FERDINAND PORSCHE
FERN FH

Payment Solutions – PSD2 und die Veränderungen für die NutzerInnen im österreichischen Zahlungsverkehr

Masterarbeit

eingereicht von: **Fabian Kleindienst, BA**
Matrikelnummer: 51833904

im Fachhochschul-Masterstudiengang Wirtschaftsinformatik

der Ferdinand Porsche FernFH GmbH

zur Erlangung des akademischen Grades

Master of Arts in Business

Betreuung und Beurteilung: Thomas Krabina, MSc

Zweitgutachten: Ing. DI Andreas Eisenbock, BA MA

Wien, Mai 2020

Ehrenwörtliche Erklärung

Ich versichere hiermit,

1. dass ich die vorliegende Masterarbeit selbständig verfasst und keine anderen als die angegebenen Quellen und Hilfsmittel benutzt habe. Alle Inhalte, die direkt oder indirekt aus fremden Quellen entnommen sind, sind durch entsprechende Quellenangaben gekennzeichnet.

2. dass ich diese Masterarbeit bisher weder im Inland noch im Ausland in irgendeiner Form als Prüfungsarbeit zur Beurteilung vorgelegt oder veröffentlicht habe.

3. dass die vorliegende Fassung der Arbeit mit der eingereichten elektronischen Version in allen Teilen übereinstimmt.

Wien, 18.05.2020 _____

Unterschrift

Kurzzusammenfassung: Payment Solutions – PSD2 und die Veränderungen für die NutzerInnen im österreichischen Zahlungsverkehr

Im Rahmen der Masterarbeit wird die Einführung der Payment Service Directive 2 (PSD2) und die Auswirkungen auf die NutzerInnen von online Services im österreichischen Zahlungsverkehr analysiert. Die PSD2 ist eine Zahlungsdienstrichtlinie und wurde im Jahr 2015 innerhalb der Europäischen Union eingeführt. Im Jahr 2019 trat eine Delegierte Verordnung als Ergänzung zur Zahlungsdienstrichtlinie in Kraft, welche die Bereiche Zwei-Faktor-Authentifizierung und Open Banking reguliert. Diese Regulierung lassen Lösungswege zur Umsetzung der Anforderungen bewusst offen, um keinen Einfluss auf Innovationen zu nehmen. Die Hauptziele sind die Förderung des Wettbewerbs und die Erhöhung der Sicherheit im europäischen Zahlungsverkehr. Zusätzlich zur Aufbereitung der Theorie, wurde eine online Befragung, in Form eines Fragebogens unter 287 gültigen TeilnehmerInnen ausgewertet. Dabei wurde das Verhalten der Nutzung von online Zahlungsservices, das Empfinden zur Sicherheit, der Usability und dem Vertrauen zur Zwei-Faktor-Authentifizierung und Open Banking evaluiert. Dabei zeigt sich, dass sowohl die Sicherheit, das Vertrauen als auch die Usability von Zwei-Faktor-Authentifizierungen positiv bewertet wurde. Beurteilungsunterscheidungen gibt wenn das Alter, die Herkunft, der Beruf und der Zahlungsdienstleister einbezogen werden. Open Banking ist unter den TeilnehmerInnen überwiegend unbekannt und daher wenig in Verwendung. In diesem Bereich fehlt es an Informationen für die NutzerInnen. Ein Trend Richtung App-basierter Zahlungslösungen ist erkennbar, auch die Anzahl der Nutzung von online Banking ist im Vergleich zum Jahr 2018 steigend.

Schlagwörter:

Payment Service Directive 2, Strong Customer Authentication, Open Banking, Zahlungsdienstrichtlinie, IT-Sicherheitsrichtlinien

Abstract: Payment Solutions – PSD2 and the changes for users in the Austrian payment sector

This master thesis deals with the new European payment regulation called "Payment Service Directive 2" (PSD2) and in particular with its effects on users in online services in the Austrian payment sector. The regulation was established in 2015 by the European Union. Four years later, in 2019, an additional regulation was established which deals with the Two-Factor-Authentication and Open Banking. These bodies of laws have room for interpretation and innovation. The main goal of PSD2 and its amendments is to foster competition and security within the European payment sector. This work analyses the status quo and uses an online survey with a questionnaire producing 287 valid data sets. Results: The sense for security, usability and trust in Two-Factor-Authentication was seen positively. There are demographic differences between age groups, professions, and localisation. Also, the payment service provider influences the result. Open Banking is a large unknown to the participants where there is lack of information for more than 75 percent. Generally, there was noticed a trend using app-based payment technologies and online payment services compared to a research from 2018.

Danksagung

Ein besonderer Dank gilt Herrn Thomas Krabina, MSc für die Betreuung während der Entstehung der Masterarbeit. Durch umfassendes und auch kritisches Feedback war es mir möglich eine laufende Qualitätssteigerung der Arbeit zu erreichen und fachliche Themenbereiche zu verbessern.

Zusätzlichen Dank möchte ich allen Personen aussprechen, die mich im Rahmen der Erstellung dieser Masterarbeit sowie im laufenden Studium unterstützten.

Inhaltsverzeichnis

1. Einleitung

In Kapitel 1 geht es darum, den LeserInnen einen Überblick über die Themenstellung, die Forschungsfrage, das Ziel der wissenschaftlichen Arbeit und die folgenden Kapitel zu geben.

1.1 Themenstellung und Relevanz der Themenstellung

Am 13. Januar 2018 ist die Payment Service Directive (PSD2) in der Europäischen Union (EU) in Kraft getreten. Ursprünglich galt, dass alle Zahlungsdienstleister bis 14. September 2019 der PSD2 Richtlinie nachkommen und unter anderem Strong Customer Authentification (SCA), weiter erläutert im Regulatory Technical Standards (RTS), anbieten müssen. Die Europäische Bankenaufsichtsbehörde (EBA) hat im Juni 2019 beschlossen, den Zahlungsdienstleistern einen Aufschub zu gewähren. Am 16.10.2019 verkündete die EBA den Aufschub bis 31.12.2020 zu gewähren. Dies gelte jedoch nur für SCA und nicht für Open Banking, der Öffnung von Konten für Drittanbieter. (Europäische Bankenaufsichtsbehörde, 2019b, S. 3)

Die SCA hat das Ziel, den AnwenderInnen ein sicheres Authentifizierungsverfahren anzubieten und das Betrugsrisiko zu minimieren. Des Weiteren wird in der Richtlinie die Vorgehensweise für Open Banking geregelt, welche die Öffnung des Zahlungsverkehrs für Drittanbieter ermöglicht. Im RTS sind die Anforderungen zu SCA und Open Banking definiert, lassen jedoch Lösungswege, den Anforderungen zu entsprechen, offen. In der RTS sind die Faktoren Wissen, Besitz und Inhärenz beschrieben, sowie welche Möglichkeiten, welchem Faktor zugeordnet werden können. Ebenso ist die sogenannte Zwei-Faktor-Authentifikation (2FA), bei der Verwendung von zwei der drei genannten Faktoren, definiert. Die Art der Kombination der Faktoren sowie die zu verwendeten Umsetzungsmöglichkeiten obliegt den Zahlungsdienstleistern. Einige Zahlungsdienstleister, unter ihnen die BAWAG P.S.K, haben die Anforderungen im September 2019 umgesetzt. Die Erste

Group Bank hat bereits eine konforme Lösung umgesetzt und löste damit die bestehende im Juni 2019 vollständig ab.

In der, der PSD2 zugrundeliegenden Problemstellung werden Lösungs- und Interpretationsspielräume offen gelassen. Daraus entstehen verschiedene Auswirkungen auf die KundInnen. Diese werden in der Masterarbeit evaluiert, der Vor- und Nachteile aufgezeigt, sowie mittels Befragung, durch die KundInnensichtweise ergänzt. Dabei wird auf Themen wie Vertrauen, Sicherheit und Benutzerfreundlichkeit näher eingegangen. Vor allem für Zahlungsdienstleister, die der Umsetzung der PSD2 noch nicht nachgekommen sind oder zukünftige Zahlungsdienstleister, die für deren Lösungsansätze Informationen heranziehen wollen, ist das Ergebnis dieser Masterarbeit eine Unterstützung, da es keine „Best Practice"-Lösungen gibt. Ebenso ist das Ziel die verschiedenen Ergebnisse für die NutzerInnen aufzubereiten.

Um für die LeserInnen einen roten Faden zu erzeugen, wird in den ersten Kapiteln die Theorie aus vorhandener Literatur, vor allem online Literatur, Sachbücher, Spezifikationen und Richtlinien, erläutert. Darin enthalten sind Informationen zur PSD2 und zur RTS. Des Weiteren werden die Vor- und Nachteile sowie Chancen und Risiken der PSD2 bzw. RTS erarbeitet. Durch eine online Befragung der KundInnen verschiedener österreichischer Zahlungsdienstleister wird die Forschungsfrage beantwortet.

Der Bezug zur Wirtschaftsinformatik ist durch Inhalte der Sicherheits- und Informationstechnologie bei SCA und Open Banking vorhanden. Ebenso besteht eine Verbindung zu verteilten Systemen, da verschiedene Systemlösungen miteinander kombiniert werden können. Anhand der Auswirkungen wird der Bezug zum Qualitäts- und Kundenbeziehungsmanagement hergestellt.

1.2 Forschungsfrage und Zielsetzung

Wie wirken sich die Veränderungen der PSD2 auf die NutzerInnen im österreichischen Zahlungsverkehr aus?

Das Ziel dieser Masterarbeit ist, die in der Einleitung beschriebene Problemstellung, zu erarbeiten. Dafür werden die verschiedenen Möglichkeiten mit deren Vor- und Nachteilen sowie Chancen und Risiken analysiert und mittels Befragungen der NutzerInnen statistische Ergebnisse ausgewertet und interpretiert.

Dabei werden einerseits die verschiedenen Möglichkeiten der Zahlungsdienstleister in deren Umsetzung von SCA aufgezeigt, ein Überblick über Open Banking geschaffen und die Wissenslücke von NutzerInnen zu diesem Thema geschlossen. Mittels Befragung der NutzerInnen werden die Auswirkungen und die Vor- und Nachteile aufgezeigt.

