatz. Die Fokusgruppenmethode hat ihren Ursprung im amerikanischen Raum und wurde für Marktforschungszwecke entwickelt, später aber auch im Rahmen sozialwissenschaftlicher und medizinischer Forschung eingesetzt. Sie wird als ein „Gespräch einer Gruppe von Untersuchungspersonen zu einem bestimmten Thema unter Laborbedingungen“ (Lamnek, 2010, S. 413) beschrieben. Die Methode wurde gewählt, da sie die Interaktion zwischen den Teilnehmenden berücksichtigt. Dies ist zentral, um zu verstehen, wie die Akzeptanz der verschiedenen Authentifizierungsservices aus Sicht der Kund/innen beziehungsweise der Bank ist – auch bezüglich Dimensionen, die vom Forscher nicht vorweggenommen wurden und deshalb von der Gruppe aufgedeckt werden konnten: Die Methode generiert während der Bewertung zusätzliche Anhaltspunkte und deckt neue Aspekte auf, da die Teilnehmenden nicht nur auf die Vorgaben der Forschenden, sondern auch auf die Interaktionen innerhalb der Gruppe reagieren. Die Fokusgruppe leistet insbesondere in dieser frühen Produktentwicklungs-Phase einen guten Beitrag, um sowohl bekannte als auch neue Aspekte aufzudecken.

  Für die vorliegende Untersuchung werden 8 Vertreter/innen von Banken und Finanzdienstleistern bezüglich ihrer Einschätzung der Marktfähigkeit des Services respektive der einzelnen Methoden, welche in den Service integriert werden, befragt. Die Proband/innen bewerten dabei pro Methode sämtliche Dimensionen. Die Assoziationsmessung erfolgt mittels eines semantischen Differentials. Zur Auswertung des semantischen Differentials dient der nicht-parametrische Wilcoxon-Vorzeichen-Rang-Test.

4 EMPIRISCHER TEIL

4.1 BASIS-PRODUKTE-VISION

Im Zeitalter der Digitalisierung von Produkten und Prozessen hat jede Bank den Anspruch, die Bedienung der Kundenschnittstelle sowie das Kundenerlebnis an den Kontaktpunkten, wie beispielsweise der Zugriff auf das Online Banking oder das Auslösen von Zahlungen, so sicher und bequem wie möglich zu gestalten. Durch die rasante technologische Weiterentwicklung der letzten Jahre, aber auch durch neue Regulierungen wie PSD2, welche unter anderem die Innovation von neuen Dienstleistungen im Zahlungsverkehr zum Ziel hat, entstehen neue digitale Visionen, Strategien und Geschäftsmodelle. Die meisten Schweizer Banken haben ihr Kartenzahlungsgeschäft aufgrund der Komplexität der Prozesse und der notwendigen und teuren IT-Infrastruktur sowie zum Zweck der Nutzung von Skaleneffekten (Grenzkostenoptimierung) an einen externen Dienstleister ausgelagert. Der Einsatz von modernen Technologien für die Risikobewertung und Betrugsbekämpfung, welche der Dienstleister einsetzt, führt dazu, dass mehr Betrugstransaktionen erkannt werden, während gleichzeitig die False Decline Rate sinkt und die Anzahl autorisierter Transaktionen (Approval Rates) steigt. Höhere Aproval Rates bei E-Commerce-Transaktionen sind nicht nur aus kommerziellen Überlegungen für die gesamte Wertschöpfungskette essenziell. Die reibungslose und erfolgreiche Abwicklung einer Zahlungstransaktion verbessert das Kundenerlebnis erheblich und steigert damit die Kundenzufriedenheit und Loyalität gegenüber der Akzeptanzstelle, der Kartenherausgeberin und letztlich vor allem auch der Bank.

Das Produkt „Risikobasierter und adaptiver Authentifizierungsservice“ ist aus der Sicht eines Dienstleisters (Issuers) als digitaler Mehrwertservice für die auslagernde Partei (Bank) konzipiert und beschrieben. Die offene Architektur lässt es ohne weiteres zu, dass die Funktion des Services in eine bankeigene Authentifizierungslösung integriert werden kann. Die Basis-Produkte-Vision beinhaltet im Wesentlichen einen reibungslosen kartenbasierten Multi-Faktor-Authentifizierungsservice (MFA) mit folgenden Eigenschaften:

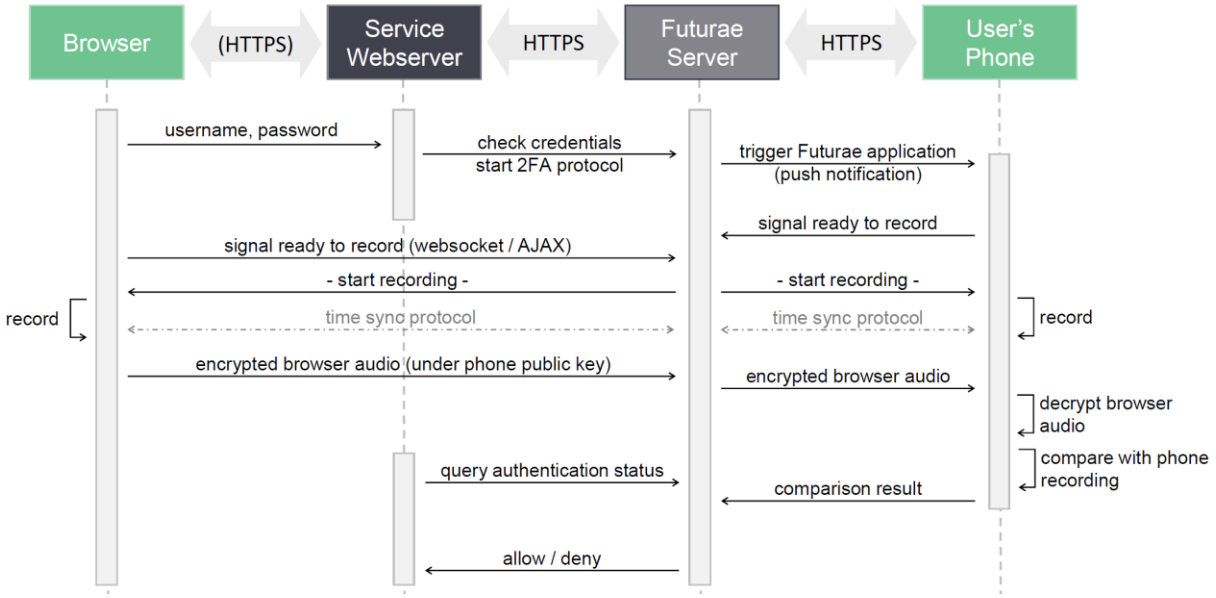
- Eliminierung von Passwörtern oder anderen schwachen Authentisierungsfaktoren bei der Anmeldung (Login) bei der Akzeptanzstelle durch die Nutzung der digitalen Identität, welche bei der Kartenherausgeberin hinterlegt ist
- Sicherung der Qualität der Registrierung analog dem E-ID Sicherheitsniveau „substanziell“, da Identifikation der Person (Kontoinhaber/in, wirtschaftlich Berechtigte/r, Kontrollinhaber/in, Bevollmächtigte/r und Zeichnungsberechtigte/r) durch persönliche Vorsprache bei der Bank oder auf dem Korrespondenzweg gestützt auf einen Ausweis erfolgt (Pass, Identitätskarte, Ausländerausweis)
- PSD2/SCA-konforme, reibungslose und kundenfreundliche Authentifizierung durch die Nutzung von verhaltensbiometrischen Analysen (Inhärenzfaktor) und dem Vergleich von Hintergrundgeräuschen (Besitzfaktor) ohne zusätzliche Interaktion mit den Kund/innen
- Implementierung des „Federated Identity“-Ansatzes mit OpenID Connect basierend auf Oauth 2.0
- Nutzung von RESTful API's für die Kommunikation des Authentifizierungsergebnisses an die Relying Party (Akzeptanzstelle)
- Absicherung von Zahlungstransaktionen durch Nutzung des EMVCo-3D-Secure-Protokolls 2.2
- Verzicht auf starke Kundenauthentifizierung im Zahlungsprozess durch die Anwendung von PSD2/SCA TRA Exemptions bei tiefem Risiko

- Möglichkeit bei Transaktionen mit hohem Risiko, eine Out-Of-Band-Kundenauthentifizierung durchzuführen
- Zusammenführen von Authentifizierungsdaten mit Autorisierungsdaten für Risikobewertung und Betrugsbekämpfung in einem System
- Anreicherungen der Transaktionsdaten mit zusätzlichen Eventdaten vom Kundengerät (Trusted Device) wie Login oder Kontoänderungen für die Entscheidungsfindung
- Kombinierter Einsatz von Machine-Learning-Algorithmen und Modellen (Artificial Intelligence) mit regelbasierten Verfahren (Human Intelligence)

Funktionsweise von ZeroTouch / Soundproof
Die einzigartige Technologie mit dem Vergleich des Hintergrundgeräusches zu Authentifizierungszwecken wurde vom Schweizer ETH-Spin-off-Unternehmen Futurae Technologies unter dem Namen „ZeroTouch“ respektive „Soundproof“ entwickelt.

Bei einem Login-Event triggert das Backend im Browser eine Java-Komponente, die das Mikrofon des Browsergerätes aktiviert, parallel wird auf dem Mobiltelefon des Zahlungsdienstnutzers zeitgleich eine kurze Hintergrundgeräuschaufzeichnung vorgenommen und mittels „Machine-Learning“-Verfahren auf dem Mobiltelefon der Karteninhaberin oder des Karteninhabers abgeglichen. Falls das Browsergerät kein Mikrofon hat, das Mikrofon ausgeschaltet ist oder gerade keine Geräusche im Raum vorhanden sind, wird über die Lautsprecher des Browsergerätes ein Ultraschallsignal (in einer für das menschliche Ohr unhörbaren Frequenz über 20 Kiloherz) ausgegeben und auf dem Mobiltelefon abgeglichen und das Resultat wieder an das Backend zurückgespielt. Durch den Vergleich der Audiodaten (welche nicht als Audiodaten gespeichert werden) kann mit einer hohen Wahrscheinlichkeit berechnet werden, ob sich das Browsergerät sowie das Mobiltelefon am gleichen Ort befinden. Dies ist ein starker Indikator dafür, dass die Anmeldung im Webshop des Händlers durch die Karteninhaberin oder den Karteninhaber und nicht durch eine unbekannte dritte Person mit Betrugsabsichten erfolgt ist.

Abbildung 23: ZeroTouch / Soundproof – High-Level-Authentifizierungsfluss



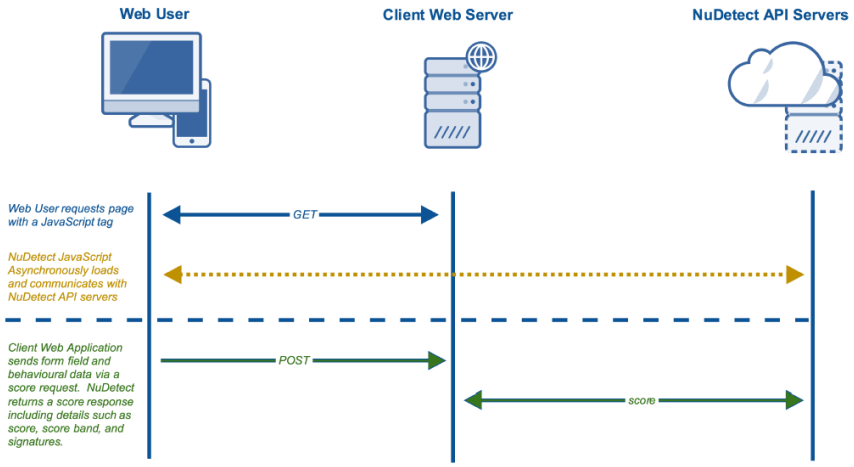
Quelle: Futurae, Technical Slides, S.11

Funktionsweise von NuDetect

NuData Security ist eine kanadische Unternehmung mit Hauptsitz in Vancouver, welche zu den Pionieren in Bezug auf „passive Biometrie“ sowie „verhaltensbiometrische Analyse“ gehört. 2017 wurde NuData Security vom US-amerikanischen Zahlungsnetzwerk übernommen und die NuData-Lösungen wurden in die Mastercard-Produktpalette integriert. Die NuDetect-Lösung ist nach eigenen Angaben eine „Behavioral Analytics Platform“, welche unter anderem Interaktionen von Benutzenden im Browser und in Apps analysiert, um Anomalien und potentiellen Betrug zu entdecken. Für jede Benutzerin oder jeden Benutzer wird aufgrund der Verhaltensmuster ein Profil aus passiven biometrischen Daten (z.B. Tastaturanschlagsdynamik), Informationen zu Geräten, welche die Benutzenden typischerweise bei Online-Zahlungen einsetzen, sowie technischen Verbindungsdaten (z.B. IP-Adresse) erstellt. Einmal angelegte Profile können bei der Akzeptanzstelle beim Login- oder Checkout-Prozess eingesetzt werden, um wiederkehrende Kund/innen zu erkennen oder um beispielsweise betrügerische Kontoeröffnungen durch automatisierte Attacken zu entlarven. Der risikobasierte und adaptive Authentifizierungsservice, welcher für die Authentifizierung die „Federated Identity Credentials“ der Kartenherausgeberin nutzt, leitet die Benutzenden beim Login bei der Akzeptanzstelle auf die Webseite der Kartenherausgeberin um (sogenannter Redirect), welche ebenfalls durch die NuDetect-Lösung geschützt ist. Das „Profiling“ beginnt, sobald die Benutzenden mit der Webseite der Kartenherausgeberin verbunden werden, indem NuDetect im Browser der Benutzenden ein Java Script im Browser ausführt, welches unter anderem passive Biometrie-Daten sammelt und dann die Daten über den Webserver der Kartenherausgeberin über ein API an den NuDetect API Server schickt. Das Backend-System berechnet aufgrund der vom Browser übermittelten Informationen ein dreistufiges Score Band mit einem numerischen Score, welches angibt, ob es sich um einen Event mit tiefem, mittlerem oder hohem Risiko handelt. Zudem werden sogenannte „Behavioral Signals“ an die Kartenherausgeberin übermittelt. Diese beinhalten unter anderem Informationen wie eine ungewöhnliche Anzahl an Login-Fehlversuchen auf einem oder verschiedenen Kontos mit dem gleichen Gerät oder gleichen Ort. Ebenso können Informationen geliefert werden, welche die Inputparameter mit menschlichem Verhalten vergleichen, um so beispielsweise durch Maschinen automatisiertes Ausfüllen von Formularen zu entdecken.

Der Gesamtscore ergibt sich aus der Summe verschiedener Kategorien und berücksichtigt unter anderem Eingabeparameter der „Behavioral Signals“ wie beispielsweise Benutzerkonto, E-Mail-Adresse, E-Mail-Domäne, Device Fingerprint, Broswer-Informationen, IP-Adresse, Proxy Server, Netzwerk-Reputationsanalyse, Tipp-Details, Maussteuerungsdaten, Tastaturanschlagsdynamik etc.