1.3 Methodische Vorgehensweise

Die Beantwortung der Forschungsfrage basiert auf einer Literatur Recherche sowie einer quantitativen Recherche, eine Befragung der NutzerInnen mittels online Fragebogen. In der Literatur wird recherchiert, welche Auswirkungen durch die Umsetzung der RTS innerhalb der PSD2 gegeben sind und welche Vor- und Nachteile sowie Chancen und Risiken daraus resultieren. Nach Aufbereitung dieser Inhalte, wird mittels online Fragebogen die Sichtweise der NutzerInnen erhoben. Die Datenerhebung mittels online Fragebogen hat den Vorteil, dass eine große Anzahl verschiedener Merkmale von KundInnen und eine Verteilung über verschiedene Zahlungsdienstleister erzielt werden können. Durch gezielte Kontaktaufnahme im Kreis der Familie und KollegInnen sowie sozialen Medien und Foren wird versucht eine hohe Rücklaufquote zu erhalten. Dafür werden rund 400 KundInnen von verschiedenen österreichischen Zahlungsdienstleistern befragt, um ein statistisch signifikantes Feedback zu erhalten. Bei einer Populationsgröße von über 5 Millionen KundInnen, welche im Zahlungsverkehr online Services nutzen, ist

mit einem Konfidenzniveau von 90% und einer zu erwartenden Fehlerrate von 5% eine Stichprobe von 271 KundInnen repräsentativ. (surveymonkey, 2019; qualtrics, 2020; statista, 2020a; statista, 2020b)

Mit der Unterstützung von Kanälen wie LinkedIn, XING, Facebook und E-Mail wird die Umfrage verbreitet. Mit den Ergebnissen können die Auswirkungen von SCA und die Meinung über Open Banking ermittelt werden. Zur Analyse verschiedener Auswirkungen auf die NutzerInnen werden demographische Merkmale hinzugezogen. Durch diese Erhebung sollen deskriptive statistische Erkenntnisse erarbeitet und, in Kombination mit den theoretischen Erhebungen, die Forschungsfrage beantwortet werden. Mit geeigneter Software (Microsoft Excel) wird die Auswertung unterstützt und aufbereitet. Für die Durchführung der quantitativen Methode, die online Fragebögen, wird das online Tool von „UmfrageOnline“ herangezogen.

1.4 Aufbau der Masterarbeit

Um den LeserInnen einen klar strukturierten Überblick der Themenstellung und die Vorgehensweise zur Beantwortung der Forschungsfrage zu geben, ist diese Arbeit wie folgt aufgebaut: Im Kapitel 2 sind die wichtigsten Begriffe zum besseren Verständnis für die weiteren Kapitel erklärt. Im Kapitel 3 wird auf den theoretischen Teil der PSD2, das ist einerseits die SCA und andererseits Open Banking, eingegangen. In Kapitel 4 werden die Erkenntnisse aus Kapitel 3 mittels empirischer Methode – die online Befragung – erhoben und analysiert. Im Kapitel 5 werden die statistischen Ergebnisse interpretiert und die Forschungsfrage beantwortet. In der Conclusio werden die Erkenntnisse zusammengefasst und ein Ausblick über weitere Forschungsmöglichkeiten gegeben.

2. Begriffserklärungen und Grundlagen

Im Kapitel 2 werden die wichtigsten Grundlagenbegriffe, zur besseren Verständlichkeit der folgenden Kapitel, definiert.

2.1 Organe, Zahlungsdienstleister und Drittanbieter

2.1.1 Europäische Bankenaufsicht

Die Europäische Bankenaufsichtsbehörde (EBA) hat zur Aufgabe, den europäischen Bankensektor zu regulieren und zu beaufsichtigen. Die EBA handelt als unabhängige EU-Behörde mit Rechenschaftspflichten gegenüber der Europäischen Kommission und dem Rat der Europäischen Union. Eine der Hauptaufgaben ist die Erarbeitung von technischen Standards und Leitlinien, damit ein einheitliches Regelwerk im Finanzsektor der EU gewährleistet ist. Folglich resultiert der Vorschlag des technischen Regulierungsstandards (RTS) für SCA und Open Banking von der EBA. (Europäische Bankenaufsichtsbehörde, 2018b)

2.1.2 Europäische Kommission

Die Europäische Kommission (EU-Kommission) besteht aus VertreterInnen der 28 EU-Ländern. Die VertreterInnen informieren darüber, welche Auswirkungen der EU-Politik auf ihr jeweiliges Land zutreffen und berichten über Entwicklungen der einzelnen Länder in der Kommission in Brüssel. Von der EU-Kommission wurde einerseits die Richtlinie (EU) 2015/2366 (PSD2) verabschiedet und andererseits die RTS für SCA und Open Banking angenommen, minimal adaptiert und als Delegierte Verordnung (EU) 2018/389 verabschiedet. Die Delegierte Verordnung gibt die Möglichkeit, innerhalb von Fristen, Anmerkungen zu definieren und ein in Kraft treten des Beschlusses zu verhindern. (Europäische Kommission, 2015; Juraforum, o. J.)

2.1.3 Zahlungsdienstleister

Als Zahlungsdienstleister sind Kreditinstitute, E-Geld Institute, Zentralbanken und Unternehmen, die Zahlungsdienste anbieten und nicht in die zuvor genannten Kategorien einzuordnen sind, einzustufen. Als Unternehmen, welche Zahlungsdienste anbieten, können die im Folgekapitel 2.1.4 beschriebenen Drittanbieter gesehen werden. (Metzger, o. J.)

2.1.4 Drittanbieter, dritte Zahlungsdienstleister, Third Party Provider

Die Entwicklungen im Zahlungsverkehr innerhalb Europas bringen neue Zahlungsanbieter auf die Märkte. Diese Marktteilnehmer werden unter den Begriffen Drittanbieter, dritte Zahlungsdienstleister oder Third Party Provider (TPP) angeführt. In diesem Zusammenhang wird auch der Begriff FinTech genannt. (Europäische Kommission, 2017)

Drittanbieter lassen sich in zwei Gruppen teilen: (Europäische Kommission, 2017)

- Die Zahlungsauslösedienstleister, auch genannt Payment Initiation Service Provider (PISP), haben die Aufgabe die Zahlungen im Einverständnis von KundInnen auszulösen und den HändlerInnen die Abwicklung einer Transaktion zu bestätigen.
- Die Kontoinformationsdienstleister, auch genannt Account Information Service Provider (AISP), schaffen Portale und haben die Aufgabe den KundInnen einen Überblick über deren Finanzen zu gewähren.

2.2 Payment Service Directive 2

Die Payment Service Directive 2 (PSD2) ist eine Zahlungsdienstrichtlinie, welche die Richtlinie (EU) 2007/64/EG (PSD) durch die Richtlinie (EU) 2015/2366 ablöst. Die PSD, auch PSD1 genannt, wurde bereits im Jahr 2007 innerhalb der EU in Kraft gesetzt. Die Richtlinie regelte bereits den elektronischen und nicht elektronischen Zahlungsverkehr und hatte das Ziel, den Wettbewerb im Finanzsektor zu fördern.

Gleichzeitig sollte die Regulierung der Banken die VerbraucherInnen schützen. Die Single European Payment Area (SEPA) hat ihren Ursprung in der PSD1 und vereinheitlicht den Zahlungsverkehr im europäischen Raum. Durch ein vermehrtes Eintreten von Drittanbietern in den europäischen Finanzmarkt wurden Finanztransfers ohne Zustimmung der EBA, auf nationaler Ebene die Finanzmarktaufsichtsbehörde (FMA), durchgeführt. Dies resultiert aus nicht vorhandenen und interpretierbaren Regelungen. Die PSD2 bildet eine Überleitung zur Aufnahme von Kontoinformations- und Zahlungsauslösedienstleistern in die neue Richtlinie.

Eine weitere Unterscheidung ist die Regelung zur verpflichtenden Kontoöffnung der Banken für Drittanbieter, unter der Einwilligung der VerbraucherInnen. Ständige technologische Entwicklungen der Digitalisierung und Weiterentwicklungen in der Kommunikation erzwangen die Überarbeitung der Richtlinie. (Krautkrämer, 2018)

Die PSD2 beinhaltet Regelungen für Zahlungsdienstleister und Drittanbieter im europäischen Zahlungsverkehr. Die Regelung wurde von der EU Kommission, nach Beauftragung der Europäischen Bankenaufsichtsbehörde (EBA) und der Europäischen Zentralbank (EZB) zur Ausarbeitung, freigegeben. Die verfolgten Hauptziele sind die Erhöhung des Wettbewerbes und die Sicherheit im Zahlungsverkehr des europäischen Marktes. Der Ausarbeitungsprozess vollzog sich über einen Zeitraum von Oktober 2015 bis zur in Kraft Setzung im September 2019. (MoneyToday, o. J.)

Die Hauptziele der PSD2 sind die Förderung des europäischen Wettbewerbs in einem digitalisierten Umfeld und der Schutz der VerbraucherInnen. Maßnahmen, die zur Erreichung dieser Ziele beitragen sollen und von den Zahlungsdienstleistern sowie Drittanbietern einzuhalten sind, werden darin definiert. Hier wird auch beschrieben, wann eine Anwendung von SCA notwendig ist und wann Ausnahmen gültig sind. (Europäische Kommission, 2017)

2.3 Technische Regulierungsstandards

Der technische Regulierungsstandard (RTS) hilft allen MarktteilnehmerInnen die Anweisungen der PSD2 erfüllen zu können. Der RTS basiert auf einem erarbeiteten Entwurf der EBA und der EZB, welcher durch die EU Kommission minimal abgeändert und als Delegierte Verordnung (EU) 2018/389 veröffentlicht wurde. (Europäische Kommission, 2017)

Die Änderungen der EU Kommission beziehen sich auf die Kapitel 1, 3 und 5. In Kapitel 1 schlägt die EBA vor, dass die risikobasierte Ausnahme von SCA (siehe Kapitel 3.2.4) periodisch von internen oder externen AuditorInnen überprüft werden muss. Dies ergänzt die EU Kommission insofern, dass sie festhält, dass das Risikomodell zusätzlich, mindestens alle drei Jahre, von unabhängigen externen AuditorInnen überprüft werden muss. (Europäische Bankenaufsichtsbehörde, 2017b, S. 2; Europäische Bankenaufsichtsbehörde, 2017a, S. 19; DelVO (EU) 2018/389 ABl. L 69/28, 3)

Des Weiteren wurde zu den Ausnahmen der Artikel 17 (siehe Kapitel 3.2.4) von der EU Kommission hinzugefügt. Bei einem Artikel der SCA Ausnahmen wurde ergänzt, dass die Überschreitung von Schwellwerten der Betrugsraten an die EBA und die nationale Behörde, in Österreich die FMA, zu melden ist. (Europäische Bankenaufsichtsbehörde, 2017b, S. 2)

Zuletzt wurde von der EU Kommission hinzugefügt, dass bei einer Nichtverfügbarkeit einer dedizierten Schnittstelle zum Zahlungsdienstleister, jene Schnittstelle, die der Zahlungsdienstleister den eigenen KundInnen anbietet, als Alternative verfügbar gemachen werden muss. (Europäische Bankenaufsichtsbehörde, 2017b, S. 2; DelVO (EU) 2018/389 ABl. L 69/39, 33)

2.4 Strong Customer Authentification

Die Strong Customer Authentification (SCA) ist bereits bekannt für die Anwendung im herkömmlichen Handel. Mittels dem „Besitz“ einer Karte und dem „Wissen“ eines

PIN-Codes wird bereits SCA zur Validierung bei Transaktionen am Bezahlterminal angewendet. Bei elektronischen Ferntransaktionen ist SCA bis zur in Kraft Setzung der PSD2 nicht verpflichtend. Mit dem RTS werden die Details von SCA geregelt. Die SCA setzt sich aus der Anwendung von zwei der drei Kriterien „Wissen", „Besitz" und „Inhärenz" zusammen. Das heißt, KundInnen müssen zum Auslösen einer Transaktion z.B. einen PIN-Code wissen, eine Karte besitzen oder mittels Fingerabdruck identifizierbar sein, um sich aus der Kombination von zwei der drei Kriterien validieren zu können. (Europäische Kommission, 2017)

2.5 Open Banking

Open Banking bedeutet die Bereitstellung von Daten und Funktionen über eine Schnittstelle zum Zahlungsdienstleister, die es ermöglicht Inhalte von Bank A bei Bank B anzuzeigen oder Transaktionen für Bank A in der Oberfläche von Bank B auszulösen. Mit dieser Schnittstelle wird auch Drittanbietern die Möglichkeit gegeben, unter der Einwilligung von NutzerInnen, Transaktionen einer Bank auszulösen oder Informationen von verschiedenen Banken zusammengefasst darzustellen. (MoneyToday, o. J.)