Abbildung 24: NuDetect – Risiko-Score-Anfrage

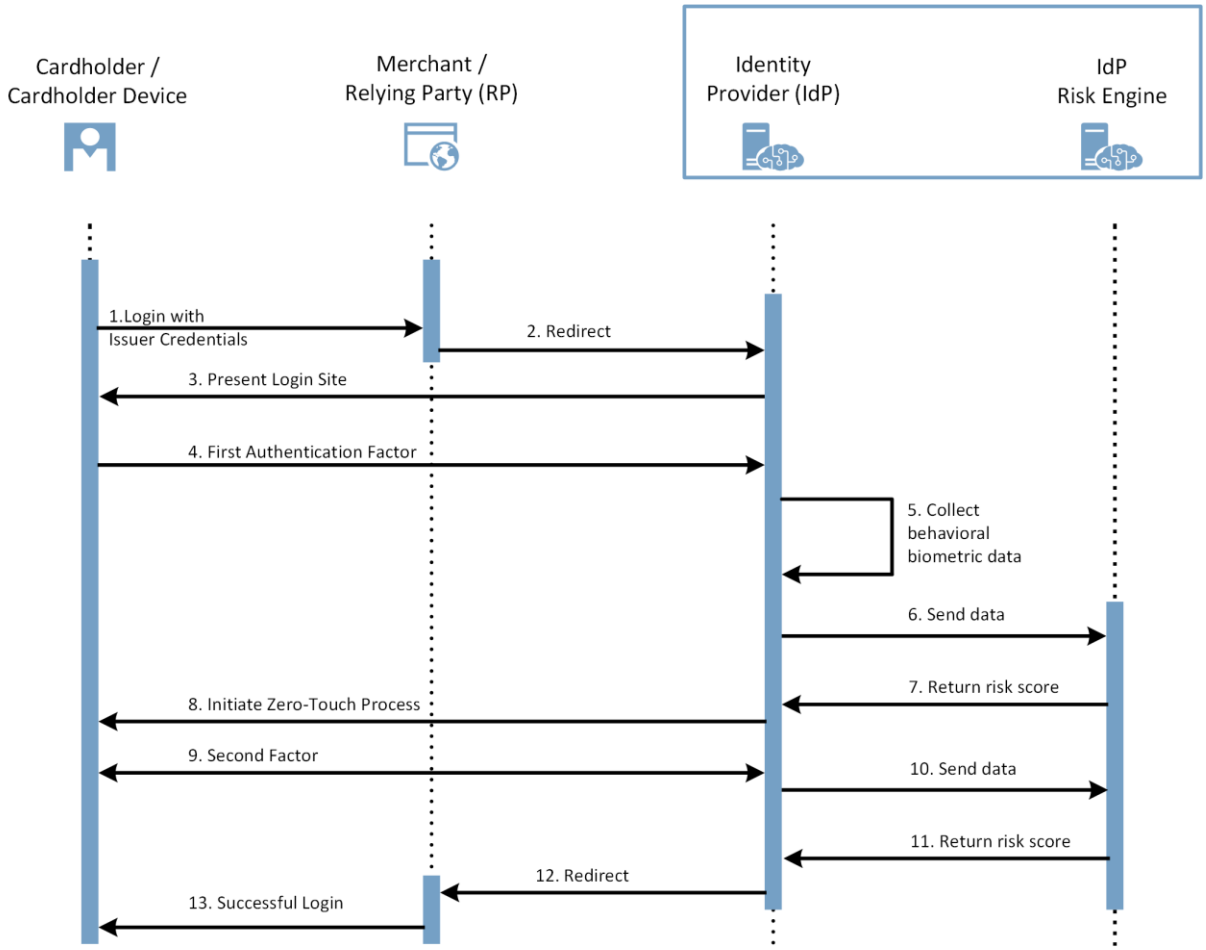


Quelle: NuData, Nudetect Integration Guide 2.2, S. 4

4.2 RISIKOBASIERTER UND ADAPTIVER AUTHENTIFIZIERUNGSSERVICE

Der Authentifizierungsservice und Authentifizierungsfluss basiert auf dem auf dem OpenID Connect / OAuth 2.0 sowie dem 3D-Secure-Protokoll 2.2.

Abbildung 25: Vereinfachte Darstellung einer OpenID Connect Authentifizierung - mit Karten-herausgeber Zugangsdaten



Quelle: Eigene Darstellung in Anlehnung an OpenID Connect

Schritt 1:
Die Karteninhaberin oder Karteninhaber befindet sich auf der Webseite eines Händlers (Relying Party) und möchte sich anmelden.

Schritt 2:
Die Karteninhaberin oder Karteninhaber wählt „Anmelden mit Kartenherausgeberkonto“ und wird durch die Nutzung der OpenID Connect Schicht (basierend auf dem OAuth 2.0 Protokoll) auf die Webseite des Identity Provider (Kartenherausgebers) umgeleitet.

Schritt 3:
Der IdP zeigt der Karteninhaberin oder dem Karteninhaber die Anmeldeseite im Browser an.

Schritt 4:
Die Karteninhaberin oder Karteninhaber gibt im Anmeldformular seine persönlichen Kontoanmeldedaten (Benutzername und Passwort) ein und übermittelt somit den ersten Authentisierungsfaktor aus der Kategorie Wissen an den IdP.

Schritt 5:
Der IdP führt im Browser des Benutzenden ein Java Script aus und sammelt unter Anderem verhaltensbiometrische Daten wie beispielsweise Tastaturanschlagsdynamik, Tippverhalten oder Mausbewegungen

Schritt 6:
Der IdP übermittelt die biometrischen Daten, sowie die „Behavioral Signals“ an das System für die Risikobewertung und Betrugsbekämpfung.

Schritt 7:
Das System für die Risikobewertung und Betrugsbekämpfung berechnet aufgrund der vom Browser übermittelten Informationen ein Score Band mit einem numerischen Score, welches angibt, ob es sich um einen Event mit tiefem, mittlerem oder hohem Risiko handelt.

Falls das System für die Risikobewertung und Betrugsbekämpfung einen Event mit tiefem Risiko ermittelt hat, wird der Prozess bei Schritt 12 weitergeführt.

Schritt 8:
Falls das System für die Risikobewertung und Betrugsbekämpfung einen Event mit mittlerem oder hohem Risiko ermittelt hat, wird der Zero-Touch Authentifizierungsprozess initiiert.

Schritt 9:
Der IdP triggert im Browser des Benutzenden eine Java-Komponente, die das Mikrofon des Browsergerätes aktiviert, parallel wird auf dem Mobiltelefon des Zahlungsdienstnutzers zeitgleich eine kurze Hintergrundgeräuschaufzeichnung vorgenommen und mittels „Machine-Learning“-Verfahren auf dem Mobiltelefon der Karteninhaberin oder des Karteninhabers abgeglichen.

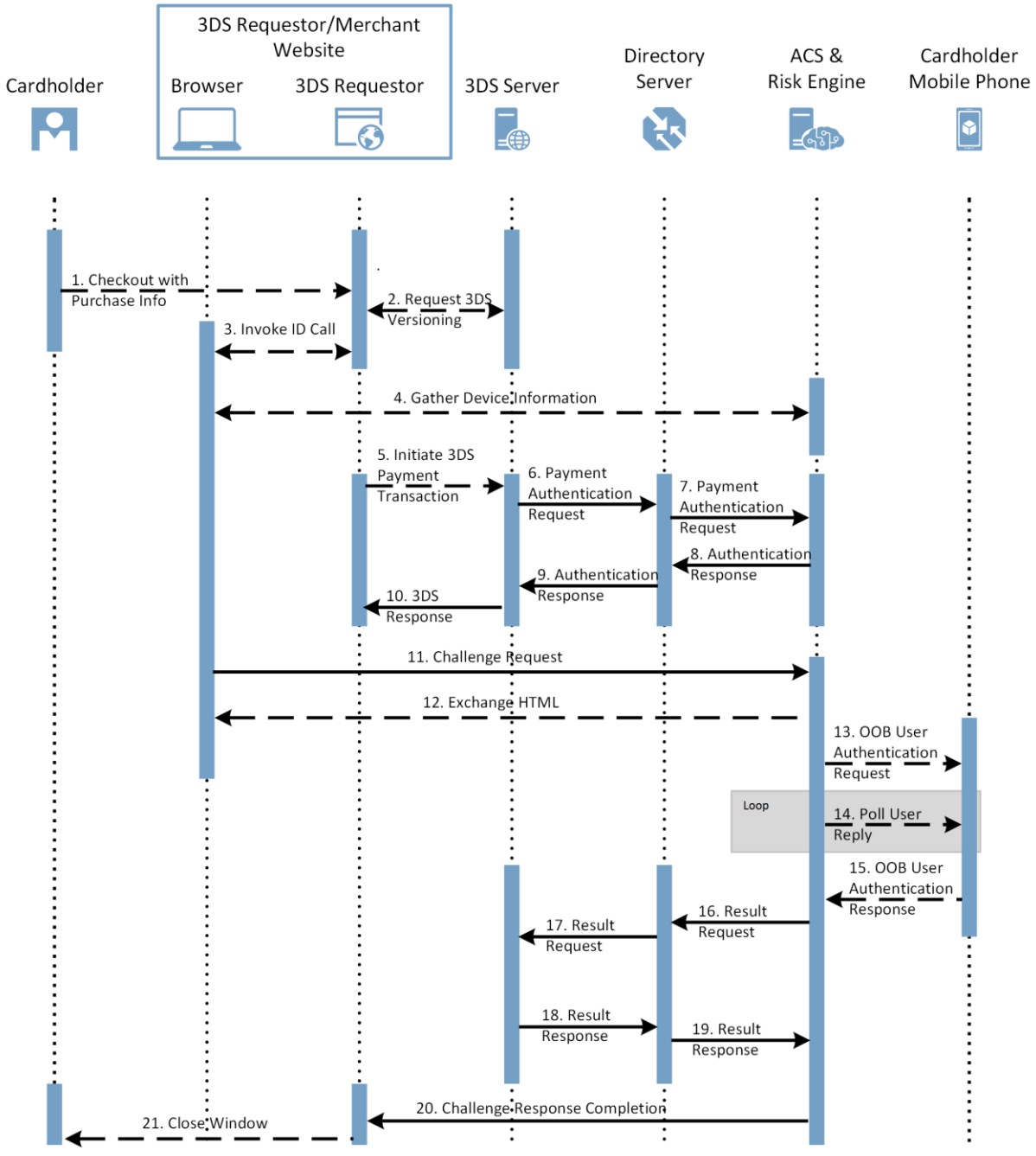
Schritt 10:
Das System für die Risikobewertung und Betrugsbekämpfung berechnet mit den Vergleichswerten der Audiodaten die Wahrscheinlichkeit, ob sich das Browsergerät sowie das Mobiltelefon am gleichen Ort befinden und berechnet den entsprechenden Risiko-Score.

Schritt 11:
Das System für die Risikobewertung und Betrugsbekämpfung sendet den Risiko-Score an den IdP. Der IdP entscheidet aufgrund des Risiko-Scores, ob die Authentifizierung erfolgreich abgeschlossen werden kann.

Schritt 12:
Bei einer erfolgreichen Authentifizierung wird die Karteninhaberin oder Karteninhaber wieder auf die Webseite des Händlers umgeleitet und ist somit auf der Webseite des Händlers angemeldet.

Schritt 13:
Der Händler meldet der Karteninhaberin oder dem Karteninhaber, dass die Anmeldung erfolgreich war.

Abbildung 26: Browserbasierter 3-D-Secure-Authentifizierungsfluss OOB-Authentifizierung



Quelle: Eigene Darstellung in Anlehnung an EMVCo Transaktionsfluss

Schritt 1:
Die Karteninhaberin oder Karteninhaber startet den Zahlvorgang und erfasst die Kartendaten. Der Händler möchte seine Transaktionen über das EMVCo 3D Secure Protokoll absichern um damit die Haftungsumkehr zu erwirken.

Schritt 2:
Der 3DS Requestor liefert die von den Karteninhabenden erfassten Kartendaten an den 3DS Server, um damit Authentifizierungsprozess zu starten. Die Anfrage beinhaltet die Protokoll-Versionen des Directory Server und ACS und die 3DS Method URL für den Bereich der spezifischen Bankidentifikationsnummer (BIN). Der 3DS Server meldet die 3D Secure-Protokollversionen, welche sowohl auf dem Directory Server als auch ACS zur Verfügung stehen an den 3DS Requestor zurück. Für die hier vorgestellte Variante ist die 3D Secure Version 2.2 Voraussetzung für die Abwicklung.

Schritt 3:

Der 3DS Server stellt sicher, dass die 3DS-Methode auf der 3DS Requestor Website ausgeführt wird.

Schritt 4:
Der Browser stellt eine Verbindung über einen sicheren Link mit dem ACS respektive dem System für die Risikobewertung und Betrugsbekämpfung her. Der ACS führ über die 3DS Method URL im Browser des Benutzenden ein Java Script aus und sammelt unter Anderem verhaltensbiometrische Daten wie beispielsweise Tastaturanschlagsdynamik, Tippverhalten oder Mausbewegungen und übermittelt diese, sowie „Behavioral Signals“ an das System für die Risikobewertung und Betrugsbekämpfung.

Schritt 5:
Das 3D Requestor Environment sammelt die notwendigen Informationen, welche der 3DS Server für die Erstellung der Authentifizierungsanfrage (AReq) benötigt.

Schritt 6:
Der 3DS Server erstellt die Authentifizierungsanfrage und sendet diese an den Directory Server. Der AReq beinhaltet unter anderen folgenden spezifischen Wert:

- Message Category: „01“ = Payment Authentication
- 3DS Requestor Authentication Method: „04“ = Login to the cardholder account at the 3DS Requestor system using issuer credentials
- 3DS Requestor Challenge Indicator: „07“ = No Challenge Requested (strong consumer authentication is already performed)

Schritt 7:
Der Directory Server empfängt die AReq, führt diverse Validierungen durch und leitet bei erfolgreicher Validierung die AReq an den ACS weiter.

Schritt 8:
Der ACS empfängt den AReq und leitet nach erfolgreicher Validierung die Daten an das System für die Risikobewertung und Betrugsbekämpfung weiter. Dieses prüft in Echtzeit, ob für diese Zahlungstransaktion eine gültige Authentifizierung aus dem Anmeldeprozess beim Händler mittels

Kartenherausgeber Anmeldedaten vorliegt. Basierend auf diesen Informationen und den Information aus dem AReq führt das System für die Risikobewertung und Betrugsbekämpfung eine Transaktionsrisikoanalyse durch und entscheidet, ob die Authentifizierung reibungslos (Frictionless-Flow) vorgenommen werden kann. Falls die Authentifizierung für den Zahlungsprozess keine Kundeninteraktion erfordert sendet der ACS die Authentication Response (ARes) an den Directory Server.