2.6 Abgrenzung

Die Richtlinie (EU) 2007/64/EG (PSD 1) ist seit 2007 innerhalb Europas in Kraft und wurde durch die Richtlinie (EU) 2015/2366 (PSD2) im Jahr 2015 abgelöst. Diese wurde aufgrund der Veränderungen im Zahlungsverkehr, die vermehrte Verwendung von mobile Banking und das ungeregelte Eindringen von Drittanbietern in den Finanzmarkt, durch die Delegierte Verordnung (EU) 2018/389 ergänzt.

Das Hauptaugenmerkt der Masterarbeit bezieht sich auf die Richtlinie (EU) 2015/2366 (PSD2) und speziell auf die Delegierte Verordnung (EU) 2018/389, welche die Richtlinie in den Schwerpunkten SCA und Open Banking ergänzt. Die PSD1 wird hier nicht näher bearbeitet.

In der Richtlinie (EU) 2015/2366 (PSD2) werden weitere Themen behandelt, auf welche im Rahmen dieser Masterarbeit nicht weiter eingegangen wird. Folgend einige Aufzählungen:

- Beantragung und Erteilung und Entzug der Zulassung zum Zahlungsdienstleister
- Beteiligungen, Kapitalzusammensetzung und Eigenmittel
- Rechnungslegung und Abschlussprüfung
- Beaufsichtigung und Kontrolle der zuständigen Behörden
- Geheimhaltungspflichten
- Vertragsrelevante Inhalte

3. PSD2 Richtlinie

In Kapitel 3 wird vorerst näher auf aktuelle, themenrelevante Artikel eingegangen. In weiterer Folge wird auf den RTS, die SCA mit ihren Möglichkeiten sowie Handlungsspielräumen, die Eigenschaften von Open Banking, einige Beispiele und Erkenntnisse aus der Praxis und die resultierenden Vor- und Nachteile, eingegangen.

In Folge der PSD2 Richtline wurden die Transaktionsnummern (TAN), bekannt in der Form einer Papier Liste, abgeschafft. Ersetzt wurde diese Art der Authentifizierung weitgehend durch mobile Applikationen (mobile-App). Einzelne Zahlungsdienstleister bieten zusätzlich die Möglichkeit einer mobileTAN, eine Transaktionsnummer, die als SMS zugesendet wird, an. Zurückzuführen sind diese Änderungen auf die SCA. (derstandard, 2019)

Mehr als die Hälfte der ÖsterreicherInnen nutzen Online Banking. Das liegt über dem europäischen Durchschnitt. (eurostat, 2019) Daher sind die Auswirkungen der PSD2 sowohl für die NutzerInnen als auch für die Zahlungsdienstleister spürbar. Durch SCA soll vor allem die Sicherheit für NutzerInnen im Zahlungsverkehr erhöht werden. Die Verwendung setzt jedoch ein Smartphone voraus, was vor allem von NutzerInnen jener Zahlungsdienstleister, welche ausschließlich SCA mittels App anbieten, einen Kritikpunkt darstellt. Zusätzlich wird die Verwendung aus Sicht der Freundlichkeit für die NutzerInnen in den Medien diskutiert und bringt den Zahlungsdienstleistern negative Kritiken. (Al-Youssef, 2019) NutzerInnen, welche Online Banking mittels Computer oder Notebook bevorzugen, sind zukünftig ebenso an das Smartphone gebunden. (red./tirol.ORF, 2019)

Im zweiten Teilbereich der PSD2, dem Open Banking, werden Zahlungsdienstleister verpflichtet, bei Verlangen ihrer KundInnen das Konto zu öffnen. Dazu müssen alle Zahlungsdienstleister seit September 2019 eine Schnittstelle anbieten, welche Drittanbietern den Zugriff auf Konten ermöglicht. Mit dieser Maßnahme sollen die

Dienstleistungen und Innovationen für NutzerInnen erweitert werden, sowie der Wettbewerb unter den Zahlungsdienstleistern erhöht werden. (erstegroup, 2019)

3.1 Regulatorischer technischer Standard

Der RTS betrifft die Regelung von SCA und Open Banking. Der RTS ist in enger Zusammenarbeit zwischen der Europäischen Banken Aufsicht (EBA) und der Europäischen Zentral Bank (EZB) entwickelt worden. (Europäische Bankenaufsichtsbehörde, 2017a, S. 3 f.) In den Jahren 2015 bis 2017 wurden Entwürfe erarbeitet, zu denen Stellung genommen werden konnte. Dafür wurden Veranstaltungen für alle TeilnehmerInnen innerhalb des Zahlungsverkehrs und TeilnehmerInnen aus anderen Branchen organisiert. Am 23. Februar 2017 wurde ein finaler Entwurf durch die EBA veröffentlicht, welcher am 27. November 2017 durch die EU Kommission angenommen wurde. Am 13. März 2018 ist der angenommene Entwurf als Delegierte Verordnung (EU) 2018/389 und Ergänzung zur Richtlinie (EU) 2015/2366 veröffentlicht worden. (Fletzberger, 2019)

Innerhalb der RTS wird in die Bereiche der

- Anforderungen an SCA,
- Ausnahmen von SCA,
- Anforderungen an die Sicherheitsmaßnahmen zur Wahrung von personalisierten Daten der NutzerInnen und
- Anforderungen an Open Banking in Bezug auf die Kommunikation zwischen Zahlungsdienstleistern, Zahlungsauslösediensten und Kontoinformationsdiensten unterteilt. (Europäische Bankenaufsichtsbehörde, 2017a, S. 3 f.)

Die Schlüsselstellen, resultierend aus den Diskussionen und dem Feedback, sind die technologischen Anforderungen, den technologischen Umfang neutral zu behandeln, der Umgang mit Ausnahmen von identifizierten „low risk“ Transaktionen und die

Anforderungen an Zahlungsdienstleister und Drittanbieter im Zusammenhang mit Open Banking. Innerhalb der genannten Schlüsselstellen ist auf

- die Verbesserung der Sicherheit,
- die Förderung des Wettbewerbs,
- die Gewährleistung der Neutralität von Technologien und Geschäftsmodellen,
- den Schutz der NutzerInnen,
- die Erleichterung von Innovationen und
- die Verbesserung des Komforts der NutzerInnen einzugehen.

Dabei handelt es sich um herausfordernde Kompromisse in den konkurrierenden Zielen der PSD2. (Europäische Bankenaufsichtsbehörde, 2017a, S. 3 f.)

3.1.1 Umfang und neutrale Technologien

Aufgrund interpretierbarer Artikel, welche innerhalb der RTS geregelt sind, stellt die EBA klar, dass diese den Inhalt der RTS nicht selbst festlegen, sondern Inhalte bereits in der Richtlinie (EU) 2015/2366 definiert sind. In Artikel 97 und 98 dieser Richtlinie wird die Geltung für die Authentifizierung und die technologischen Standards der Authentifizierung und der Kommunikation festgehalten. (Europäische Bankenaufsichtsbehörde, 2017a, S. 7 f.; RL (EU) 2015/2366 ABl. L 337/106, 97; RL (EU) 2015/2366 ABl. L 337/106, 98)

Im Artikel 97 beschreibt die EU Kommission, dass ein Zahlungsdienstleister aus einem EU Mitgliedsstaat die SCA bei online Zugriffen auf ein Zahlungskonto, bei einer Auslösung eines elektronischen Zahlungsvorgangs und bei Fernzugängen anbieten muss. Bei Fernzugängen muss SCA verwendet werden, sobald Prozesse ausgeführt werden, welche das Risiko zu Betrug und Missbrauch beinhalten. Des Weiteren muss sichergestellt werden, dass die Beträge beim Zahlungsvorgang mit den ZahlungsempfängerInnen dynamisch verlinkt und die personalisierten Sicherheitsmerkmale der NutzerInnen geschützt sind. Die kontoführenden Zahlungsdienstleister sind verpflichtet den Kontoinformationsdiensten und

Zahlungsauslösediensten das Authentifizierungsverfahren, welches den NutzerInnen zur Verfügung gestellt wird, ebenso zur Verfügung zu stellen. (RL (EU) 2015/2366 ABl. L 337/106, 97)

Im Artikel 98 hält die EU Kommission fest, dass die EBA, die EZB und alle Akteure des Zahlungsverkehrs, im Einklang mit entsprechender Interessensberücksichtigung und Einhaltung bereits genannter Ziele, die RTS ausarbeitet.

Die Ausnahmen unter welchen es zu keiner Anwendung von Artikel 97 kommt, stehen in Verbindung mit dem Risikoniveau, mit dem Betrag, mit der Regelmäßigkeit und dem Zahlungsweg eines Zahlungsvorganges. Die unter Artikel 97 und 98 erwähnten Punkte werden innerhalb des RTS von der EBA regelmäßig analysiert und überarbeitet, um den aktuellen Entwicklungen nachzukommen. (RL (EU) 2015/2366 ABl. L 337/106, 98)

Um Innovation nicht zu beeinflussen, entschied sich die EBA, die drei Kriterien der SCA, in der RTS auf hoher Ebene zu behandeln und nicht mit Beispielen oder Details den Entwicklungen vorzugreifen. Es wird grundsätzlich davon abgesehen, Verweise auf ISO- oder HTTPs-Standards innerhalb der RTS zu integrieren. Dennoch verweist die EBA auf die ISO20022, welche ein standardisiertes Nachrichtenformat vorgibt und damit die Kommunikation zwischen Zahlungsdienstleistern regelt. (Europäische Bankenaufsichtsbehörde, 2017a, S. 8)

3.1.2 Ausnahme von „low risk“ Transaktionen

Aus dem Feedback an die EBA geht hervor, dass innerhalb der RTS klare SCA Ausnahmeregelungen gefordert werden. Laut Angaben der EBA ist es schwierig objektive Ausnahmen, welche rechtlich akzeptabel und mit dem Gesetz abgestimmt sind, anzuführen. Ausnahmen, die eine Mehrheit von Transaktionen im Zahlungsverkehr von der SCA befreien, entsprechen nicht dem Ziel der PSD2, nämlich die Sicherheit zu erhöhen. Dennoch stimmt die EBA einer Ausnahme für Kleinbetragszahlungen zu und lässt diese in der Delegierte Verordnung (EU)

2018/389 unter Artikel 16 anführen. (DelVO (EU) 2018/389 ABl. L 69/32, 16) Weitere SCA-Ausnahmen werden im Kapitel 3.2.4 beschrieben. (Europäische Bankenaufsichtsbehörde, 2017a, S. 9)

3.1.3 Zugang zum Zahlungskonto

Innerhalb der RTS konzentriert sich der Zugang zum Zahlungskonto auf die Kommunikation zwischen den Zahlungsdienstleistern, den Kontoinformationsdiensten und den Zahlungsauslösediensten. Für die Kommunikation ist definiert, wie oft ein Kontoinformationsdienst Kontoinformationen anfordern darf. Nach Vorschlägen von zweimal täglich bis zu stündlich, beschloss die EBA eine maximal Anzahl von vier Anforderungen pro Tag. Zu beachten ist, dass diese Zugriffe aktiv und unter der Zustimmung von NutzerInnen erfolgen. Es kann jedoch zu Sondervereinbarungen zwischen den Parteien kommen. Erwähnt, jedoch nicht explizit berücksichtigt, sei in diesem Zusammenhang die Weiterentwicklung von Echtzeittransaktionen.