Der ARes kann unter anderem folgenden spezifischen Werte enthalten:

- Transaction Status: „Y“ = Authentication Verification successful
- ECI Value (z.B. bei Mastercard): „02“ = 3DS Authentication is successful, both card and issuing bank are secured by 3DS
- Authentication Value: zahlungsnetzwerkabhängiger Base64 symmetrisch verschlüsselter Wert

Falls der ACS aufgrund einer hohen Risikobewertung eine starke Kundenauthentifizierung verlangt, sendet der ACS die Authentication Response (ARes) an den Directory Server.

Der ARes kann unter anderem folgenden spezifischen Werte enthalten:

- Transaction Status: „C“ = Challenge Required; Additional authentication is required using the CReq/Cres
- ACS Challenge Mandated Indicator: „C“ = Challenge is mandated
- ACS URL: Fully Qualified ACS URL
- Authentication Type: 03 = Out-of-Band (OOB)

Schritt 9:
Der Directory Server empfängt den ARes und führt diverse Validierungen durch. Sind die Validierungen erfolgreich, sendet der Directory Server den ARes an den 3DS Server.

Schritt 10:
Der 3DS Server empfängt den ARes und sendet die notwendigen Informationen aus dem ARes an den 3DS Requestor. Falls der ACS im Schritt 8 eine erfolgreiche Authentifizierung rückmeldet, ist der Authentifizierungsprozess hier abgeschlossen.

Falls der ACS eine Challenge verlangt und der 3DS Requestor diese akzeptiert, generiert der 3DS Server den Challenge Request (CReq) und sendet diese über einen serverseitig authentifizierten TLS Link vom Cardholder Browser mittels http POST an die im ARes enthaltene ACS URL.

Der Cardholder hat jedoch die Möglichkeit den Authentifizierungsprozess abzubrechen. In diesem Fall würde der Challenge Cancelation Indicator = „01“ Cardholder selected „Cancel“ gesetzt.

Schritt 11:
Der ACS empfängt den CReq vom Browser und führt diverse Validierungen durch.

Schritt 12:
Falls der Cardholder die Challenge nicht abgebrochen hat, sendet der ACS der Karteninhaberin oder dem Karteninhaber über den Browser Instruktionen, wie die Authentifizierung erfolgt.

Schritt 13:
Der ACS startet die „Out-Of-Band"-Authentifizierung und schickt beispielsweise über Apple Push Notification Service (APNS) oder Google Firebase Messaging (FCM) eine sogenannte „Actionable Push Notification" auf das Mobiltelefon (Trusted Device) der Karteninhaberin oder des Karteninhabers. Dies hat den Vorteil, dass sich im Hintergrund (falls gewollt auch im Vordergrund) automatisch die Authentifizierungs-App der Kartenherausgeberin öffnet, wenn die Karteninhaberin oder der Karteninhaber die Notification antippt. In der Push Notification wird den Karteninhabenden der Name des Händlers, der zu autorisierenden Betrag sowie die Währung angezeigt sowie die Möglichkeit, die Transaktion zu akzeptieren oder abzulehnen. Optional kann die Authentifizierung um einen Faktor wie beispielsweise „Fingerprint" oder „FaceID" erweitert werden, um eine starke 2-Faktor-Authentifizierung zu erhalten, welche PSD2-konform ist. Die von Issuer entwickelte und mittels kryptographischer Verfahren an das Gerät der Karteninhaberin oder des Karteninahbers gekoppelte App entspricht dabei dem Faktor Besitz, optional ergänzt durch den Inhärenzfaktor, welcher durch das aktive biometrische Verfahren involviert wird.

Schritt 14:
Um das Resultat der OOB-Authentifizierung zu erhalten, initiiert der ACS eine zyklische Abfrage (Polling).

Schritt 15:
Der ACS empfängt das Resultat der OOB-Authentifizierung und validiert es.

Schritt 16:
Der ACS generiert die Results Request (RReq) und sendet diese über eine sichere Verbindung an den Directory Server.

Der RReq kann beispielsweise unter anderem folgende Informationen enthalten:
- Transaction Status: „Y" = Authentication Verification Successful
- Authentication Method: „07" = OOB Biometrics
- Authentication Value: zahlungsnetzwerkabhängiger Base64 symmetrisch verschlüsselter Wert
- Electronic Commerce Indicator (ECI): „02" = 3DS Authentication is successful, both card and issuing bank are secured by 3DS.

Schritt 17:
Der Directory Server empfängt den RReq und sendet diesen über eine sichere Verbindung an den 3DS Server.

Schritt 18:
Der 3DS Server empfängt den RReq und generiert die Result Response und schickt diese über eine sichere Verbindung an den Directory Server.

Die RRes kann beispielsweise unter anderem folgende Informationen enthalten:
- Results Message Status: „01" = RReq received for further processing

Schritt 19:
Der Directory Server empfängt die RRes und sendet diese anhand einer sicheren Verbindung an den ACS.

Schritt 20:
Der ACS empfängt den RRes und generiert als Antwort auf den CReq (Schritt 11) die finale Challenge Response Message (CReq) und schickt diese via HTTP POST (z.B. über Java Script) durch den Browser an die in der AReq angegebene Notification URL.

Schritt 21:
Das 3DS Requestor Environment schliesst das Authentifizierungsfenster.

Der Händler kann nun bei der Händlerbank (Acquirer) die Zahlungstransaktion für die Autorisierung einreichen. Da vorgängig eine reibungslose starke Kundenauthentifizierung mit den „Issuer Credentials“ erfolgt ist und im Falle eines hohen Risikos zusätzlich noch eine OOB SCA erforderlich ist, ist die Betrugswahrscheinlichkeit auf der zur Authentifizierung verknüpften Autorisierungstransaktion sehr tief. Falls der Kartenstatus „aktiv“ ist und der zu autorisierende Betrag nicht über der verfügbaren Limite liegt, wird die Kartenherausgeberin die Zahlungstransaktion autorisieren. Der Händler hat nun die Möglichkeit, die erfolgreich autorisierten Transaktionen in die Clearing- & Settlement-Prozesse zu schicken.

4.3 PRÜFUNG DER MARKTFÄHIGKEIT

Um die Marktchancen eines risikobasierten und adaptiven Authentifizierungsservices zu prüfen, wurden Vertreter/innen der Schweizer Finanzindustrie im Rahmen Fokusgruppe befragt. Damit der Datenschutz und die Anonymität der Testpersonen gewährleistet werden konnten, nahm ein auf Marktforschung spezialisiertes Unternehmen die Rekrutierung der Proband/innen vor. Das Unternehmen unterliegt als Mitglied von ESOMAR (European Society for Opinion and Market Research) dem internationalen Kodex für die Markt- und Sozialforschung. Der ESOMAR-Kodex wurde 1948 von der internationalen Handelskammer (ICC) veröffentlicht, die aktuellste Version wurde 2017 publiziert und wird von mehr als 60 Vereinigungen in über 50 Ländern unterstützt. Der Kodex setzt Standards für ethisches und professionelles Verhalten bei der Durchführung von Forschung. Die grundlegenden Prinzipien schreiben unter anderem vor, dass die Forschenden klar über den Zweck informieren und darüber, welche Daten sie erheben und an wen die Daten übermittelt werden. Zudem müssen die Forschenden die Daten vor unbefugten Zugriffen schützen und dürfen sie ohne Zustimmung der Teilnehmenden nicht offenlegen.

Die Selektionskriterien für die Rekrutierung beinhalten folgende Anforderungen:

- Geschäftsleitungsmitglieder von Banken, oberes und mittleres Kader aus der Finanzindustrie, welche sich mit den Themen Zahlungsverkehr und Kartengeschäft auskennen
- Die Teilnehmenden wissen, was PSD2 ist, und sind idealerweise auch von den Konsequenzen respektive Auswirklungen betroffen. Der Fokus liegt dabei auf dem Thema „starke Kundenauthentifizierung“.
- Die Teilnehmenden können in ihrer Funktion Entscheidungen für ihren Zuständigkeitsbereich treffen.

Die Befragung wurde in speziell für Marktforschungen ausgestatteten Räumlichkeiten der Rekrutierungsgesellschaft durchgeführt. Die Proband/innen unterzeichneten vor dem 2-stündigen Anlass eine Einverständniserklärung für die Tonaufnahme sowie eine Geheimhaltungserklärung. Die Fokusgruppe wurde durch einen erfahrenen Moderator geleitet, der bei einer auf Kundenfokusthemen spezialisierten Unternehmung beschäftigt ist. Der Forscher war während der Durchführung ebenfalls im Raum anwesend, machte sich Notizen zum Gesprächsverlauf und beantwortete inhaltliche Fragen der Proband/innen. Um die Anonymität auch während der Durchführung der Fokusgruppe gewährleisten zu können, stellten sich die Teilnehmenden nur mit Vornamen vor. Erst am Ende des Anlasses stellte der Forscher sich selbst und seine konkreten Forschungsabsichten vor.

Die zentrale Forschungsfrage lautet, wie die Proband/innen unsichtbare und friktionslose Authentifizierungsmethoden gegenüber etablierten Verfahren hinsichtlich der folgenden zwölf Dimensionen einschätzen:

- Sicherheit der Lösung
- Datenschutz
- Anonymität der Kund/innen
- Privatsphäre der Kund/innen
- Einfachheit in der Handhabung
- Bequemlichkeit und Komfort
- Kundenerlebnis in der Anwendung
- Vertrauen in die Lösung

- Generelle Akzeptanz der Lösung durch die Kund/innen
- Innovationskraft
- Möglichkeiten der Monetarisierung
- Implementierungsaufwand der Lösung für die Bank

Die fünf Authentifizierungsmethoden wurden auf ausgedruckten Postern im DIN-A1-Format visualisiert und beschrieben. Die grundsätzliche Funktionsweise der verschiedenen Methoden sowie die Abgrenzung der Begriffe „Authentisierung“ und „Authentifizierung“ gegenüber der nicht forschungsrelevanten Autorisierung erklärte der Forscher den Teilnehmenden.

Abbildung 27: Fokusgruppe – Definition der Forschungsbegriffe und Abgrenzung

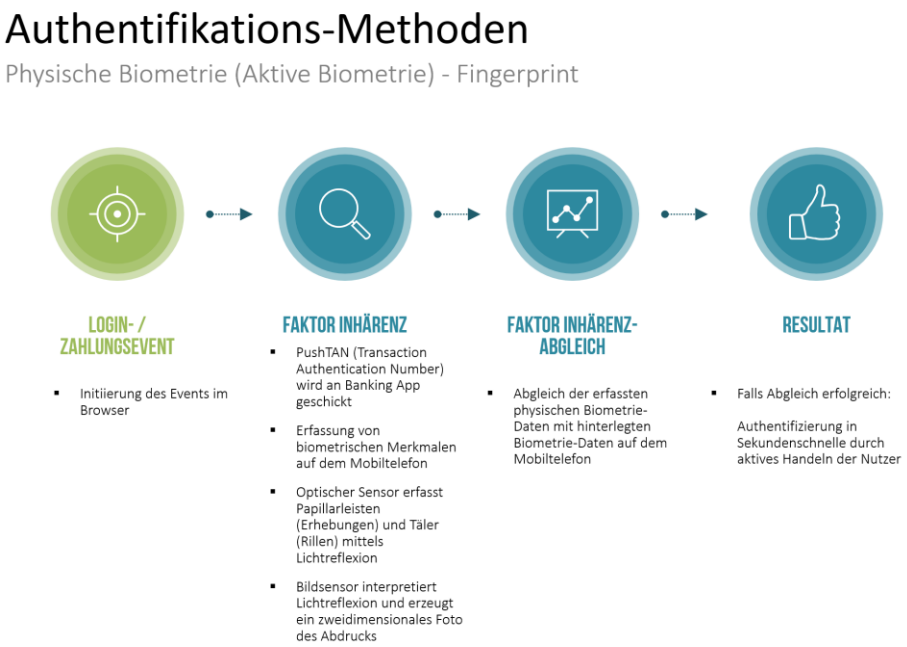
Quelle: Eigene Darstellung

Um einen allfälligen Sequenzeffekt zu verringern (z.B. wäre es plausibel, dass die Teilnehmenden neue Methoden besser bewerten, nur weil sie nach den bekannten Methoden vorgestellt werden), wurde die Reihenfolge der Methoden zufällig mittels Losverfahren bestimmt. Ausserdem waren die Proband/innen nach dem Vorstellen jeder weiteren Variante dazu aufgefordert, die bereits vorgenommen Bewertungen der vorangegangen Methoden anzupassen, falls sie dies wollten.

Zudem sollten die Teilnehmenden nur die vorgestellte Methode an sich bewerten und nicht die Kombination von Methoden, beispielsweise im Rahmen einer 2-Faktor-Authentifizierung. Aus diesem Grund wurde jedem Verfahren als Startpunkt eine generische Initiierung eines Log-ins oder Zahlungsevents vorangestellt.

Physische Biometrie (Aktive Biometrie)

Abbildung 28: Fokusgruppe – Fingerabdruckerkennung (Aktive Biometrie)



Quelle: Eigene Darstellung

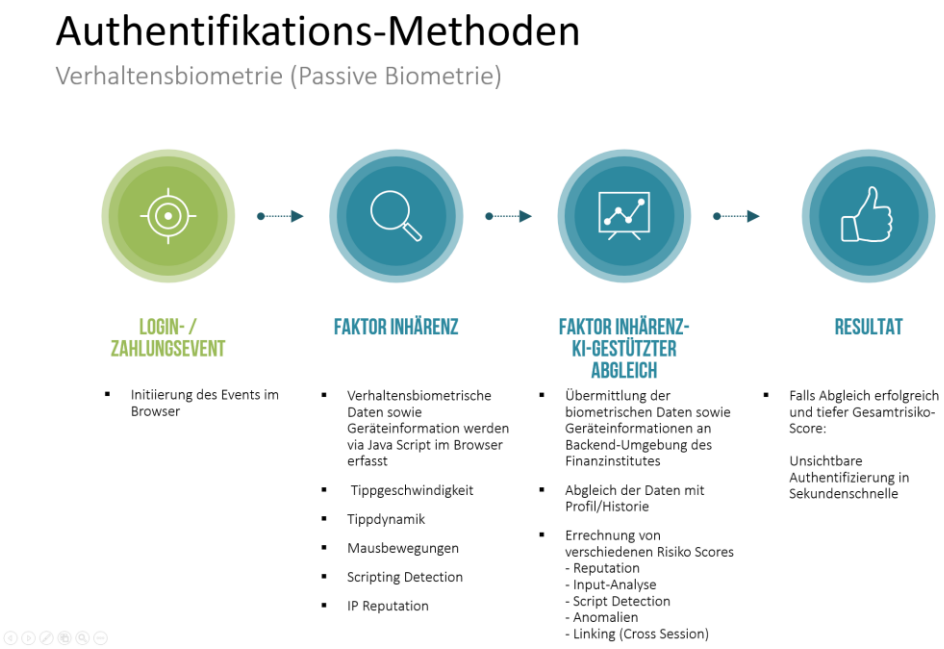
Secure Hardware

Abbildung 29: Fokusgruppe – Secure Hardware Token

Quelle: Eigene Darstellung

Passive Biometrie

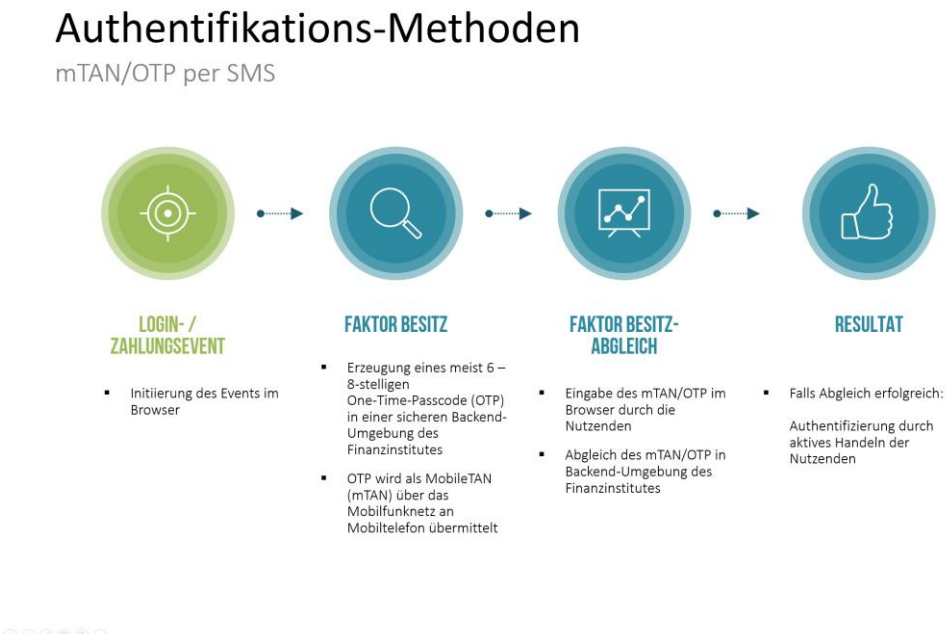
Abbildung 30: Fokusgruppe – Passive Biometrie



Quelle: Eigene Darstellung

SMS/OTP

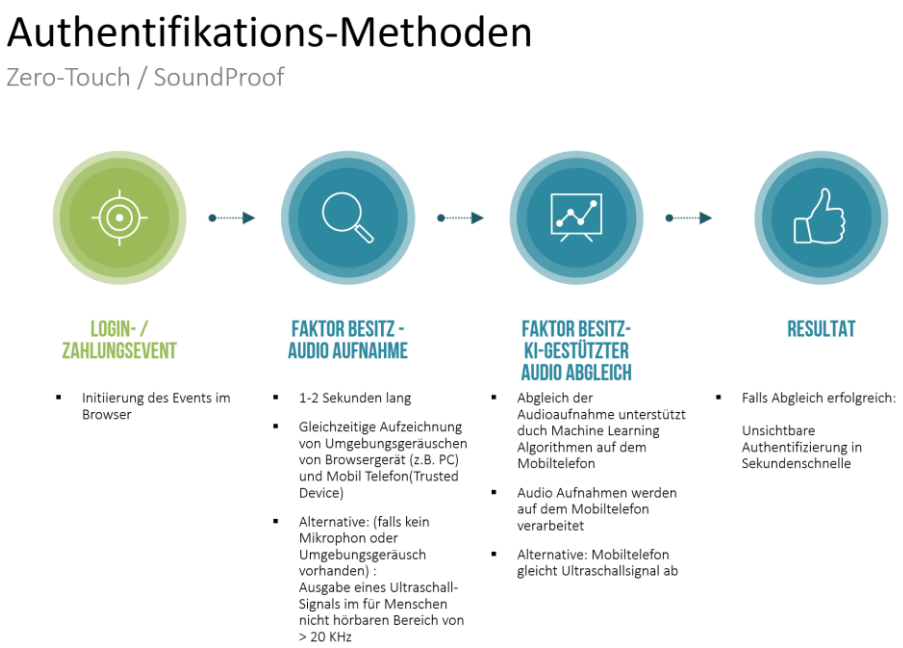
Abbildung 31: Fokusgruppe - SMS/OTP



Quelle: Eigene Darstellung

ZeroTouch/ Soundproof

Abbildung 32: Fokusgruppe - ZeroTouch / Soundproof



Quelle: Eigene Darstellung

Um bei der Bewertung die soziale Erwünschtheit (es gibt keine richtigen oder falschen Antworten) und allfällige Restriktionen des Arbeitgebers der jeweiligen Probandin oder des jeweiligen Probanden abzuschwächen und gleichzeitig die Validität der Antworten zu erhöhen, dient ein aus der Psychologie bekanntes sogenanntes projektives Verfahren. Bei diesem Verfahren werden die Fragen so gestellt, dass eine Probandin oder ein Proband nicht für sich selbst, sondern in der Rolle einer Drittperson antwortet – obwohl die Antworten natürlich von Einstellungen und Hintergrund des Befragten stark abhängen. Die Forscherin oder der Forscher erfährt also etwas über die Befragten, indem sie oder er indirekt fragt. Dies geschieht mittels des fiktiven Szenarios „BetterCard“:

- Die Proband/innen sollen sich vorstellen, sie würden vom fiktiven FinTech-Unternehmen „BetterCard“ abgeworben und dann so antworten, als ob sie dort arbeiten.
- Ihre Aufgabe bei BetterCard ist, sich damit zu beschäftigen, wie das bargeldlose Zahlen im Kontext der starken Kundenauthentifizierung verbessert werden kann.
- Der neue Arbeitgeber hat schon Berater/innen angeheuert, welche die fünf beschriebenen Authentifizierungsmethoden, welche im Zentrum dieser Forschung stehen, ausgearbeitet haben.
- Die Proband/innen bewerten je für sich alleine die zwölf Dimensionen der Methoden, welche als semantisches Differential mit 12 Gegensatzpaaren realisiert sind.
- Ist es den Proband/innen nicht möglich, aufgrund der vorliegenden Informationen eine Bewertung abzugeben, können sie dies in einer dafür vorgesehenen separaten Spalte direkt im Bewertungsbogen eintragen.

Abbildung 33: Fokusgruppe – Bewertungsbogen Authentifizierungsmethoden

Bewertungsbogen Fokusgruppe "Authentifikation"

Bitte schreiben Sie die Nummer der vorgestellten Variante in eines der fünf Kästchen – abhängig davon, wie nahe die vorgestellte Variante an der Formulierung ist. Nummerierung der Varianten:

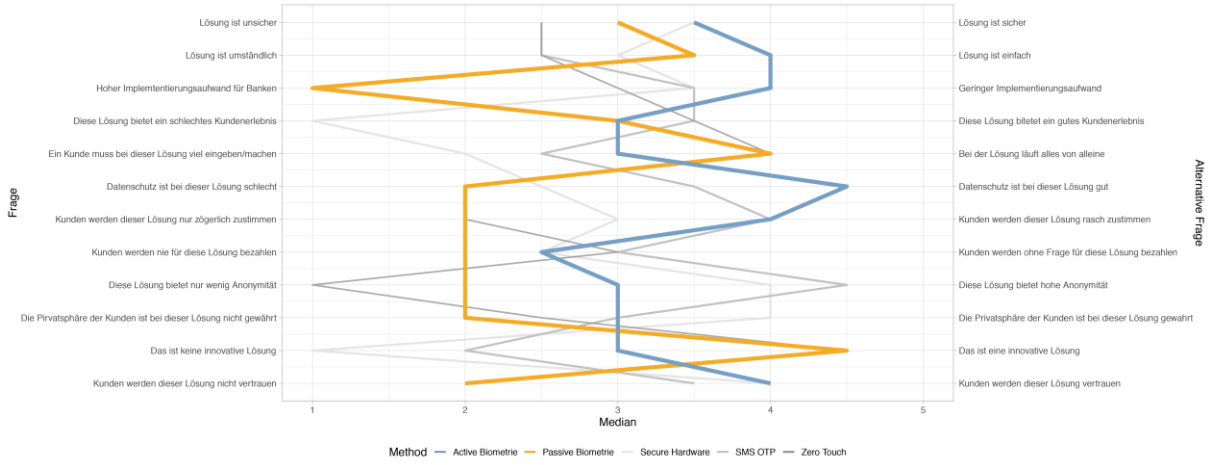
1) Physische Biometrie (aktive Biometrie)
2) Secure Hardware
3 Verhaltensbiometrie (passive Biometrie)
4) mTAN/OTP per SMS
5 Zero-Touch / SoundProof

								für diese Variante/n kann ich das nicht beurteilen (Nummer):
D1	Lösung ist unsicher						Lösung ist sicher	
D2	Lösung ist umständlich						Lösung ist einfach	
D3	Hoher Implementierungsaufwand für Banken						Geringer Implementierungsaufwand für Banken	
D4	Diese Lösung bietet ein schlechtes Kundenerlebnis						Diese Lösung bietet ein gutes Kundenerlebnis	
D5	Ein Kunde muss bei dieser Lösung viel eingeben/machen						Bei dieser Lösung läuft alles von alleine	
D6	Datenschutz ist bei dieser Lösung schlecht						Datenschutz ist bei dieser Lösung gut	
D7	Kunden werden dieser Lösung nur zögerlich zustimmen						Kunden werden dieser Lösung rasch zustimmen	
D8	Kunden werden nie für diese Lösung bezahlen						Kunden werden ohne Frage für diese Lösung bezahlen	
D9	Diese Lösung bietet Kunden nur wenig Anonymität						Diese Lösung bietet Kunden hohe Anonymität	
D10	Die Privatsphäre der Kunden ist bei dieser Lösung nicht gewahrt						Die Privatsphäre der Kunden ist bei dieser Lösung gewahrt	
D11	Das ist keine innovative Lösung						Das ist eine innovative Lösung	
D12	Kunden werden dieser Lösung nicht vertrauen						Kunden werden dieser Lösung vertrauen	

Quelle: Eigene Darstellung

Die Assoziationsmessung erfolgt mittels eines semantischen Differentials. Das semantische Differential wurde im Jahr 1952 vom US-amerikanischen Psychologen Charles E. Osgood zur Analyse von affektiven Wortbedeutungen entwickelt. Ermittelt wurde das semantische Differential anhand von mehrstufigen, bipolaren Ratingskalen, welche an den Skalenenden Gegensatzpaare enthalten, auf denen die Befragten eine vorgegebene Methode einzustufen haben. Zur Auswertung des semantischen Differentials dient der grafische Vergleich von unterschiedlichen Methoden bei identischen Befragungsgruppen (Wirtschaftslexikon24, 2017). (Der Median liefert insbesondere bei schiefen Verteilungen eine realistischere Einschätzung bezüglich der Verteilung als der Mittelwert.

Abbildung 34: Fokusgruppe – Auswertung Polaritätsprofil mit Median aller fünf Methoden



Quelle: Eigene Abbildung in R Studio

Da die Stichprobengrösse mit 8 Personen klein ist, erfolgt die statistische Auswertung des semantischen Differentials anhand des von dem US-amerikanischen Chemiker und Statistiker Frank Wilcoxon entwickelten Wilcoxon-Vorzeichen-Rangtests. Der Test vergleicht, ob die zentralen Tendenzen (Mediane) zweier abhängiger Stichproben signifikant verschieden sind. Der Wilcoxon-Vorzeichen-Rangtest ist ein nichtparametrischer Test, bei dem die Messwertpaare nicht, wie beim Student t-Test für abhängige Stichproben, normalverteilt sein müssen und besitzt, verglichen mit dem t-Test, eine Effizienz von 95% (Zöfel, 2003, S. 144). „Von abhängigen Stichproben wird gesprochen, wenn ein Messwert in einer Stichprobe und ein bestimmter Messwert in einer anderen Stichprobe sich gegenseitig beeinflussen“ (Universität Zürich, 2018).

- Die Nullhypothese (H0) lautet: Die Differenz zwischen den zentralen Tendenzen von jeweils zwei ausgewählten Authentifizierungsmethoden ist gleich 0.
- Die Alternativhypothese (H1) lautet: Die Differenz zwischen den zentralen Tendenzen von jeweils zwei ausgewählten Authentifizierungsmethoden ist nicht gleich 0.

Ob die Nullhypothese beibehalten oder verworfen werden kann, wurde berechnet. Im ersten Schritt wurde jeder Skalenstufe des semantischen Differentials ein Score von eins bis fünf zugeordnet und die Antworten der Proband/innen wurden entsprechend kodiert. Das Skalenende links mit negativen Aussagen erhält den Wert eins, das Skalenende rechts mit positiven Aussagen erhält den Wert fünf. Anschliessend wird für die graphische Auswertung pro Proband/in das arithmetische Mittel des Scores des entsprechenden Authentifizierungsverfahrens berechnet.

Abbildung 35: Fokusgruppe – Beispiel Aktive Biometrie – Scoresheet pro Proband/in und Dimension

	Wort 1	Wort 2	Person A	Person B	Person C	Person D	Person E	Person F	Person G	Person H	Durchschnitt pro Dimension
D1	Lösung ist unsicher	Lösung ist sicher	1	3	5	3	5	4	3	5	3.6
D2	Lösung ist umständlich	Lösung ist einfach	5	2	4	3	3	4	4	4	3.6
D3	Hoher Implemtentierungsaufwand für Banken	Geringer Implementierungsaufwand	5	2	3	5	2	4	4	4	3.6
D4	Diese Lösung bietet ein schlechtes Kundenerlebnis	Diese Lösung bitetet ein gutes Kundenerlebnis	5	4	3	3	3	3	1	5	3.4
D5	Ein Kunde muss bei dieser Lösung viel eingeben/machen	Bei der Lösung läuft alles von alleine	5	1	2	5	3	3	3	3	3.1
D6	Datenschutz ist bei dieser Lösung schlecht	Datenschutz ist bei dieser Lösung gut	5	4	3	5	1	4	5	5	4.0
D7	Kunden werden dieser Lösung nur zögerlich zustimmen	Kunden werden dieser Lösung rasch zustimmen	5	3	4	5	2	5	3	4	3.9
D8	Kunden werden nie für diese Lösung bezahlen	Kunden werden ohne Frage für diese Lösung bezahlen	2	3	4	5	2	1	2	5	3.0
D9	Diese Lösung bietet nur wenig Anonymität	Diese Lösung bietet hohe Anonymität	3	3	3	3	3	3	2	5	3.1
D10	Die Pirvatsphäre der Kunden ist bei dieser Lösung nicht gew	Die Privatsphäre der Kunden ist bei dieser Lösung gewa	4	3	4	3	2	3	2	5	3.3
D11	Das ist keine innovative Lösung	Das ist eine innovative Lösung	2	3	3	2	3	3	3	3	2.8
D12	Kunden werden dieser Lösung nicht vertrauen	Kunden werden dieser Lösung vertrauen	4	1	4	5	3	5	3	5	3.8
		Durchschnitt pro Proband und Methode	3.8	2.7	3.5	3.9	2.7	3.5	2.9	4.4	3.4

Quelle: Excel, eigene Berechnung

Nun werden mit dem Wilcoxon-Test Paarvergleiche zwischen den fünf Methoden angestellt. Bei k Methoden, welche paarweise verglichen werden, ergibt dies $k * \left(\frac{(k-1)}{2}\right)$ mit $5 * (\frac{(5-1)}{2}) = 10$ Paarvergleiche.