Die Aktualität von Informationen kann unter der Zugriffsbegrenzung leiden. Die Zahlungsauslösedienste und Kontoinformationsdienste fordern parallel alternative Zugriffsmöglichkeiten auf Zahlungsdaten zu den offiziellen Schnittstellen. Dies dient als Backup für nicht funktionierende Schnittstellen. Von der EBA wird das aus Gründen der SCA, der Identifizierung von zugreifenden Drittanbietern und der Protokollierung von Zugriffen untersagt. Zum Entgegenkommen der Forderung bestimmte die EBA, dass die offiziellen Schnittstellen der Zahlungsdienstleister eine gleiche Serviceleistung der Verfügbarkeit und gleiche Maßnahmen bei Problemen wie für ihre eigenen KundInnen vorweisen müssen. (Europäische Bankenaufsichtsbehörde, 2017a, S. 10 ff.)

3.2 Strong Customer Authentification

3.2.1 Funktionsweise von SCA

Sobald die SCA zur Anwendung kommt, wird aus zumindest zwei der drei Kriterien – „Wissen“, „Besitz“ und „Inhärenz“ – ein Code zur Authentifizierung generiert. Nach der Generierung eines Authentifizierungscodes und der einmaligen Verwendung durch den/die NutzerIn wird dieser vom Zahlungsdienstleister verworfen. Dadurch wird das Risiko von missbräuchlicher Verwendung reduziert. Für die Sicherheit des Authentifizierungscodes müssen die Zahlungsdienstleister sorgen. Das bedeutet, dass

- aus dem Authentifizierungscode keine Informationen ableitbar sind,
- auf Basis eines bereits generierten Authentifizierungscode kein neuer Authentifizierungscode generierbar ist und
- der Authentifizierungscode nicht fälschbar ist. (Europäische Bankenaufsichtsbehörde, 2017a, S. 20 f.)

Etwas vereinfacht bedeutet dies, dass mit dem Authentifizierungscode sichergestellt sein muss,

- dass keine Rückschlüsse auf Zahlungsbeträge und zahlungsauslösende Personen möglich sind,
- dass mit dem jeweiligen Authentifizierungscode nur einmalig eine Transaktion bestätigt werden kann,
- dass aus dem Authentifizierungscode nicht hervorgeht wie sich dieser zusammensetzt, sodass es Dritten nahezu unmöglich gemacht wird, diesen für eine neue Transaktion zu generieren.

In Abbildung 1 ist die Funktionalität eines SCA-Prozesses dargestellt. Im oberen Abschnitt ist die Freigabe mit dem Faktor „Wissen“, das Passwort und dem Faktor „Besitz“, die mobileTAN ersichtlich. Im unteren Abschnitt ist die Freigabe mit dem Faktor „Besitz“, die App und dem Faktor „Wissen“, die PIN oder dem Faktor „Inhärenz“, der Fingerabdruck oder der Gesichtsscan dargestellt.

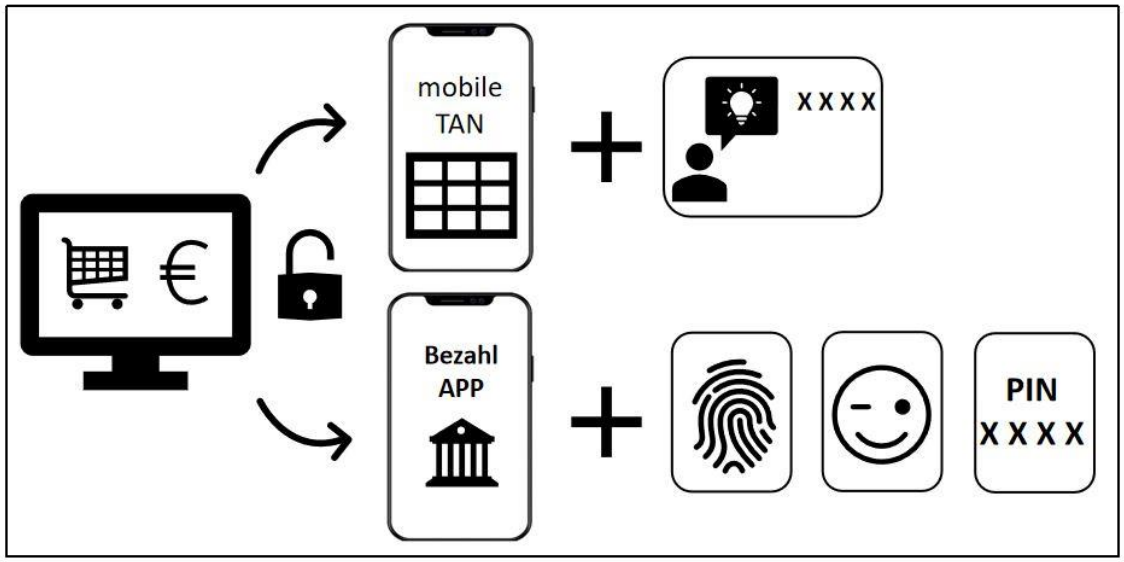


Abbildung 1: Darstellung eines SCA Prozesses (PayLife, o. J.)

3.2.2 Anforderungen an Zahlungsdienstleister während SCA

Die Zahlungsdienstleister müssen während der Durchführung einer SCA Anforderungen erfüllen, so dass

- während der Transaktion den NutzerInnen der Betrag und der/die ZahlungsempfängerIn zur Durchsicht mitgeteilt werden,
- der Authentifizierungscode nur für die Kombination von Betrag und ZahlungsempfängerIn, welchem zu Zahlungsbeginn zugestimmt wurde, Gültigkeit hat und
- eine Änderung des Betrags oder dem/der ZahlungsempfängerIn den Authentifizierungscode ungültig macht.

Die, im zweiten Aufzählungspunkt, erwähnte Kombination aus dem Authentifizierungscode, dem Betrag und dem/der ZahlungsempfängerIn wird auch „dynamische Verlinkung“ genannt. Diese Verlinkung sieht vor, dass eine bestehende Transaktion, in dieser verlinkten Kombination, nicht erneut durchgeführt werden kann. Durch diese Maßnahme können im Betrugsfall keine wiederholten Transaktionsversuche erfolgreich durchgeführt werden, wodurch die Betrugssicherheit erhöht wird. (Europäische Kommission, 2017)

Die Zahlungsdienstleister tragen die Verantwortung für die Vertraulichkeit, die Authentizität und Integrität der verwendeten und angezeigten Daten während des gesamten SCA Prozesses. Das betrifft insbesondere die Informationen über den Betrag und den/die ZahlungsempfängerIn. (Europäische Bankenaufsichtsbehörde, 2017a, S. 21)

Die genannten Begrifflichkeiten können unter dem Begriff Sicherheitsziele zusammengefasst werden.

- Die **Vertraulichkeit** stellt sicher, dass keinen unbefugten Personen und Systemen Informationen über Daten ausgehändigt werden.
- Die **Authentizität** beweist ob die Änderung oder Beauftragung einer Transaktion durch eine befugte Person oder ein befugtes System durchgeführt wird.
- Die **Integrität** ist nicht gegeben, wenn eine Transaktion während des Zahlungsprozesses manipuliert wird und sich dadurch etwas unscheinbar für Zahlungsauslösende ändert. (Gabriel, o. J.)

Eine Basis für die Einhaltung der Anforderung von Vertraulichkeit, Authentizität und Integrität bietet der Payment Card Industry Data Security Standard (PCI DSS). Der PCI DSS ist ein international einheitlicher Standard und richtet sich unter anderem an Finanzdienstleister, welche Zahlungsdaten verarbeiten, speichern und weitergeben. (PCI Security Standards Council, 2013, S. 7)

3.2.3 Definition der Kriterien Wissen, Besitz und Inhärenz

Bei den drei Kriterien, welche Bestandteile der SCA sind, ist zwischen Wissen, Besitz und Inhärenz zu unterscheiden. Die Anforderungen an die Zahlungsdienstleister und die NutzerInnen unterscheiden sich. Die Anforderungen in Tabelle 1 bilden Zusammenhänge zwischen den Kriterien und dem Zahlungsdienstleister sowie den NutzerInnen. (Europäische Bankenaufsichtsbehörde, 2017a, S. 21 f.)

Kriterium	**Zahlungsdienstleister**	**NutzerInnen**
Wissen	Die Zahlungsdienstleister tragen die Verantwortung Maßnahmen zu treffen, welche verhindern, dass Kriterien, die als Wissen eingestuft sind, von Dritten offengelegt werden können.	Die NutzerInnen tragen die Verantwortung für Maßnahmen, welche verhindern, dass das Kriterium Wissen an Dritte weitergegeben wird.
Besitz	Die Zahlungsdienstleister haben Sorge zu tragen, dass das Element Besitz nicht von Dritten für die Kundenauthentifizierung eingesetzt wird.	Die NutzerInnen müssen verhindern, dass Dritte das Element Besitz zur Verwendung nachahmen können.
Inhärenz	Die Zahlungsdienstleister müssen das Risiko gering halten, dass Zugangsgeräte und -software für die Authentifizierung von Dritten fälschlich verwendet werden können. Zusätzlich muss die Wahrscheinlichkeit, dass Dritte Personen als korrekte NutzerInnen erkannt werden, gering sein.	Die NutzerInnen haben entsprechende Maßnahmen zu gewährleisten, dass Dritte keine unbefugte Verwendung für die Zugangsgeräte und -software erhalten können.

Tabelle 1: Sicherheitsbedingungen für die Kriterien Wissen, Besitz und Inhärenz

Für die Umsetzung der in Tabelle 1 definierten Kriterien gibt es von der EBA vorgeschlagene Elemente zur Implementierung für Zahlungsdienstleister. In folgender Tabelle 2 sind Beispiele für jedes der drei Kriterien ersichtlich. Die Kombination aus zwei der drei Kategorien mit jeweils einem Element bildet die SCA. Ausnahmedefinitionen gibt es bei „Wissen" und „Besitz". Ein generiertes Einmalpasswort oder ein Benutzername wird im SCA Prozess nicht zum Element „Wissen", sondern zum „Besitz" gezählt. Eine Installation einer App ist im SCA Prozess noch nicht als Kriterium „Besitz" gültig. Das Wort „selbstgewählt" gibt Auskunft über die Definition von „Wissen" sowie die „Verknüpfung", z.B. eine App mit dem Smartphone, den „Besitz" definiert. Es gilt zu beachten, dass die Vorschläge der Kriterien auf aktuelle Marktgegebenheiten zurückzuführen und nicht statisch zu sehen, sondern dynamisch weiterentwickelbar sind. (Europäische Bankenaufsichtsbehörde, 2019a, S. 5 ff.)