- Aktive Biometrie verglichen mit Secure Hardware

- Aktive Biometrie verglichen mit Passiver Biometrie
- Aktive Biometrie verglichen mit Mobile TAN (mTAN) /OPT per SMS
- Aktive Biometrie verglichen mit ZeroTouch/Soundproof
- Secure Hardware verglichen mit Passiver Biometrie
- Secure Hardware verglichen mit mTAN/OTP per SMS
- Secure Hardware verglichen mit ZeroTouch/Soundproof
- Passive Biometrie verglichen mit mTAN/OTP per SMS
- Passive Biometrie verglichen mit ZeroTouch/Soundproof
- mTAN/OTP per SMS verglichen mit ZeroTouch/Soundproof

Im ersten Schritt werden die Differenzen zwischen den verglichenen Methoden ausgehend vom kleinsten Wert aufsteigend sortiert und nummeriert. Die Nummer entspricht dabei dem Rang einer Differenz. Beträgt die Differenz eines Wertepaares Null, so wird dieser Wert vom Vorzeichentest ausgeschlossen, da der Wert Null kein positives oder negatives Vorzeichen hat. Kommt beispielsweise wie beim Paarvergleich „Aktive Biometrie vs. Passive Biometrie" der kleinste Wert zweimal vor, wird ein Mittelwert der Ränge gebildet $\left(\frac{(1+2)}{2}\right) = 1.5$ und bei den Messwerten zugewiesen. Anschliessend wird die Summe der positiven Abweichungen und die Summe der negativen Abweichungen berechnet.

Abbildung 36: Fokusgruppe – Wilcoxon-Test mit „Aktiver Biometrie" und „Passiver Biometrie"

	Daten					Testwerte		
Person #	Aktive Biometrie	Passive Biometrie	Differenz	Vorzeichen	Rang	Positive Ränge	Negative Ränge
A	3.8	2.3	1.5	-	7		7
B	2.7	2.0	0.7	-	3		3
C	3.5	2.2	1.3	-	6		6
D	3.9	3.5	0.4	-	1.5		1.5
E	2.7	2.7	0.0			0	
F	3.5	3.1	0.4	-	1.5		1.5
G	2.9	1.8	1.1	-	4.5		4.5
H	4.4	3.3	1.1	-	4.5		4.5
AVG	3.4	2.6			Rangsummen	0	28
					Anzahl Paardifferenzen mit Wert grösser Null = n	7	
					W	0	
					Kritischer Wert für W	2	

Quelle: Excel, eigene Berechnung

Zwischen den Rangsummen besteht folgender Zusammenhang:

$$T_+ + T_- = \frac{n(n+1)}{2}$$

mit

T_+ = Summe der positiven Ränge
T_- = Summe der negativen Ränge
n = Anzahl der von Null verschiedenen Paardifferenzen
Ist beispielsweise bei 7 Paardifferenzen > 0 die Summe der positiven Ränge = 0 und die Summe der negativen Ränge = 28, so gilt mit $T_+ = 0$ sowie $T_- = 28$ folgende Gleichung:

$$0 + 28 = \left(\frac{7 * (7+1)}{2}\right)$$

Für die Teststatistik W wird nun die kleinere der beiden Zahlen verwendet mit $W = 0$ da 0 < 28.

Da die Anzahl der Proband/innen mit 8 kleiner als 25 ist, kann der kritische Wert, der unterschritten werden muss, um die Nullhypothese zu verwerfen, aus einer Tabelle mit kritischen Werten abgelesen werden.

Tabelle 5: Kritische Werte für den Wilcoxon-Test

Signifikanzniveau (Alpha)		n				
zweiseitig	einseitig	4	5	6	7	8
0,1000	0,0500		0	2	3	5
0,0500	0,0250			0	2	3
0,0200	0,0100				0	1
0,0100	0,0050					0
0,0050	0,0025					
0,0010	0,0005					

Quelle: Excel, eigene Darstellung in Anlehnung an Real-Statistics

Bei einem zweiseitigen Test (ungerichtete Hypothese) und einem Konfidenzniveau von 95% ist der kritische Wert, welcher unterschritten werden muss, 2. Da der Wert W aus der Teststatistik mit 0 kleiner ist als der kritische Wert 2, unterscheiden sich die Versionen „Aktive Biometrie“ und „Passive Biometrie“ signifikant voneinander.

Der statistische Test kann alternativ auch in Statistikprogrammen wie beispielsweise SPSS von IBM durchgeführt werden.

Abbildung 37: Fokusgruppe – SPSS Statistik für Wilcoxon-Vorzeichen-Rangtest

Zusammenfassung des Wilcoxon-Tests bei verbundenen Stichproben

Gesamtzahl	8
Teststatistik	28.000
Standardfehler	5.895
Standardisierte Teststatistik	2.375
Asymptotische Sig. (zweiseitiger Test)	.018

Quelle: SPSS, eigene Berechnung

Bei einem Signifikanzniveau α auch von 0.05 und einem Konfidenzintervall von 95% ergibt die standardisierte Teststatistik einen Z-Wert von 2.375 und eine asymptotische Signifikanz von 0.18. Die Asymptote ist eine Gerade, die sich einer ins Unendliche verlaufende Kurve nähert, ohne sie zu erreichen (Bedeutung von Wörtern, 2019). Der Z-Wert des auf der Standardnormalverteilung basierenden kritischen Wertes für das Signifikanzniveau α mit 0.05 ist = 1.96. Der Vergleich der Z-Werte zeigt, dass die Teststatistik mit 2.375 grösser ist als der Z-Wert des kritischen Wertes mit

1.96. Die asymptotische Signifikanz ist mit 0.018 kleiner als das Fehlerniveau α mit 0.05. Dies bedeutet, dass die Nullhypothese verworfen werden kann.

Um die Bedeutsamkeit der Ergebnisse zu beurteilen, wird die Effektstärke (Stärke des Zusammenhangs) mittels Korrelationskoeffizient (r) von Pearson berechnet.

$$r = \left|\frac{z}{\sqrt{n}}\right|$$

$$r = \frac{2.375}{\sqrt{8}} = 0.84$$

Nach der Einstufung von Effektstärken nach Cohen hat ein Wert r von 0.84 eine hohe Korrelation bei 0.7 > r <= 0.9.

Mittels des Wilcoxon-Vorzeichen-Rangtests konnten nur bei dem Paarvergleich von Aktiver Biometrie mit Passiver Biometrie ein signifikanter Unterschied bezüglich der zentralen Tendenzen festgestellt und damit die Nullhypothese verworfen werden. Die Proband/innen haben insgesamt die Methode der Aktive Biometrie besser bewertet. Ein Blick auf die grafische Darstellung der einzelnen Bewertungen der Proband/innen zeigt: Die Varianz unter den 8 Proband/innen war vermutlich so gross, dass bei den 9 anderen Tests kein Unterschied entstanden ist.

5 SCHLUSSFOLGERUNGEN UND EMPFEHLUNGEN

Im Folgenden werden die beiden eingangs formulierten Forschungsfragen nochmals zusammengefasst beantwortet sowie Empfehlungen für die Praxis abgegeben.

- Wie könnte ein möglicher innovativer und PSD2-konformer Authentifizierungsservice aussehen, welcher es den Banken ermöglicht, ihre Kund/innen beim Zugriff auf Kartenzahlungskonten sowie bei der Auslösung von kartenbasierten Zahlungen auf eine bequeme und sichere Art zu authentifizieren?
- Welche Verfahren sind geeignet, um während der Authentifizierung ein möglichst gutes Kundenerlebnis zu schaffen bei einem möglichst hohen Sicherheitsniveau?

Da der risikobasierte und adaptive Authentifizierungsservice auf der Kombination der verhaltensbiometrischen Analyse sowie dem Abgleich von Umgebungsgeräuschen beruht, ist für den Forscher lediglich die Bewertung der beiden Methoden sowie der Paarvergleich, bei welchem die Null-Hypothese verworfen werden konnte, von Relevanz.

Abbildung 38: Ampelsystem - Polaritätsprofile

Dimension	Aktiv Biometrie	Secure Hardware	Passive Biometrie	SMS/ OTP	Zero-Touch / Soundproof
D1 - Sicherheit	3.63	3.00	2.86	3.13	2.63
D6 - Datenschutz	4.00	2.88	2.14	3.63	2.50
D9 - Anonymität	3.13	4.13	2.00	4.13	1.86
D10 - Privatsphäre	3.25	4.00	2.00	3.14	2.75
D12 Vertrauen	3.75	3.63	1.88	3.50	1.86
D7 - Kundinnen- / Kundenakzeptanz	3.88	2.88	2.00	4.00	2.00
D2 - Einfachheit	3.63	2.88	3.33	2.75	2.38
D5 - Bequemlichkeit	3.13	2.00	4.00	2.63	3.38
D4 - Kundinnen- / Kundenerlebnis	3.38	1.63	3.43	3.25	3.00
D11 - Innovation	2.75	1.75	4.50	2.00	4.50
D3 - Implementierungsaufwand	3.63	3.25	1.75	3.50	2.88
D8 - Monetarisierung	3.00	2.75	2.43	3.25	3.29

Quelle: Excel, eigene Darstellung

Die Auswertung der Fokusgruppe zeigt auf, dass bei den Proband/innen Einigkeit darüber herrscht, dass in ihrer Wahrnehmung die Authentifizierungsmethode „Aktive Biometrie“ die beste Methode ist. Zudem liefert lediglich der Paarvergleich „Aktive Biometrie“ mit „Passiver Biometrie“ signifikante Unterschiede bezüglich der zentralen Tendenzen. Bei allen anderen Paarvergleichen herrscht Uneinigkeit bezüglich der Bewertung der Dimensionen, was sich statistisch anhand der Varianz zeigt.

Bei der „Aktiven Biometrie“ mittels Fingerabdruckerkennung liegt der Median, mit Ausnahme von der Dimension „Monetarisierung“ (Sind die Kunden bereit, für diese Lösung zu bezahlen?), auf oder über dem arithmetischen Mittelwert von 3. Es fällt auf, dass der Median bei der Dimension

„Datenschutz“ mit 4.5 die insgesamt höchste Bewertung aller Dimensionen erhält. Zudem wurde die „Sicherheit“ mit 3.5 ebenfalls über dem statistischen Mittel bewertet. Dies ist bemerkenswert, da 2013, als Apple die Fingerabdruckerkennung (TouchID) auf einem Smartphone (iPhone 5S) lancierte, grosse Bedenken hinsichtlich des Datenschutzes bestanden. So wurden damals Stimmen laut, dass Apple mit der NSA kooperiere und diese mit Sicherheit Zugang zu den biometrischen Daten habe. Apple hat stets beteuert, dass der Fingerabdruck verschlüsselt in einem geschützten Bereich der sogenannten „Secure Enclave“ lokal auf dem Smartphone und nicht beispielsweise in einer „Cloud“ gespeichert werden (Applepiloten, 2019).

Bei grossen Data Breaches werden ausserdem immer wieder auch biometrische Daten wie Fingerabdruckdaten gestohlen. Diese werden in einschlägigen Foren im Internet und Darknet angeboten und erlauben es Kriminellen, Duplikate zu erzeugen. In der Praxis sind Angriffe mittels eines Fingerabdrucks kaum bekannt, da der Angriffsvektor nicht skalierbar ist. Das heisst, es muss beispielsweise für jeden Fingerabdruck relativ aufwändig ein Duplikat erstellt werden. Die Fokusgruppe zeigt nun auf, dass die anfänglich vorherrschende Skepsis gegenüber der Aktivierung eines biometrischen Erkennungsverfahrens auf dem Smartphone verschwunden ist. Dies lässt sich auch anhand der Bewertung 4.0 bei der Dimension „Vertrauen“ belegen.

Bei der Methode „Passive Biometrie“ wurde die Dimension „Innovation“ gleich wie bei der Methode „ZeroTouch/Soundproof“ mit 4.5 bewertet, was der höchsten Bewertung dieser Dimension bei allen Methoden entspricht. Die Dimension „Bequemlichkeit“ (Muss die Kundin oder der Kunde viele Daten eingeben oder nicht?) erhielt mit 4.0 ebenfalls eine hohe Bewertung. Die Proband/innen sind sich aber ziemlich einig, dass die Kund/innen dieser Lösung, falls überhaupt, nur zögerlich zustimmen werden, da sie die Dimensionen Datenschutz, Anonymität und Schutz der Privatsphäre jeweils mit 2.0 bewerteten.

Bei der Methode „Soundproof/ZeroTouch fällt auf, dass die Dimension Anonymität von allen Proband/innen mit 1.0 bewertet wurden. Zudem beurteilten sie den Datenschutz mit 2.0 sowie die Sicherheit mit 2.5 jeweils unterdurchschnittlich, hingegen die „Innovationskraft“, wie bereits erwähnt, mit 4.5 überdurchschnittlich hoch und die Dimension „Bequemlichkeit“ mit 4.0 ebenfalls.

Insgesamt lässt sich sagen, dass die Proband/innen, die für den Authentifizierungsservice verwendeten Methoden zwar innovativ und bequem finden (gute User Experience), jedoch Bedenken bezüglich Sicherheit, Datenschutz, Wahrung der Anonymität und des Schutzes der Privatsphäre haben. Hinsichtlich eines Marktlaunches des Services ist es wichtig, nicht das Produkt an sich zu ändern, sondern genau auf diese Ängste zu kommunizieren. Somit werden mit der Zeit die Bedenken vermutlich ähnlich wie bei der Aktiven Biometrie verschwinden. Zudem ist zu erwähnen, dass anhand von verhaltensbiometrischen Daten keine Rückschlüsse auf eine natürliche Person gezogen werden können, sondern lediglich eine Verifikation anhand des Datenabgleiches zwischen den neuen Authentisierungsdaten (z.B. Tastaturanschlagsdynamik) mit den gespeicherten Templatedaten vorgenommen wird, um so eine erfolgreiche Authentifizierung zu erwirken. „ZeroTouch/Soundproof“-Daten werden wie Fingerabdruckdaten nur auf dem Mobiltelefon gespeichert, allerdings nicht als Audiodaten und sind somit im Falle eines potentiellen Datendiebstahles

unbrauchbar, da sich die Umgebungsgeräusche nicht wiederherstellen und abhören lassen. Es wäre empfehlenswert, den Proband/innen in einer nächsten Ausbaustufe des Services die Funktionen von „Passiver Biometrie“ sowie „ZeroToch/Soundproof“ mittels eines Proof-of-Concepts zu zeigen, da das echte „Erleben“ des Services unter Umständen anders wahrgenommen wird. Es können andere Eindrücke vermittelt werden, als dies mit einer Beschreibung und Visualisierung möglich ist. Abzuklären wäre auch, wie die Methode „Aktive Biometrie“ bewertet wird, falls anstelle der Fingerabdruckerkennung die Gesichtserkennung (FaceID) eingesetzt wird. Dies ist bei Apple seit der Iphone Version X Standard, die Fingerabdrucksensoren wurden entsprechend entfernt und sind auch bei der allerneuesten Generation 11 nicht mehr vorhanden.