Kriterium	**Vorschlag der Elemente der EBA**
Wissen	• selbstgewähltes Passwort • selbstgewählte PIN • Sicherheitsfragen
Besitz	• Einmalpasswort per SMS • Einmalpasswort per Token[1] generiert • QR Code[2] welcher durch ein anderes Gerät gescannt werden kann • Verbindung einer App mit einem Device

[1] Der Token ist ein Gerät – oft in der Form eines Schlüsselanhängers – welches in regelmäßigen Abständen einen Code erzeugt. Dieser wird Token-Code genannt und kann z.B. bei einem Login oder einer Transaktion als zweiter Faktor dienen. (Reitbauer, o. J.)

[2] Der QR Code steht für „quick response" code, zu Deutsch „schnelle Antwort" und ist eine 2D Grafik, welche von Devices abgescannt werden kann, um z.B. einen Link auf eine Website herzustellen oder zwei Devices miteinander zu verknüpfen. (Bendel, o. J.)

Kriterium	Vorschlag der Elemente der EBA
Inhärenz	• Fingerprint • Stimmerkennung • Venenerkennung • Gesichtserkennung • Iris Scan

Tabelle 2: Beispiele zu den Elementen der SCA

3.2.4 Ausnahmen der SCA

Zahlungsdienstleister haben die Möglichkeit Transaktionen, welche in der Übergangszeit bis zum 31.12.2020 durchgeführt werden, nicht mit der SCA abzuwickeln. Nach dem 31.12.2020 kann SCA nur entsprechend der definierten Ausnahmen entfallen. (Europäische Bankenaufsichtsbehörde, 2017a, S. 7)

In Tabelle 3 werden die Ausnahmen aus der Delegierte Verordnung (EU) 2018/389 aufgelistet und mit einer Kurzbeschreibung jeweils erläutert. Es ist zu erwähnen, dass die Ausnahmen Regelwerke sind, welche innerhalb des Rahmens verschieden von den Zahlungsdienstleistern angewendet werden können. Es besteht die Möglichkeit auf Ausnahmen zu verzichten und SCA in jedem Zahlungsvorgang zu verlangen. (viveum, o. J.)

Ausnahme	Kurzbeschreibung
Artikel 10 – Zahlungskonto-informationen	Von einer SCA kann abgesehen werden, wenn beim Zugriff auf Zahlungskontoinformationen keine sensiblen Daten offen ersichtlich werden und dieser Zugriff mehrfach innerhalb von 90 Tagen erfolgt. Beim ersten Zugriff auf die Zahlungskontoinformationen, sowie ein verstreichen von mehr als 90 Tagen ohne SCA, muss SCA einmalig verlangt werden.

Ausnahme	Kurzbeschreibung
Artikel 11 – Kontaktlos-transaktionen	Bei eine Kontaktlostransaktion, unter der Verwendung der Near Field Communication (NFC), kann auf SCA verzichtet werden, • wenn der Zahlungsbetrag nicht höher als € 50 ist, • wenn der kumulierte Zahlungsbetrag der letzten Transaktionen seit der letzten SCA nicht höher als € 150 ist und • wenn die Anzahl der zuletzt durchgeführten Transaktionen seit der letzten SCA nicht größer als fünf ist. In allen anderen Fällen ist SCA anzuwenden und die Zahlungsdienstleister haben die Möglichkeit die Limits nach unten zu setzen. Ebenso können diese Limits im Praxiseinsatz des EU Raums variieren. Bei der Durchführung von SCA werden die Limits zurückgesetzt.
Artikel 12 – Modular Terminals	Auf SCA darf bei unbeaufsichtigten Automaten zum Entrichten von Maut- oder Parkgebühr verzichtet werden.
Artikel 13 – Vertrauen in EmpfängerIn	Es gibt die Möglichkeit des Führens von Listen, auf jenen ZahlungsempfängerInnen das Vertrauen von ZahlungsauslöserInnen gegeben werden kann – auch „White List“ genannt. Für die Erstellung oder Änderung einer solchen Liste ist SCA anzuwenden. Dies funktioniert, indem Zahlungsdienstleister ausgewählte HändlerInnen, welchen vertraut werden kann, definieren. Zahlungsauslösende können im Rahmen einer E-Commerce Transaktion im Zuge der SCA diese HändlerInnen auf eine sogenannte „White List“ setzen. Folglich werden die Zahlungsauslösenden bei weiteren

Ausnahme	Kurzbeschreibung
	Transaktionen zu diesen HändlerInnen nicht mehr zu einer SCA aufgefordert.
Artikel 14 – Wiederholende Zahlungen	Bei der Erstellung einer Serie von Transaktionen mit selbigem Betrag und selbigem/r EmpfängerIn ist SCA anzuwenden. Für gleichbleibende folgende Transaktionen darf auf SCA verzichtet werden.
Artikel 15 – Überweisung zwischen Konten bei welchen AuslöserIn und EmpfängerIn selbe Personen sind	Wenn die Zahlungskonten von selbigem Zahlungsdienstleister geführt werden und der/die AuslöserIn sowie der/die EmpfängerIn dieselbe Person ist, muss keine SCA ausgeführt werden.
Artikel 16 – Kleinbetrags-zahlungen	In ähnlicher Form zu Artikel 11 gibt es in Artikel 16 Limits, bei welchen kein SCA angewendet werden muss. Der Bezug besteht jedoch zu elektronischen Fernzahlungen und nicht zu Zahlungen bei welchen die AuslöserInnen am Zahlungsort anwesend sind. SCA ist ausgenommen, wenn • der Betrag nicht größer als € 30 ist, • der kumulierte Betrag nicht größer als € 100 ist und • die Anzahl der aufeinanderfolgenden Transaktionen nicht größer als fünf ist. Es gilt, dass diese Limits von Zahlungsdienstleistern nach unten gesetzt werden können. Ebenso können diese Limits im Praxiseinsatz des EU Raums variieren. Wird SCA angewendet, werden die Limits zurückgesetzt.

Ausnahme	Kurzbeschreibung
Artikel 17 – automatische Zahlungsprozesse zwischen Unternehmen	Zwischen Unternehmen kann auf SCA verzichtet werden, wenn ein Zahlungsvorgang über spezielle Prozesse oder Protokolle ausgelöst wird und keine EndverbraucherInnen involviert sind.
Artikel 18 – Transaktions-risikoanalyse	Es gibt Möglichkeiten einer Risikoanalyse durch die Zahlungsdienstleister, womit auf SCA verzichtet werden kann, wenn das Risiko der Transaktion als niedrig eingestuft wird. Dazu gibt es einzuhaltende Schwellwerte beim Zahlungsbetrag, vergleiche von Betrugsraten und Echtzeitanalysen, die allesamt in die Beurteilung einfließen. Innerhalb der Echtzeitanalyse werden Verhaltensmuster, ungewöhnliche Softwareverwendung, ungewöhnliche Verhalten im Authentifizierungsprozess und ungewöhnliche oder mit hohem Risiko belastete Orte der ZahlerInnen überprüft. Transaktionen können bei einer Betrugsrate bis zu 0,005% (innerhalb des Instituts) bis zu € 500 ohne der Anforderung einer SCA abgewickelt werden. Bei niedrigeren Schwellwerten steigt die zugelassene prozentuelle Betrugsrate.

Tabelle 3: Ausnahmen vom SCA Prozess (DelVO (EU) 2018/389 ABl. L 69/31, 10-18)

Lastschriftverfahren, welche über den/die ZahlungsempfängerIn veranlasst werden, sind aus dem Artikel 97 der Richtlinie (EU) 2015/2366 von der SCA ausgenommen, wenn eine Zustimmung der/des Zahlungsauslösenden mittels Mandat zum Lastschriftverfahren, unter der Berücksichtigung des Zahlungsdienstleisters, besteht. Es heißt in diesem Artikel jedoch, dass SCA grundsätzlich anzuwenden ist, wenn das Risiko zum Betrug oder Missbrauch vorhanden ist. (Europäische Bankenaufsichtsbehörde, 2017a, S. 7 f.; RL (EU) 2015/2366 ABl. L 337/106, 97)

Für grenzüberschreitende Transaktionen, bei welchen Nationalitäten involviert ohne einer rechtlichen Anforderung der SCA sind, gibt es keine klare Regelung. Die Zahlungsdienstleister werden jedoch dazu angehalten, notwendige Vorkehrungen zu leisten, die für eine korrekte Verwendung im Zahlungsverkehr sorgen. (Europäische Bankenaufsichtsbehörde, 2017a, S. 8)

Innerhalb der PSD2 wird der Ausdruck „Restricted Network“, was so viel bedeutet wie „bezahlen in einem geschlossenen Netzwerk“, genannt. Dies findet in der PSD2 Ausnahmen. Jene Zahlungsdienstleister, die ein Produkt innerhalb eines Netzwerks anbieten können, müssen SCA nicht anwenden. Wenn das monatsdurchschnittliche Transaktionsvolumen größer als € 1 Million ist, benötigen sie eine Genehmigung bei einer zuständigen Aufsichtsbehörde,. (Fletzberger, 2018) Der Grund für diese Sonderregelung ist, dass Zahlungskarten, welche auf einen Raum begrenzt sind nicht als Zahlungsdienst gelten. Ein Beispiel für solche Produkte sind Gutscheinkarten, die nur in einer Shopping Malls akzeptiert werden. (Walz, n.d.)

3.3 Open Banking

Einleitend ist es wichtig zu sagen, dass im folgenden Abschnitt erwähnte Anforderungen nicht für Sparkonten gültig sind. Sparkonten sind Kontoformen, welche von Zahlungsdienstleistern angeboten werden und sich immer auf ein Girokonto referenzieren. Diese Sparkonten ermöglichen keine Transaktionen auf andere Konten als das definierte Referenzkonto. Entsprechend der Richtlinie (EU) 2015/2366 sind Sparkonten daher von den Regelungen ausgenommen. (RL (EU) 2015/2366 ABl. L 337/57, 4, Abs. 5)

Zusätzlich zu den geregelten Maßnahmen der SCA werden innerhalb der RTS die Vorschriften für Open Banking definiert. In Österreich wird dafür auf einen gemeinsamen Standard gesetzt. Die Berlin Group bietet eine Schnittstellenbeschreibung, unter Rücksichtnahme auf den österreichischen Markt, an. Die Umsetzung gemäß dem Standard der Berlin Group ermöglicht die Bereitstellung einer API, die sich im europäischen Raum einsetzen lässt. Die Berlin

Group hat die Beschreibung der Schnittstellenimplementierung, unter der Gründung von Arbeitsgruppen im europäischen Bereich, erstellt und folgend eine Basis für die PSD2 Konformität bereitgestellt. (STUZZA, o. J.)