Auf der technischen Seite ist das EMVCo-3D-Secure-Protokoll 2.2 noch nicht in der Lage, Detailinformationen zu einem biometrischen Authentifizierungsverfahren, welches auf der Händlerseite vorgenommen wurde, an die Kartenherausgeberin zu übermitteln. Der Autor und Forscher der vorliegenden Arbeit ist im Kontakt mit zwei grossen Zahlungsnetzwerken, mit dem Ziel, dass in künftigen Versionen des Protokolls beispielsweise Daten, die durch Passive Biometrie ermittelt werden, an die Kartenherausgeberin übermittelt werden können, um den Authentifizierungsservice noch sicherer und bequemer zu machen. Zudem prüft der Forscher derzeit mit den Zahlungsnetzwerken, ob und wie es künftig technisch möglich wäre, lediglich einen Faktor (z.B. den Inhärenzfaktor) an den Händler zu delegieren, den zweiten jedoch nicht. Hier stellt sich die Frage, welche Konsequenzen dies für die Haftungsbestimmungen hätte, wenn dies technisch realisierbar wäre. Abschliessend lässt sich sagen, dass die beiden Methoden des Authentifizierungsservices ein grosses Marktpotential haben. Noch ist es aber zu früh für einen Marktlaunch eines risikobasierten und adaptiven Authentifizierungsservices basierend auf Passiver Biometrie und ZeroTouch/Soundproof. Die Empfehlung lautet jedoch, die Konzeption und Spezifikation des Services weiterzuführen und zu verbessern, um den richtigen Zeitpunkt für die Entwicklung und Lancierung nicht zu verpassen.

6 ANHANG

6.1 QUELLENVERZEICHNIS

Apple. (2019). About Face ID Advanced Technology. Abgerufen am 18. September 2019, von https://support.apple.com/en-ca/HT208108

Applepiloten. (2019). Apple bestreitet Kooperation mit NSA. Abgerufen am 17. September 2019, von https://applepiloten.de/apple-bestreitet-kooperation-mit-nsa/

Bedeutung von Wörtern. (2019). Asymptotisch. Abgerufen am 23. September 2019, von https://www.bedeutung-von-woertern.com/asymptotisch

Brands Consulting. (2011). Unterschiede zwischen Datenschutz und Datensicherheit. Abgerufen am 11. August 2019, von https://brands-consulting.eu/unterschiede-zwischen-datenschutz-und-datensicherheit-wieso-datensicherheit-nicht-immer-zum-datenschutz-beitraegt

Core. (2018). EBA-Kommentar zur PSD3-RTS – Auflösen von Unklarheiten wirft neue Fragen auf. Abgerufen am 17. September 2019, von https://core.se/de/techmonitor/eba-kommentar-zur-psd2-rts-aufloesen-von-unklarheiten-wirft-neue-fragen-auf

Verizon. (2019) Data Breach Investigations Report (DBIR)

Datenschutzbeauftragter. (2019). Authentisierung, Authentifizierung und Autorisierung. Abgerufen am 18. September 2019, von https://www.datenschutzbeauftragter-info.de/authentisierung-authentifizierung-und-autorisierung/

Deacademic (2019). Regenbogentabelle. Abgerufen am 17. September 2019, von https://deacademic.com/dic.nsf/dewiki/1166977

Duden. (2019). Rechtschreibung. Abgerufen am 19. September 2019, von https://www.duden.de/rechtschreibung/Identitaet

Eckert, C., (2018) IT-Sicherheit. Berlin: Walter de Gruyter Verlag

Gründerszene. (2019). Interoperabilität. Abgerufen am 25. September 2019, von https://www.gruenderszene.de/lexikon/begriffe/interoperabilitaet

Handelsblatt. (2019). Erneute Datenpanne bei Facebook – Firmen speicherten ungeschützt Daten von Millionen Nutzern. Abgerufen am 18. September 2019, von https://www.handelsblatt.com/technik/it-internet/neue-sicherheitspanne-erneute-datenpanne-bei-facebook-firmen-speicherten-ungeschuetzt-daten-von-millionen-nutzern/24179574.html?ticket=ST-47918739-iIsPvVyInbhdPkBF4aqu-ap4

IBM Developer. (2019). IBM Developer. Abgerufen am 18. September 2019, von https://developer.ibm.com/mainframe/wp-ontent/uploads/sites/46/2018/04/PSD2-Overview.png

Ingenico. (2019). Starke Kunden-Authentifizierung im Rahmen der Umsetzung der PSD2, abgerufen am 29. September 2019, von https://cdn.ingenico.com/binaries/content/assets/germany-payment-services/news/faq-kunden-authentifizierung-psd2_2019-07-19.pdf

IT Talents. (2019). Was ist Cross-Site-Scripting. Abgerufen am 1. Juni 2019, von https://www.it-talents.de/blog/it-talents/was-ist-cross-site-scripting-xss

Kompass-Nachhaltigkeit. (2013). Willkommen bei Kompass Nachhaltigkeit. Abgerufen am 23. Januar, von https://www.kompass-nachhaltigkeit.ch

Lamnek, S. (2010), Qualitative Sozialforschung, Psychologie Verlagsunion

Opera. (2019). Opera. Abgerufen am 10. August 2019, von https://www.opera.com/de/features/free-vpn

Privatim, Leitfaden Biometrie, 2006

Real Statistics. (2019). Wilcoxon-Signed-Rank-Table, abgerufen am 24. Oktober 2019 auf http://www.real-statistics.com/statistics-tables/wilcoxon-signed-ranks-table/

Research Gate. (2019). A Novel Approach to Probabilistic Biomarker-Based Classification Using Functional Near-Infrared Spectroscopy. Abgerufen am 20. August 2019 von https://www.researchgate.net/figure/Confusion-matrix-summarizing-the-errors-made-by-the-classifier-on-the-test-set_fig1_230830197

Safenet. (2019). Out-of-Band-Authentifizierung. Abgerufen am 29. September 2019, von https://safenet.gemalto.de/multi-factor-authentication/authenticators/out-of-band-authentication/

Schweizerische Eidgenossenschaft. (2017). Botschaft zum Bundesgesetz über die Totalrevision des Bundesgesetzes über den Datenschutz und die Änderung weiterer Erlasse zum Datenschutz vom 15. September 2017. Abgerufen am 18. September 2019, von https://www.admin.ch/opc/de/federal-gazette/2017/6941.pdf

Snowflake. (2019). Beratung zur DSGVO. Abgerufen am 11. August 2019, von https://www.snowflake.ch/dsgvo/

Stakeoverlow. (2019). How to Implement a Reduced Rainbow Table in Python. Abgerufen am 18. September 2019, von https://stackoverflow.com/questions/57101012/how-to-implement-a-reduced-rainbow-table-in-python

Stengel, C. & Weber, T. (2016). Digitale und mobile Zahlungssysteme. Zürich: Schulthess Verlag.

SwissID. (2019). SwissID. Abgerufen am 18. September 2019, von https://www.swissid.ch

Wirtschaftslexikon24. (2017). Semantisches Differential. Abgerufen am 22. September 2019, von http://www.wirtschaftslexikon24.com/d/semantisches-differential/semantisches-differential.htm

Universität Zürich. (2018). Methodenberatung. Abgerufen am 23. September 2019, von https://www.methodenberatung.uzh.ch/de/datenanalyse_spss/unterschiede/zentral/wilkoxon.html

Zöfel, P. (2003). Statistik für Wirtschaftswissenschaftler im Klartext. Pearson Studium

6.2 ABKÜRZUNGSVERZEICHNIS

Abkürzung	Bedeutung
2FA	2-Faktor-Authentifizierung
3RI	3DS Requestor Initiated
AAL	Authenticator Assurance Level
ACS	Acces Control Server
AIS	Account Information Service
AISP	Account Information Service Provider
API	Aplication Programming Interface
AREQ	Authentication Request
ARES	Authentication Response
ASPSP	Account Servicing Payment Service Provider
CA	Competent Authorities
CNP	Card Not Present
COF	Credential-on-File
CREQ	Challenge Request
CRES	Challenge Response
CSC	Common and Secure Communication
CSP	Credential Service Provider
CVC2	Card Validation Code 2
CVV2	Card Card Verification Value
DBIR	Data Breach Investigation Report
DIN	Deutsches Institut für Normung
DS	Directory Server
DSG	Bundesgesetz über den Datenschutz
DSGVO	Datenschutz-Grundverordnung
EBA	European Banking Authority
E-ID	Elektronische Identität
EJPD	Eidgenössisches Justiz- und Polizeidepartement
EMV	Eurocard, Mastercard, Visa
ERR	Equal Error Rate
ETV	Exemption Threshold Value
EU	Europäische Union
EWR	Europäischer Wirtschaftsraum
EZB	Europäische Zentralbank
FAR	False Acceptance Rate
FCS	Fund Confirmation Service
FER	False Enrolment Rate
FER	Failure to enroll
FRR	False Rejection Rate
GDPR	General Data Protection Regulation
GPS	Global Positioning
HTML	Hypertext Markup Language

HTTPS	Hypertext Transfer Protocol Secure
IAL	Identity Assurance Level
ICC	International Chamber of Commerce – ICC)
ID	Identität
IOCTA	Internet Organised Crime Threat Assessment
IoT	Internet of Things
IP	Internet-Protokoll
ISO	International Standardisation Organisation
ISP	Internet Service Provider
JSON	Java Script Object Notation
KI	Künstliche Intelligenz
LOA	Level of Assurance
M2M	Machine-to-Machine
MD5	Message-Digest Algorithm 5
MFA	Multi-Faktor-Authentifizierung
MITB	Man-in-the-Browser
MTAN	Mobile TAN
NFC	Nierfield Communication
NIST	National Institute of Standards and
OCT	Original Credit Transfer
OLO	One-Leg-Out
OTP	One-Time-Password
PIN	Personal Identification Number
PIS	Payment Initiation Service
PISP	Payment Initiation Service Provider
POS	Point of Sale
PREQ	Preparation Request
PRES	Preparation Response
PSP	Payment Service Provider
PSU	Payment Service User
QoR	Quality of Registration
QR	Quick Respone Code
QR Code	Quick Respone Code
REST	Representational State Transfer
RFID	Radio-Frequenz-Identifikation
RP	Relying Party
RREQ	Results Request
RRES	Results Response
RTS	Regulatory Technical Standards
SCA	Strong Customer Authentication
SDD	Sepa Direct Debit
SDK	Software Development Kit
SEPA	Single Euro Payments Area
SIM	Subscriber Identity Module

SMS	Short Message System
TLS	Transport Layer Security
TOM	Technische und organisatorische Massnahmen
TPP	Third-Party-Provider
TRA	Transaction Risk Analysis
UCoF	Unscheduled Credential-on-File-Payment
UI	User Interface
URL	Uniform Ressource Locator
XML	Extensible Markup Language
XS2A	Access to Account
XSS	Cross Site Scripting

6.3 Tabellen- und Abbildungsverzeichnis

6.4 FOKUSGRUPPE

6.4.1 LEITFADEN

Leitfaden für Fokusgruppe

Datum/Zeit

Dienstag, 27. August 2019, 19 bis 21 Uhr

Rekrutierungskriterien

- Thema "Zahlungsverkehr & Kartengeschäft"
- Arbeiten bei Retailbanken
- Teamleitung, Abteilungsleitung oder GL
- Für Zahlungsverkehr oder im Kartengeschäft/bei Kreditkarten tätig
    - Trifft in einem dieser Bereiche mit anderen zusammen oder selbstständig Entscheidungen
- Grob oder ausführlich mit PSD2 beschäftigt ("Was sind Konsequenzen, wenn das kommt?")

Eintreffen

- **Namensetiketten**
- **Getränk anbieten / Food erklären**
- **Einverständnis und Geheimhaltung** unterzeichnen lassen
- **Einverständniserklärung für Video- und Tonaufnahme** unterzeichnen lassen: «Wie in der Einladung bereits angesprochen, würde ich die Diskussion gern auf Video aufnehmen. Das hilft uns bei der Auswertung nochmals genau hinzuhören, ob wir Sie richtig verstanden haben. Die Aufzeichnung wird für Auswertungszwecke im Projektteam verwendet. Persönliche Angaben werden vertraulich behandelt. »

  Schriftliche Einverständniserklärung unterzeichnen lassen und Video-/Tonband einschalten (bzw. im Vorfeld bei Einladung bereits abholen).

Einleitung (10 Minuten)

- Anwesende **begrüssen**: "Ich freue mich, dass Sie hier sind."

- Anwesende mit **Name und Rolle** vorstellen (z.B. Interviewführer, Protokollant, Beobachter).
    - Manuel Villiger, Moderator
    - Santosh Ritter, Forscher, Finanzdienstleister – am Schluss dann aufgelöst, für wen er arbeitet

- **Thema** einführen (Stichwort / wie in Einladung)
  Wir sprechen heute über das Thema **"Authentifikation".**

- **Danke** für Teilnahme. Betonen, dass die Diskussion der Teilnehmer sehr wertvoll sein wird. Teilnehmer wurden eingeladen, damit wir verschiedene Meinungen und Ansichten kennenlernen können.

- **Erwartungen** an den Teilnehmer nennen: Offenheit und Ehrlichkeit, Respekt vor anderen Meinungen

- Entsprechend gelten folgende **Spielregeln für Gruppendiskussion** (Poster):
  - Persönliche Daten werden vertraulich behandelt
  - Aussagen werden nur konsolidiert ausgewertet
  - Alle machen mit
  - Jede Meinung zählt
  - Es gibt keine richtigen oder falschen Antworten
  - Wir reden nicht durcheinander
  - Wir lassen den andern ausreden

- **Ablauf** der Fokusgruppe beschreiben: Grobe Inhalte von Einstieg/Hauptteil/Ausstieg.

- Dauer des Interviews erwähnen: «Die Gruppendiskussion wird maximal 2h Stunden dauern, das heisst bis 21 Uhr.»

- Gelegenheit für **Fragen zum Ablauf oder zum Hintergrund** anbieten.