Die Berlin Group ist eine Initiative, welche im Jahr 2004 in Berlin entstanden ist. Daraus resultiert der Name Berlin Group. Das Hauptziel dieser Initiative ist die europaweite Entwicklung von Standards für technischen und organisatorischen Anforderungen im Finanzmarkt. Die Organisation formte sich vor allem durch die gemeinsame Vision einen europäischen Zahlungsraum zu schaffen. Die Berlin Group setzt sich aus 26 Stakeholdern aus der Zahlungsverkehr Branche zusammen. Diese verteilen sich auf zehn Länder innerhalb der Eurozone und weitere elf Länder außerhalb wie z.B. Russland, Schweiz, Großbritannien, Schweden und Dänemark, um einige zu erwähnen. Unter diesen Stakeholdern befindet sich die PSA Payment Services Austria GmbH, um den einzigen österreichischen Zahlungsdienstleister zu nennen. Des Weiteren ist, um einzelne bekannte Unternehmen zu erwähne, die UniCredit Group, die VISA, die Mastercard Europe und die Worldline an der Initiative beteiligt. Es gilt hervorzuheben, dass die Initiative sich nicht mit der Festlegung von Lösungen befasst, sondern lediglich Empfehlungen ausspricht. Ob die Stakeholder im Zahlungsverkehr diese annehmen, bleibt ihnen überlassen. Durch die namhaften Stakeholder der Berlin Group sind diese befähigt Vorschläge im Zahlungsverkehr zu platzieren. (Berlin Group, o. J.)

Die Möglichkeiten Open Banking als NutzerIn zu verwenden ist durch die Entwicklung der Zahlungsauslösedienste und Kontoinformationsdienste möglich geworden. Individuelle Frontend Anwendungen werden dadurch entwickelt. Das bedeutet auch, dass die Entwicklung den Ansprüchen der NutzerInnen angepasst werden und das Denken auf Produktebene je Dienstleister der Vergangenheit angehört, da die Dienstleistungen der Zahlungsdienstleister nach Wunsch kombinierbar sind. Ausgehend von einer Applikation A eines Drittanbieters besteht die Möglichkeit benutzerdefinierte Services anzuzeigen. Dies können durch mehr oder weniger angesprochene Schnittstellen die Übersicht über Bankkonten, die

Verwaltung von Kreditkarten, die Durchführung von Transaktionen, die Verwaltung der Zahlungsdienste, das Finanzmanagement von Investments und vieles mehr innerhalb einer Applikation A sein. (MoneyToday, o. J.)

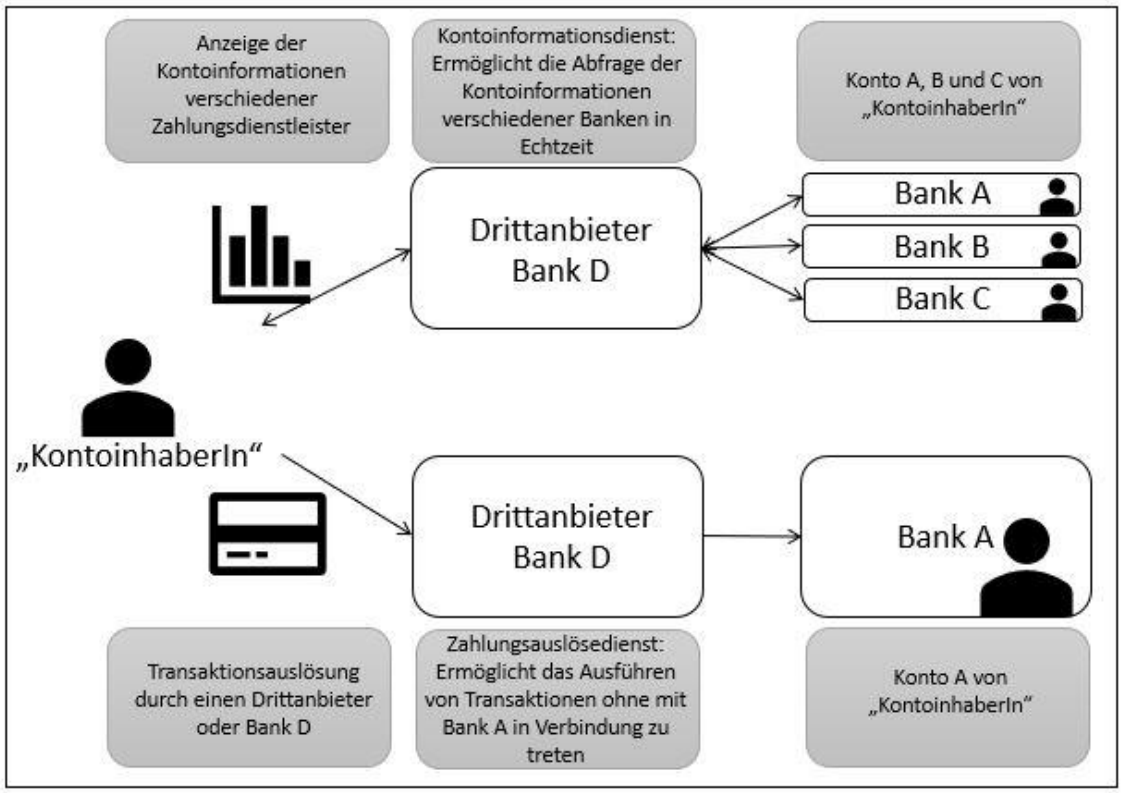


Abbildung 2: Zahlungsauslöse- und Kontoinformationsdienstleister (PISP und AISP)

In der Abbildung 2 ist in der oberen Bildhälfte der Prozess eines Kontoinformationsdienstes (AISP) und in der unteren Bildhälfte der Prozess eines Zahlungsauslösedienstes abgebildet (PISP). Wie in der Richtlinie (EU) 2015/2366 festgehalten, sind Kontoinformationsdienste entstanden, um den KundInnen in Echtzeit einen Überblick über ihre Finanzen zu geben. In der Abbildung 2 ist dargestellt, wie KundInnen über einen ausgewählten Kontoinformationsdienst, das kann ein Zahlungsdienstleister oder ein Drittanbieter sein, auf alle weiteren in Besitz befindlichen Zahlungskonten zugreifen können. Ebenso können diese bei einer Online Bestellung über einen Zahlungsauslösedienst dem/der ZahlungsempfängerIn bestätigen, dass eine Transaktion getätigt wurde. Der/die

ZahlungsempfängerIn kann umgehend die Bestellung weiterbearbeiten. Die Zahlungsabwicklung wird vom Zahlungsauslösedienst über API Schnittstellen durchgeführt. Für beide Prozesse muss der/die ZahlungskontoinhaberIn ausdrücklich den Zugriff auf das Zahlungskonto erlauben. In der Richtlinie (EU) 2007/64/EG waren diese Prozesse und dahinterstehende Drittanbieter nicht berücksichtigt und unterlagen daher keiner klar geregelten behördlichen Aufsicht. (RL (EU) 2015/2366 ABl. L 337/39, 28-29)

Open Banking hat einen Mehrwert, wenn die Zahlungsservice NutzerInnen einem Drittanbieter (Zahlungsauslösedienst oder Kontoinformationsdienst) Zugriff auf deren Zahlungskonto geben. Dabei ist zu beachten, dass nur Drittanbieter, die lizenziert sind diesen Zugriff auf die Zahlungskonten von NutzerInnen bekommen können. Zusätzlich müssen die NutzerInnen eine Einwilligung für den Zugriff von Drittanbietern auf deren Zahlungskonto erteilen. Damit Drittanbieter eine Transaktion durchführen und in Kontoinformationen einsehen dürfen, müssen diese sich gegenüber der Zahlungsdienstleister authentifizieren. Nach erfolgreicher Authentifizierung können die Services ausgeführt werden. (bawaggroup, 2019a)

Für die Auslösung einer Zahlung nutzen die Zahlungsauslösedienste die Sicherheitsmerkmale der ZahlungskontoinhaberInnen. Es ist zu beachten, dass bei nicht zugestimmten Zahlungsvorgängen umgehend der ursprüngliche Status, z.B. eine Rückerstattung des Betrages, wieder herzustellen ist. Werden nicht autorisierte Transaktionen nicht beim zuständigen Zahlungsdienstleister gemeldet und betrügerische Absicht nachgewiesen, kann der/die ZahlungsdienstnutzerIn bis zu einem Maximalbetrag von € 50 haftbar gemacht werden. Zum Schutz der ZahlungsdienstnutzerInnen liegt die Beweislast für betrügerische Absichten beim Zahlungsdienstleister. (RL (EU) 2015/2366 ABl. L 337/46, 71-72) Sobald eine Transaktion durch Zahlungsauslösedienste abgeschlossen wird, müssen die ZahlungsdienstnutzerInnen, sowohl die EmpfängerInnen als auch AuslöserInnen von ihren Zahlungsdienstleistern über den Abschluss informiert werden. Dabei kann der Betrag und der Transaktionszeitpunkt geprüft werden. (RL (EU) 2015/2366 ABl.

L 337/83, 48-49) Um eine schnelle Zahlungsabwicklung zu ermöglich, müssen kontoführende Zahlungsdienstleister in Echtzeit bestätigen, ob ein autorisierter Betrag auf dem Konto der/des Zahlungsauslösenden zur Verfügung steht. Dies sichert eine umgehende Weiterbearbeitung z.B. einer Bestellung in einem online Shop. (RL (EU) 2015/2366 ABl. L 337/91, 65)

In der Richtline (EU) 2015/2366 wird festgehalten, dass Zahlungsauslösedienste zu keiner Zeit eines Transaktionsprozesses Geldbeträge besitzen dürfen. Des Weiteren dürfen Zahlungsauslösedienste sensible Daten nur speichern und nur Daten anfordern, wenn diese für die Transaktion selbst relevant sind. Die Zahlungsauslösedienste dürfen erhaltene Daten nur für die Durchführung der Transaktion verwenden. (RL (EU) 2015/2366 ABl. L 337/92, 66) Ebenso wie Zahlungsauslösedienste dürfen auch Kontoinformationsdienste nur auf Informationen und sensible Daten zugreifen, welche mit Zahlungsvorgängen in Zusammenhang stehen. Die Sicherstellung, dass Sicherheitsmerkmale der NutzerInnen nicht an Dritte gelangen, obliegt den Kontoinformationsdiensten. Für Kontoinformationsdienste, Zahlungsauslösedienste und die kontoführenden Zahlungsdienstleister gilt eine Sicherstellung von sicheren Kommunikationskanälen zu gewährleisten. (RL (EU) 2015/2366 ABl. L 337/93, 67)

Für die Erhöhung der Sicherheit können NutzerInnen mit den Zahlungsdienstleistern Obergrenzen für Transaktionen vereinbaren. Die Zahlungsdienstleister haben das Recht das Service zu sperren, wenn ein Verdacht besteht, dass die Sicherheit gefährdet ist, betrügerische Absichten vorliegen oder der Verdacht besteht, dass die NutzerInnen einer Zahlungsschuld nicht nachkommen können. Des Weiteren kann der kontoführende Zahlungsdienstleister immer den Zugang für einen Kontoinformations- oder Zahlungsauslösedienst verweigern, wenn verdächtige Autorisierungen oder betrügerischer Verdacht zum Zugang auf das Zahlungskonto besteht. Wird aus genannten Gründen ein Zugang verweigert, muss der Vorfall an die Behörden gemeldet werden. (RL (EU) 2015/2366 ABl. L 337/94, 68) Wie bereits bei der Haftung von Transaktionen erwähnt, liegt auch der Nachweis

von einer korrekten Authentifizierung eines Zahlungsvorgangs beim Zahlungsauslösedienst und nicht bei den VerbraucherInnen. (RL (EU) 2015/2366 ABl. L 337/95, 72) Wenn Zahlungsdienstleister keine SCA anfordern, müssen Schäden an VerbraucherInnen rückerstattet werden. Des Weiteren muss auch der Schaden vom Zahlungsauslöse- oder Kontoinformationsdienst an den kontoführenden Zahlungsdienstleister rückerstattet werden. (RL (EU) 2015/2366 ABl. L 337/96, 74) In der Delegierten Verordnung wird festgehalten, dass die Zahlungsdienstleister bei elektronischen Zahlungsdiensten (z.B. mobile Payment) die Verantwortung tragen, dass Risiken in der Kommunikation zwischen den Geräten minimiert werden. (DelVO (EU) 2018/389 ABl. L 69/36, 28) Im Zuge der Kommunikation muss durch die Zahlungsdienstleister sichergestellt werden, dass zu jedem Zeitpunkt, während des Prozesses einer Transaktion, die Ereignisse rückverfolgt werden können. Für die Sicherheit müssen während der Transaktion eine Transaktionsnummer, die Zeitangaben und weitere Transaktionsdaten protokolliert werden. (DelVO (EU) 2018/389 ABl. L 69/37, 29)

3.4 Darstellungen von SCA und Open Banking

In folgenden Abschnitten sind zur besseren Vorstellung marktübliche Varianten zur SCA und Open Banking dargestellt. Aus Gründen der Verfügbarkeit für die Darstellung der Szenarien wurden die Erste Group Bank, die BAWAG P.S.K, die N26 und die Raiffeisenbank der in Österreich vertretenen Zahlungsdienstleister gewählt.

3.4.1 Login über die Web-Oberfläche bei George der Erste Group Bank

In Abbildung 3 ist der PSD2 konforme Login in George, das online Banking Portal der Erste Group Bank, ersichtlich. Die Lösung der Erste Group Bank ist eine eigene App, die s Identity-App, die zur Authentifizierung beim Login dient. Nach erfolgreicher Eingabe der Verfügernummer in der Web-Oberfläche zeigt das mit der App verknüpfte Smartphone – der „Besitz" – per push-Nachricht eine Aktion an. Nach dem Einstieg in die s Identity-App mittels Zugangscode oder Biometrie – das „Wissen" oder die „Inhärenz" – können Aktionen freigegeben werden. Dabei ist die angezeigte vierstellige Prüfziffer in der Web-Oberfläche sowie in der s Identity-App zu überprüfen und anschließend freizugeben.

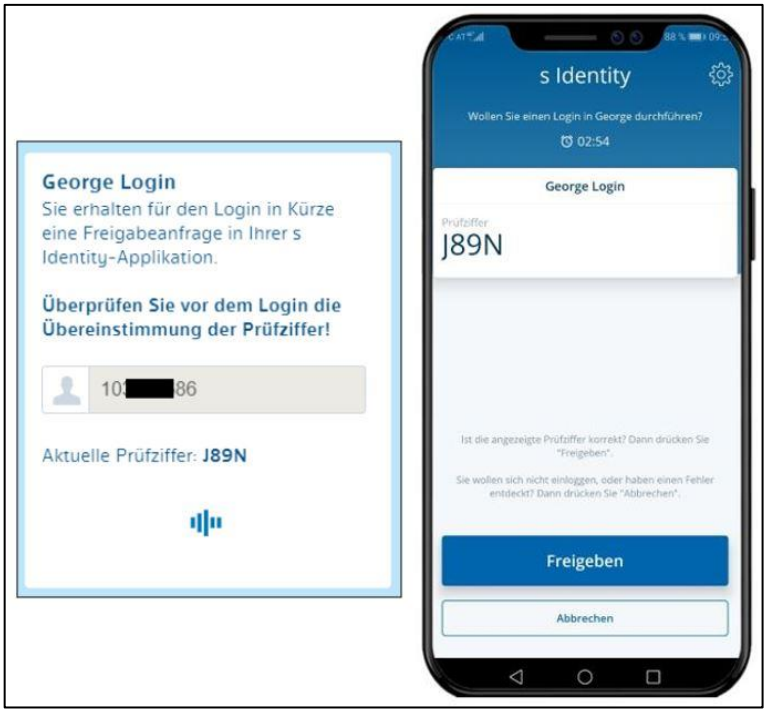


Abbildung 3: Freigabe des Logins in George mittels s Identity-App

3.4.2 Login über die George App der Erste Group Bank

Der Einstieg in die George App funktioniert ohne der s Identity-App. In dieser Lösung wird die George App bei der Installation mit dem Smartphone gekoppelt – der „Besitz“ – und mittels Biometrie oder Zugangscode – die „Inhärenz“ oder das „Wissen“ – kann auf den Account zugegriffen werden. Der Einstieg anhand von Biometrie ist in Abbildung 4 im linken Bild zu sehen. Der Einstieg funktioniert wie soeben beschrieben ähnlich zur eBanking App der BAWAG P.S.K, der N26-App und der Raiffeisenbank Elba-App.

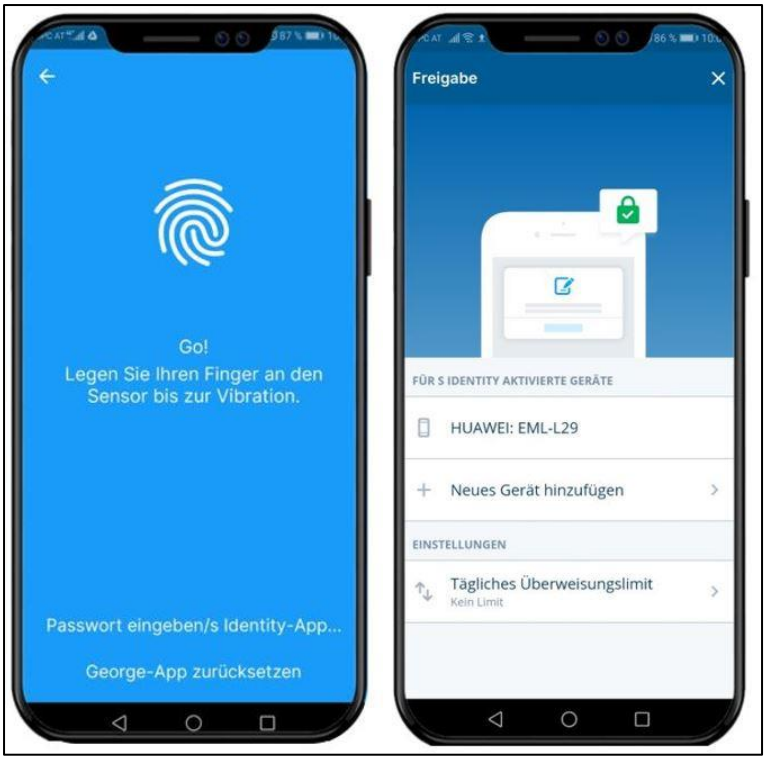


Abbildung 4: Einstieg in die George App anhand von Biometrie und der Hinweis auf die Verknüpfung

In Abbildung 4 im rechten Bild ist die Verknüpfung zwischen der App und dem Device ersichtlich. Damit wird sichergestellt, dass BenutzerInnen in Besitz des mit der App verknüpften Device sein müssen, um weitere Aktionen tätigen zu können. Im rechten Bild ist die App mit einem Device – einem Huawei: EML-L29 –

verknüpft. Folgend auf die Login Verfahren sind in den weiteren Kapiteln verschiedene Lösungsansätze verschiedener Banken im österreichischen Raum für die Authentifizierung von Transaktionen dargestellt und beschrieben.

3.4.3 Transaktion über die Web-Oberfläche von Georg der Erste Group Bank

In folgenden Abschnitten sind die Transaktionsabläufe der verschiedenen Zahlungsdienstleister abgebildet und beschrieben. Im folgenden Szenario wird die Zahlungsfreigabe einer Transaktion in der Web-Oberfläche der Erste Group Bank dargestellt. Im Zahlungsauftrag in Abbildung 5 bzw. der zu kontrollierenden Übersicht in Abbildung 6, sind der/die AuftraggeberIn sowie der/die ZahlungsempfängerIn, der Betrag und der Verwendungszweck abgebildet. Bei der Kombination von dem/der ZahlungsempfängerIn und dem Betrag, die von dem/der ZahlungsauslöserIn akzeptiert und einmalig freigegeben wird, wird die dynamische Verlinkung angewendet. Eine Änderung des Betrages oder ein Abbruch würde die Kombination für diese Freigabe ungültig machen und fordert eine neuerliche Authentifizierung mit einem neu generierten Authentifizierungscode.

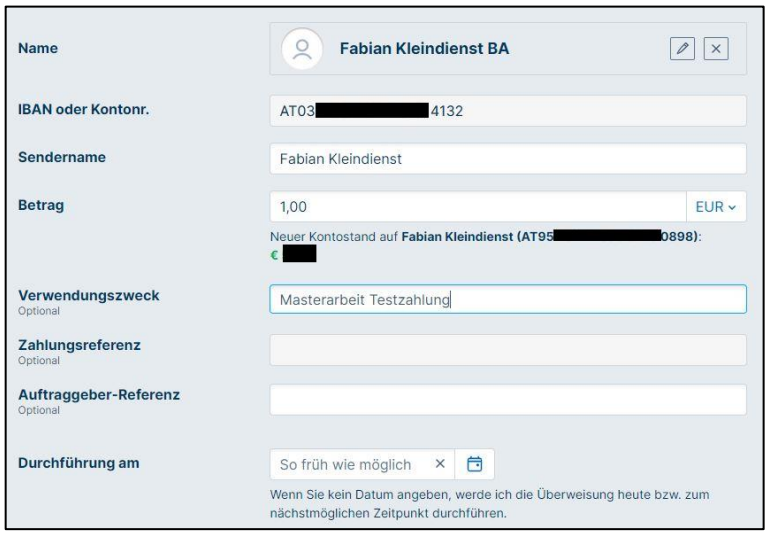


Abbildung 5: Zahlungsauftrag in George

Abbildung 6: Zahlungsübersicht in George

Der Authentifizierungscode wird durch die Verwendung der s Identity-App in Verknüpfung des Smartphones – der „Besitz“ – und die Freigabe durch die Authentifizierung mittels Biometrie – die „Inhärenz“ – gebildet. Diese Freigabe ist in Abbildung 7 zum Abschluss der Transaktion dargestellt.