Einstieg (25 Minuten)

Aufwärmen und Kennenlernen

Frage / Thema	Zeit	Material
Vorstellungsrunde / Aufwärmen (Wortmeldung) Heute geht es ja um das Thema "Authentifikation" und wir bauen das direkt in eine Vorstellungsrunde ein: Jeder nennt seinen Namen und ein Hobby / etwas was man gerne tut. Satz beenden: "Das letzte Mal musste ich mich authentifizieren lassen am [[DATUM]] für [[KAUF]]."	**5'**	Namens-etiketten Flipchart mit Satz-Vorlage

Thema einführen

Frage / Thema	Zeit	Material
A) Thema Authentifizierung: Probleme heute Jetzt haben wir Sie beim Einstieg als Kunden betrachtet, der selbst authentifiziert werden muss. Damit wir heute immer alle vom Selben sprechen, hier nochmals die Definition => *Flipchart "Authentifikation".*	**10'**	Flipchart "Authenti-fikation" auf A1 plotten => Manuel

(Santosh stellt vor) **1. Wo sehen Sie heute aus Kundensicht die grössten Probleme beim bargeldlosen Bezahlen?** Und jetzt sind Sie eingeladen, weil Sie auch bei einer Bank arbeiten, die sich ja als Bank auch damit auseinandersetzen muss. **2. Kennen Sie die grössten Probleme beim bargeldlosen Bezahlen auch aus Bankensicht?** ***Besonderes Erkenntnisinteresse:*** • *Haben alle Banken dieselben Probleme oder wie gross sind die Unterschiede?* • *Wie gross ist die Überlappung Kundensicht/Bankensicht?* **PROBLEM-LISTE BEURTEILEN** • Was sind Gemeinsamkeiten / Unterschiede zwischen Kundenproblemen und Bankenproblemen? • Was sind die grössten drei Probleme? **VOTING**		Flipcharts "Probleme Kunden-sicht" und "Probleme Banken-sicht" Klebepunkte für Voting
B) Lösungen heute: Authentifikation **3. Was machen Sie als Kundin/Kunde heute, um diesen Problemen zu begegnen?** **4. Wissen Sie, was Ihre Bank alles macht, um diesen Problemen zu begegnen?** **OLD-SCHOOL-LISTE BEURTEILEN** 1. E-Mail Adresse in Kombination mit statischem Passwort 2. Identifikation & Verifikationsfragen z.B. Ledigname der Mutter, Lieblingsfarbe, Name des ersten Haustieres 3. Smartcards mit Hardware Modulen wie SmartCard Reader 4. One-time-passcode (OTP) auf physischen Streichlisten 5. One-time-passcode per SMS (mTan) oder durch Callcenter Outbound Call • Kenne ich als Nutzer*in • Nutze ich privat • Hat meine Arbeitgeberin meines Wissens implementiert	**10'**	Flipchart "Old school liste" mit den 5 Punkten vorbereitet drauf und 3 Spalten für Antworten

Hauptteil (80 Minuten)

C.1) PSD2 eindenken Jetzt haben wir vorher von den Problemen gehört und von Massnahmen aus Kunden- und Bankensicht. Nun tritt diesen Herbst in Europa eine grössere Regulierung in Kraft: PSD2 – haben Sie davon schon gehört? => A1 Plot PSD2 “Zahlungsdiensterichtlinien” *(Santosh bereitet vor)* Kurze Diskussion: Was ändert nun konkret im Herbst in Bezug auf: ● Kundensicht? ● Bankensicht? ***Falls nichts oder Falsches zur Sprache kommt: Einbezug Santosh zur Korrektur?*** Und jetzt stellen wir uns für den Rest des Abends Folgendes vor: Wir werden alle von Fintech Bettercard abgeworben und beschäftigen uns nun damit, wie wir das bargeldlose Bezahlen für die Kunden und für uns einfacher machen können – indem wir das umsetzen, was mit der starken Kunden-Authentifizierung ausgereizt werden kann! Der neue Arbeitgeber hat schon Berater angeheuert, um Vorschläge auszuarbeiten – wir müssen die aber nun noch beurteilen. Dafür gibt es ein Scoring Sheet => Kurz erklären und jeder Person ein Sheet aushändigen. **Varianten** **1) Physische Biometrie (aktive Biometrie)** **2) Secure Hardware** **3) Verhaltensbiometrie (passive Biometrie)** **4) mTAN/OTP per SMS**	**15’**	A1 Plot PSD2 => Manuel drucken

5) Zero-Touch / SoundProof		
C.2) Scoring Variante einzeln vorstellen; nur Rückfragen beantworten, keine Diskussion; danach Scoring-Sheet ausfüllen und am Schluss abgeben (jede Person für sich). Beim Scoring Vergleiche betonen: “Blättern Sie gerne hin und her und vergleichen Sie, ob Sie die Scores korrekt gesetzt haben und korrigieren Sie, falls sich Ihre Meinung geändert hat.” ***Besonderes Erkenntnisinteresse:*** ● ***Scoring der Lösungen => Wilcoxon Test soll zeigen, was gewinnt***	**5*5 = 25’**	**5 VARIANTEN** Beamen und dann aufhängen auf A1 **Manuel alle drucken auf A1**
C.3) Diskussion Top-Varianten: Was sollen wir als Fintech nun kaufen und implementieren? **ANTWORTEN AUF POST-IT NOTIEREN UND VORSTELLEN** ***Besonderes Erkenntnisinteresse:*** ● ***Qualitative Erklärung der Scorings – WARUM findet jemand eine Lösung die beste?*** ● ***Kundensicht versus Bankensicht: Unterschiede?***	**20’**	*Grüne* Post Its direkt auf die 5 Lösungs-Flips kleben
C.4) Flop-Varianten Jetzt kennen wir Ihre Top Varianten und die Gründe. **Jetzt schauen wir uns noch kurz Ihre fünf Flops an: Was ist Ihre schlechteste Lösung? Warum?** **ANTWORTEN AUF POST-IT NOTIEREN UND VORSTELLEN** ***Besonderes Erkenntnisinteresse:*** ● ***Warum verliert eine Lösung => Darf unsere Lösung am Ende nicht haben bei Markteinführung***	**10’**	*Rote* Post Its direkt auf die 5 Lösungs-Flips kleben

D) Switch zurück in Bankenalltag Zum Schluss stellen wir uns vor: Banken wollen ja heute häufig auch mitmachen, wenn Fintechs vorpreschen und eine tolle Lösung in den Markt bringen. **Empfehlen Sie Ihrem Arbeitgeber eine Lösung zum Kauf? Warum/warum nicht?** **AUF POST-IT MITSCHREIBEN (MODERATOR)** ***Besonderes Erkenntnisinteresse:*** ● ***Was hindert künftige Kunden am Kauf?***	**10'**	Post-Its auf Flipchart

Abschluss (5 Minuten)

Aufnahmegerät ausschalten

- **Danke** für die Zeit und Aussagen der Teilnehmenden.
- Wie **geht es nun weiter? // Santosh**
  - Aduno-Gruppe
  - Masterarbeit
- Teilnehmer **verabschieden.**

(Ende)

6.4.2 BEWERTUNGSBOGEN

6.4.2.1 PROBAND A

Bewertungsbogen Fokusgruppe "Authentifikation"

Bitte schreiben Sie die Nummer der vorgestellten Variante in eines der fünf Kästchen – abhängig davon, wie nahe die vorgestellte Variante an der Formulierung ist.
Nummerierung der Varianten:

1) Physische Biometrie (aktive Biometrie)
2) Secure Hardware
3 Verhaltensbiometrie (passive Biometrie)
4) mTAN/OTP per SMS
5 Zero-Touch / SoundProof

bedingt Smartphone

was wenn richtiger Nutzer, aber wrong Authentifikation?

								für diese Variante/n kann ich das nicht beurteilen (Nummer):
D1	Lösung ist unsicher	1	4	2	3	5	Lösung ist sicher	
D2	Lösung ist umständlich	5	3	2	4	1	Lösung ist einfach	
D3	Hoher Implementierungsaufwand für Banken	3	4	2	5	1	Geringer Implementierungsaufwand für Banken	
D4	Diese Lösung bietet ein schlechtes Kundenerlebnis	5	2	3	4	1	Diese Lösung bietet ein gutes Kundenerlebnis	
D5	Ein Kunde muss bei dieser Lösung viel eingeben/machen	5	2	4	3	1	Bei dieser Lösung läuft alles von alleine ~~bedingt Smartphone~~	
D6	Datenschutz ist bei dieser Lösung schlecht	3	5	4	2	1	Datenschutz ist bei dieser Lösung gut	
D7	Kunden werden dieser Lösung nur zögerlich zustimmen	5	3	2	4	1	Kunden werden dieser Lösung rasch zustimmen	
D8	Kunden werden nie für diese Lösung bezahlen	3	1	2	4	5	Kunden werden ohne Frage für diese Lösung bezahlen	
D9	Diese Lösung bietet Kunden nur wenig Anonymität	5	3	1	2	4	Diese Lösung bietet Kunden hohe Anonymität	
D10	Die Privatsphäre der Kunden ist bei dieser Lösung nicht gewahrt	5	3	4	1	2	Die Privatsphäre der Kunden ist bei dieser Lösung gewahrt	
D11	Das ist keine innovative Lösung	2	1	4	3	5	Das ist eine innovative Lösung	
D12	Kunden werden dieser Lösung nicht vertrauen	5	3	4	1	2	Kunden werden dieser Lösung vertrauen	

6.4.2.2 PROBAND B

Bewertungsbogen Fokusgruppe "Authentifikation"

Bitte schreiben Sie die Nummer der vorgestellten Variante in eines der fünf Kästchen – abhängig davon, wie nahe die vorgestellte Variante an der Formulierung ist.
Nummerierung der Varianten:

1) Physische Biometrie (aktive Biometrie)
2) Secure Hardware
3 Verhaltensbiometrie (passive Biometrie)
4) mTAN/OTP per SMS
5 Zero-Touch / SoundProof

								für diese Variante/n kann ich das nicht beurteilen (Nummer):
D1	Lösung ist unsicher		2	1	4		Lösung ist sicher	3
D2	Lösung ist umständlich	4	1	2	5		Lösung ist einfach	3
D3	Hoher Implementierungsaufwand für Banken	3	1	4	2	5	Geringer Implementierungsaufwand für Banken	
D4	Diese Lösung bietet ein schlechtes Kundenerlebnis	2	4	5	1		Diese Lösung bietet ein gutes Kundenerlebnis	3
D5	Ein Kunde muss bei dieser Lösung viel eingeben/machen		2	1	4	5	Bei dieser Lösung läuft alles von alleine	3
D6	Datenschutz ist bei dieser Lösung schlecht		2	4	1		Datenschutz ist bei dieser Lösung gut	3
D7	Kunden werden dieser Lösung nur zögerlich zustimmen		5	1	2	4	Kunden werden dieser Lösung rasch zustimmen	3
D8	Kunden werden nie für diese Lösung bezahlen		2	1	4	5	Kunden werden ohne Frage für diese Lösung bezahlen	3
D9	Diese Lösung bietet Kunden nur wenig Anonymität		3	1	2	4	Diese Lösung bietet Kunden hohe Anonymität	5
D10	Die Privatsphäre der Kunden ist bei dieser Lösung nicht gewahrt		3	1	2	5	Die Privatsphäre der Kunden ist bei dieser Lösung gewahrt	4
D11	Das ist keine innovative Lösung	2	4	1	3	5	Das ist eine innovative Lösung	
D12	Kunden werden dieser Lösung nicht vertrauen	3	4	2	5	1	Kunden werden dieser Lösung vertrauen	

6.4.2.3 PROBAND C

Bewertungsbogen Fokusgruppe "Authentifikation"

Bitte schreiben Sie die Nummer der vorgestellten Variante in eines der fünf Kästchen – abhängig davon, wie nahe die vorgestellte Variante an der Formulierung ist.
Nummerierung der Varianten:

1) Physische Biometrie (aktive Biometrie)
2) Secure Hardware
3 Verhaltensbiometrie (passive Biometrie)
4) mTAN/OTP per SMS
5 Zero-Touch / SoundProof

								für diese Variante/n kann ich das nicht beurteilen (Nummer):
D1	Lösung ist unsicher	3	4	5	2	1	Lösung ist sicher	
D2	Lösung ist umständlich	5		2	1	4	Lösung ist einfach	3
D3	Hoher Implementierungsaufwand für Banken	3	5	1	2	4	Geringer Implementierungsaufwand für Banken	
D4	Diese Lösung bietet ein schlechtes Kundenerlebnis	5 3	1	2	4 →		Diese Lösung bietet ein gutes Kundenerlebnis	
D5	Ein Kunde muss bei dieser Lösung viel eingeben/machen	5.	1	2	4	3	Bei dieser Lösung läuft alles von alleine	
D6	Datenschutz ist bei dieser Lösung schlecht	5 3	1	4	2 →		Datenschutz ist bei dieser Lösung gut	
D7	Kunden werden dieser Lösung nur zögerlich zustimmen	5 3	2	1 →		4	Kunden werden dieser Lösung rasch zustimmen	
D8	Kunden werden nie für diese Lösung bezahlen	3	5	4	1	2	Kunden werden ohne Frage für diese Lösung bezahlen	
D9	Diese Lösung bietet Kunden nur wenig Anonymität	5 3	1	2	4 →		Diese Lösung bietet Kunden hohe Anonymität	
D10	Die Privatsphäre der Kunden ist bei dieser Lösung nicht gewahrt	5 3	4	1	2 →		Die Privatsphäre der Kunden ist bei dieser Lösung gewahrt	
D11	Das ist keine innovative Lösung	4	2	1	5	3	Das ist eine innovative Lösung	
D12	Kunden werden dieser Lösung nicht vertrauen	3	4	1	2 →		Kunden werden dieser Lösung vertrauen	

5

6.4.2.4 PROBAND D

Bewertungsbogen Fokusgruppe "Authentifikation"

Bitte schreiben Sie die Nummer der vorgestellten Variante in eines der fünf Kästchen – abhängig davon, wie nahe die vorgestellte Variante an der Formulierung ist.
Nummerierung der Varianten:

1) Physische Biometrie (aktive Biometrie)
2) Secure Hardware
3 Verhaltensbiometrie (passive Biometrie)
4) mTAN/OTP per SMS
5 Zero-Touch / SoundProof

								für diese Variante/n kann ich das nicht beurteilen (Nummer):
D1	Lösung ist unsicher	5	2	1	3	4	Lösung ist sicher	
D2	Lösung ist umständlich	5	2	1	4	3	Lösung ist einfach	
D3	Hoher Implementierungsaufwand für Banken	5	2	3	4	1	Geringer Implementierungsaufwand für Banken	
D4	Diese Lösung bietet ein schlechtes Kundenerlebnis	2	5	1	4	3	Diese Lösung bietet ein gutes Kundenerlebnis	
D5	Ein Kunde muss bei dieser Lösung viel eingeben/machen	2	4	5	3	1	Bei dieser Lösung läuft alles von alleine	
D6	Datenschutz ist bei dieser Lösung schlecht	5	2	3	4	1	Datenschutz ist bei dieser Lösung gut	
D7	Kunden werden dieser Lösung nur zögerlich zustimmen	3	5	2	4	1	Kunden werden dieser Lösung rasch zustimmen	
D8	Kunden werden nie für diese Lösung bezahlen	5	2	3	4	1	Kunden werden ohne Frage für diese Lösung bezahlen	
D9	Diese Lösung bietet Kunden nur wenig Anonymität	5	3	1	4	2	Diese Lösung bietet Kunden hohe Anonymität	
D10	Die Privatsphäre der Kunden ist bei dieser Lösung nicht gewahrt	5	2	1	4	3	Die Privatsphäre der Kunden ist bei dieser Lösung gewahrt	
D11	Das ist keine innovative Lösung	2	1	4	5	3	Das ist eine innovative Lösung	
D12	Kunden werden dieser Lösung nicht vertrauen	5	3	4	2	1	Kunden werden dieser Lösung vertrauen	

6.4.2.5 PROBAND E

Bewertungsbogen Fokusgruppe "Authentifikation"

Bitte schreiben Sie die Nummer der vorgestellten Variante in eines der fünf Kästchen – abhängig davon, wie nahe die vorgestellte Variante an der Formulierung ist.
Nummerierung der Varianten:

1) Physische Biometrie (aktive Biometrie)
2) Secure Hardware
3 Verhaltensbiometrie (passive Biometrie)
4) mTAN/OTP per SMS
5 Zero-Touch / SoundProof

								für diese Variante/n kann ich das nicht beurteilen (Nummer):
D1	Lösung ist unsicher	2	4	5	1	3	Lösung ist sicher	
D2	Lösung ist umständlich	2	4	5	1	3	Lösung ist einfach	
D3	Hoher Implementierungsaufwand für Banken	3	2	5	1	4	Geringer Implementierungsaufwand für Banken	
D4	Diese Lösung bietet ein schlechtes Kundenerlebnis	2	4	1	5	3	Diese Lösung bietet ein gutes Kundenerlebnis	
D5	Ein Kunde muss bei dieser Lösung viel eingeben/machen	2	4	1	3	5	Bei dieser Lösung läuft alles von alleine	
D6	Datenschutz ist bei dieser Lösung schlecht	3	5	2	1	4	Datenschutz ist bei dieser Lösung gut	
D7	Kunden werden dieser Lösung nur zögerlich zustimmen	3	5	2	4	1	Kunden werden dieser Lösung rasch zustimmen	
D8	Kunden werden nie für diese Lösung bezahlen	1	4	5	2	3	Kunden werden ohne Frage für diese Lösung bezahlen	
D9	Diese Lösung bietet Kunden nur wenig Anonymität	5	3	1	4	2	Diese Lösung bietet Kunden hohe Anonymität	
D10	Die Privatsphäre der Kunden ist bei dieser Lösung nicht gewahrt	3	5	1	4	2	Die Privatsphäre der Kunden ist bei dieser Lösung gewahrt	
D11	Das ist keine innovative Lösung	2	4	1	3	5	Das ist eine innovative Lösung	
D12	Kunden werden dieser Lösung nicht vertrauen	2	5	3	4	1	Kunden werden dieser Lösung vertrauen	

6.4.2.6 PROBAND F

Bewertungsbogen Fokusgruppe "Authentifikation"

Bitte schreiben Sie die Nummer der vorgestellten Variante in eines der fünf Kästchen – abhängig davon, wie nahe die vorgestellte Variante an der Formulierung ist.
Nummerierung der Varianten:

1) Physische Biometrie (aktive Biometrie)
2) Secure Hardware
3 Verhaltensbiometrie (passive Biometrie)
4) mTAN/OTP per SMS
5 Zero-Touch / SoundProof

								für diese Variante/n kann ich das nicht beurteilen (Nummer):
D1	Lösung ist unsicher	2	4	5	1	3	Lösung ist sicher	
D2	Lösung ist umständlich	2	4	5	1	3	Lösung ist einfach	
D3	Hoher Implementierungsaufwand für Banken	3	2	5	1	4	Geringer Implementierungsaufwand für Banken	
D4	Diese Lösung bietet ein schlechtes Kundenerlebnis	2	4	1	5	3	Diese Lösung bietet ein gutes Kundenerlebnis	
D5	Ein Kunde muss bei dieser Lösung viel eingeben/machen	2	4	1	3	5	Bei dieser Lösung läuft alles von alleine	
D6	Datenschutz ist bei dieser Lösung schlecht	3	5	2	1	4	Datenschutz ist bei dieser Lösung gut	
D7	Kunden werden dieser Lösung nur zögerlich zustimmen	3	5	2	4	1	Kunden werden dieser Lösung rasch zustimmen	
D8	Kunden werden nie für diese Lösung bezahlen	1	4	5	2	3	Kunden werden ohne Frage für diese Lösung bezahlen	
D9	Diese Lösung bietet Kunden nur wenig Anonymität	5	3	1	4	2	Diese Lösung bietet Kunden hohe Anonymität	
D10	Die Privatsphäre der Kunden ist bei dieser Lösung nicht gewahrt	3	5	1	4	2	Die Privatsphäre der Kunden ist bei dieser Lösung gewahrt	
D11	Das ist keine innovative Lösung	2	4	1	3	5	Das ist eine innovative Lösung	
D12	Kunden werden dieser Lösung nicht vertrauen	2	5	3	4	1	Kunden werden dieser Lösung vertrauen	

6.4.2.7 PROBAND G

Bewertungsbogen Fokusgruppe "Authentifikation"

Bitte schreiben Sie die Nummer der vorgestellten Variante in eines der fünf Kästchen – abhängig davon, wie nahe die vorgestellte Variante an der Formulierung ist. Nummerierung der Varianten:

1) Physische Biometrie (aktive Biometrie)
2) Secure Hardware
3 Verhaltensbiometrie (passive Biometrie)
4) mTAN/OTP per SMS
5 Zero-Touch / SoundProof

								für diese Variante/n kann ich das nicht beurteilen (Nummer):
D1	Lösung ist unsicher	3	5	1	2	4	Lösung ist sicher	
D2	Lösung ist umständlich	3	5	4	1	2	Lösung ist einfach	
D3	Hoher Implementierungsaufwand für Banken	3	5	4	1	2	Geringer Implementierungsaufwand für Banken	
D4	Diese Lösung bietet ein schlechtes Kundenerlebnis	2	1	3	5	4	Diese Lösung bietet ein gutes Kundenerlebnis	
D5	Ein Kunde muss bei dieser Lösung viel eingeben/machen	2	3	1	4	5	Bei dieser Lösung läuft alles von alleine	
D6	Datenschutz ist bei dieser Lösung schlecht	2	3	4	5	1	Datenschutz ist bei dieser Lösung gut	
D7	Kunden werden dieser Lösung nur zögerlich zustimmen	5	3	1	2	4	Kunden werden dieser Lösung rasch zustimmen	
D8	Kunden werden nie für diese Lösung bezahlen	3	1	5	4	2	Kunden werden ohne Frage für diese Lösung bezahlen	
D9	Diese Lösung bietet Kunden nur wenig Anonymität	5	1	3	2	4	Diese Lösung bietet Kunden hohe Anonymität	
D10	Die Privatsphäre der Kunden ist bei dieser Lösung nicht gewahrt	3	1	4	5	2	Die Privatsphäre der Kunden ist bei dieser Lösung gewahrt	
D11	Das ist keine innovative Lösung	2	4	1	3	5	Das ist eine innovative Lösung	
D12	Kunden werden dieser Lösung nicht vertrauen	3	5	1	2	4	Kunden werden dieser Lösung vertrauen	

6.4.2.8 PROBAND H

Bewertungsbogen Fokusgruppe "Authentifikation"

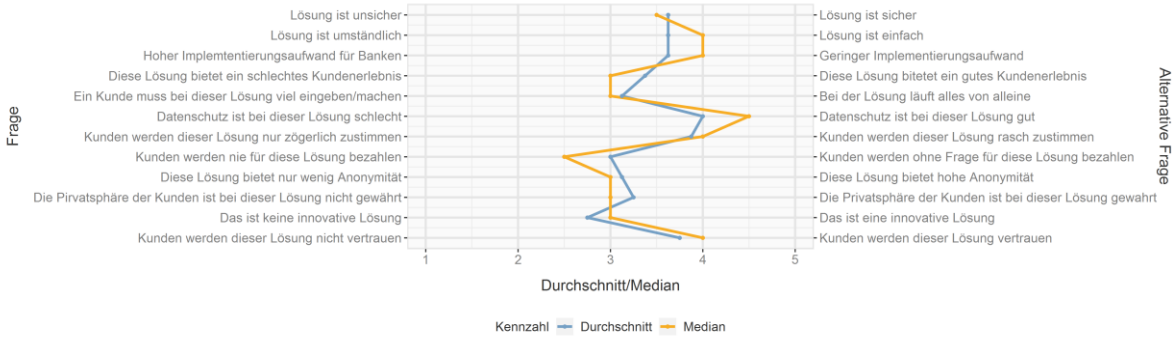
Bitte schreiben Sie die Nummer der vorgestellten Variante in eines der fünf Kästchen – abhängig davon, wie nahe die vorgestellte Variante an der Formulierung ist. Nummerierung der Varianten:

1) Physische Biometrie (aktive Biometrie)
2) Secure Hardware
3 Verhaltensbiometrie (passive Biometrie)
4) mTAN/OTP per SMS
5 Zero-Touch / SoundProof

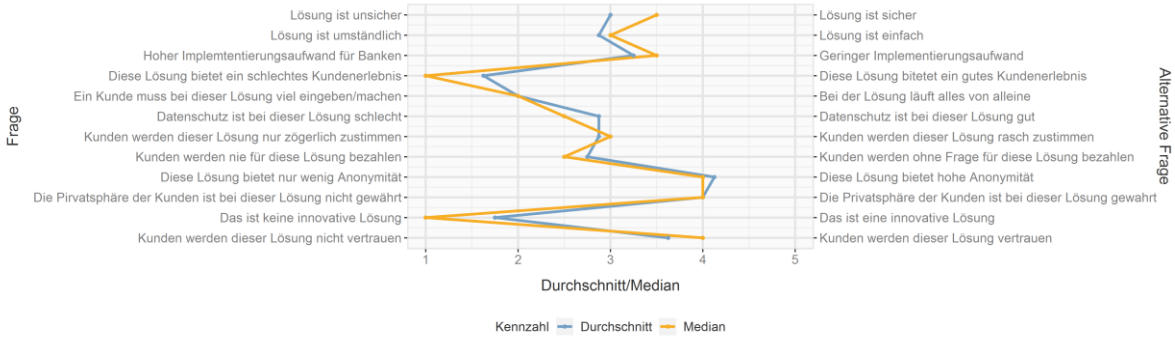
								für diese Variante/n kann ich das nicht beurteilen (Nummer):
D1	Lösung ist unsicher	5	3	4	2	1	Lösung ist sicher	
D2	Lösung ist umständlich	2	4	5	1	3	Lösung ist einfach	
D3	Hoher Implementierungsaufwand für Banken	2	4	5	1	3	Geringer Implementierungsaufwand für Banken	
D4	Diese Lösung bietet ein schlechtes Kundenerlebnis	2	3	4	5	1	Diese Lösung bietet ein gutes Kundenerlebnis	
D5	Ein Kunde muss bei dieser Lösung viel eingeben/machen	4	2	1	3	5	Bei dieser Lösung läuft alles von alleine	
D6	Datenschutz ist bei dieser Lösung schlecht	5	4	3	2	1	Datenschutz ist bei dieser Lösung gut	
D7	Kunden werden dieser Lösung nur zögerlich zustimmen	2	4	5	1	3	Kunden werden dieser Lösung rasch zustimmen	
D8	Kunden werden nie für diese Lösung bezahlen	2	3	4	5	1	Kunden werden ohne Frage für diese Lösung bezahlen	
D9	Diese Lösung bietet Kunden nur wenig Anonymität	4	3	5	2	1	Diese Lösung bietet Kunden hohe Anonymität	
D10	Die Privatsphäre der Kunden ist bei dieser Lösung nicht gewahrt	4	3	5	2	1	Die Privatsphäre der Kunden ist bei dieser Lösung gewahrt	
D11	Das ist keine innovative Lösung	2	4	1	5	3	Das ist eine innovative Lösung	
D12	Kunden werden dieser Lösung nicht vertrauen	5	2	3	4	1	Kunden werden dieser Lösung vertrauen	

6.4.3 Polariätätsprofile

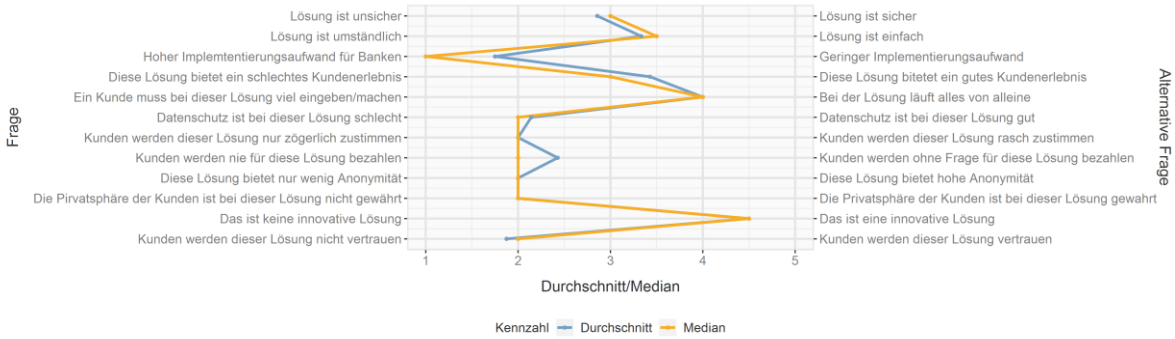
6.4.3.1 Aktive Biometrie



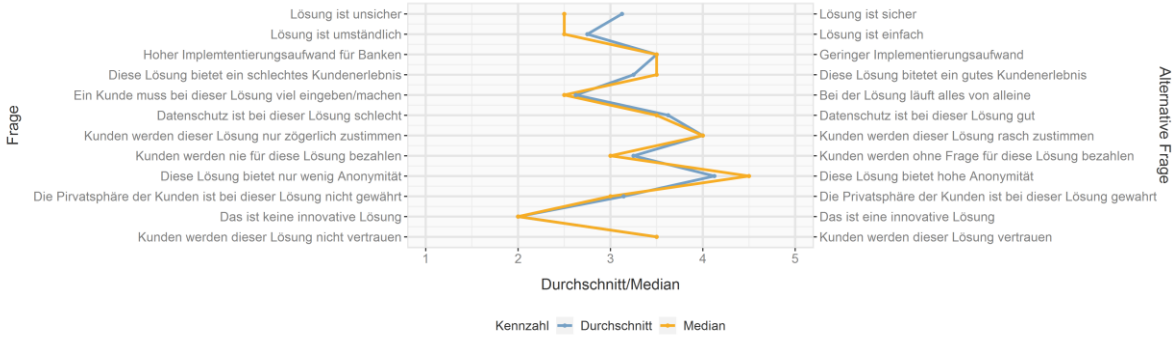
6.4.3.2 Seucre Hardware



6.4.3.3 Passive Biometrie



6.4.3.4 SMS / OTP



6.4.3.5 ZERO-TOUCH / SOUNDPROOF