Abbildung 7: Zahlungsfreigabe in der s Identity-App

3.4.4 Transaktion über die George App der Erste Group Bank

Um die zwei Lösungswege der Erste Group Bank abzuschließen, folgt die Darstellung einer Transaktion mit der George App. Für beide dieser Anwendungen besteht die Notwendigkeit eines Android oder iOS fähigen Gerätes.

Nach der Überprüfung und Freigabe der Transaktion öffnet sich wie in Abbildung 8 ersichtlich automatisch die s Identity-App zur bevorstehenden Freigabe. Für KundInnen ist der Wechsel zwischen den Apps nicht mit einem zusätzlichen Klick verbunden und damit nicht offensichtlich.

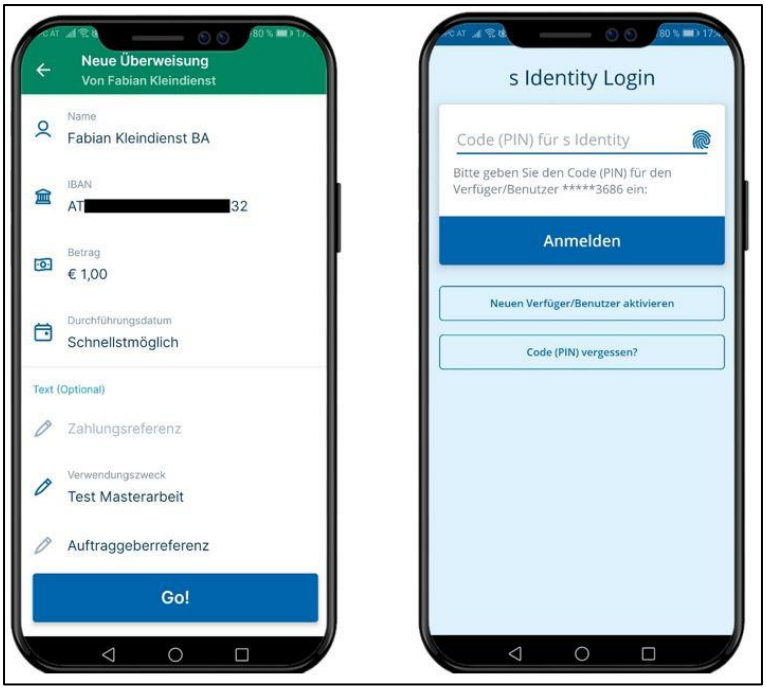


Abbildung 8: Zahlungsauftrag in der George App und Anmeldung in der s Identity-App

Die endgültige Freigabe erfolgt ident wie bereits im Szenario aus der Web-Oberfläche mit der s Identity-App (wie in Abbildung 9 ersichtlich).

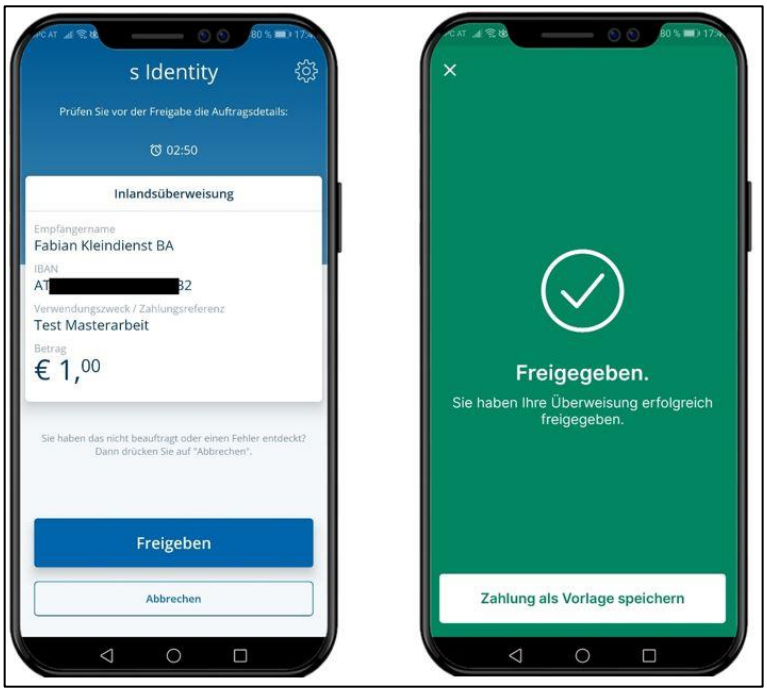


Abbildung 9: Zahlungsfreigabe in der s Identity-App und Abschluss

Alternativen zur Freigabe mit der s Identity-App über das Smartphone sind

- die Installation der s Identity Desktopversion für Windows und OS
- oder die Verwendung eines cardTAN-Generators.

Die s Identity Desktopversion kann kostenlos installiert werden, und der cardTAN-Generator kann kostenlos über die Erste Group Bank bestellt werden. Funktional entsprechen beide Alternativen der PSD2. (Sparkasse Bank AG, o. J.)

3.4.5 Transaktion über die eBanking Web-Oberfläche der BAWAG P.S.K

Im Unterschied zu den erwähnten Lösungen der Erste Group Bank besteht bei der BAWAG P.S.K die Auswahl aus einer Authentifizierung mittels mobileTAN (mTAN) sowie einer secTAN. Für die Verwendung der secTAN wird, ähnlich wie bei der Erste Group Bank, eine separate Security App zur Zahlungsfreigabe benötigt. Diese App findet Anwendung, wenn ausgehend von dem eBanking eine Transaktion veranlasst wird. Anstatt einer Übertragung einer mobileTAN als SMS wird eine fünfstellige TAN durch die secTAN App generiert und muss in das eBanking Portal übertragen werden.

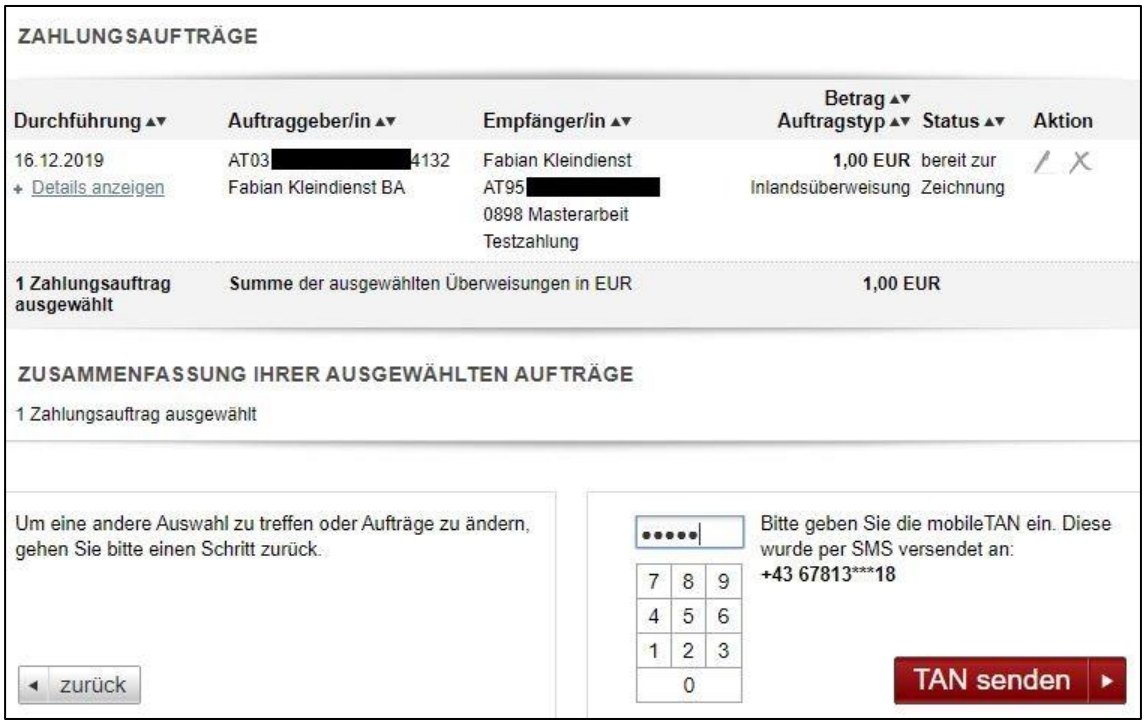


Abbildung 10: Zahlungsübersicht und -freigabe mit einem mobile TAN

In Abbildung 10 ist die Übersicht für die Zahlungsfreigabe sowie die Eingabemöglichkeit der mobileTAN ersichtlich. Abbildung 11 zeigt die Nachvollziehbarkeit der mobileTAN, welche per SMS versendet wurde. Die fünfstellige TAN „41805“ in der SMS ist jene Zahlenkombination, die im eBanking

Portal zur Authentifizierung eingegeben werden muss. Sowohl die Generierung der TAN in der Security App, als auch der Erhalt als mobileTAN mit einer SMS ist als Kriterium „Besitz“ gültig. Bei der mobileTAN ist zu berücksichtigen, dass nicht die TAN sondern die SIM-Karte den „Besitz“ darstellt. Das zweite Kriterium, um die SCA zu erfüllen, wird beim eBanking Login mit einem Passwort – das „Wissen“ – bereits abgefragt. So könnte der Account gehackt, eine Transaktion jedoch erst mit dem Besitz der zugehörigen SIM-Karte oder der verknüpften secTAN App ausgelöst werden.

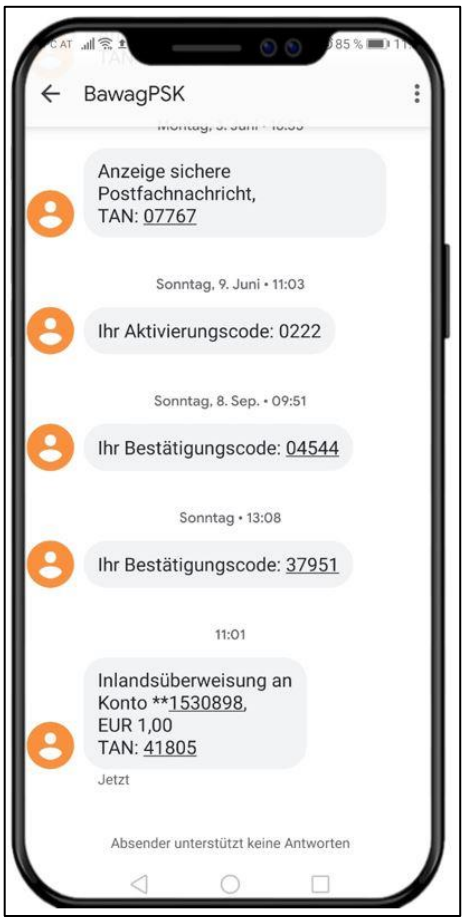


Abbildung 11: mobile TAN

3.4.6 Transaktion über die eBanking App der BAWAG P.S.K

Anders, ohne secTAN App und ohne mobileTAN, funktioniert die Zahlungsfreigabe mit der eBanking App. In der Abbildung 12 ist im linken Bild die letzte Kontrollmöglichkeit, bevor die Transaktion endgültig freigegeben wird, ersichtlich. Inhaltlich befinden sich dieselben Informationen wie bei den bereits genannten Beispielen in dieser Übersicht.

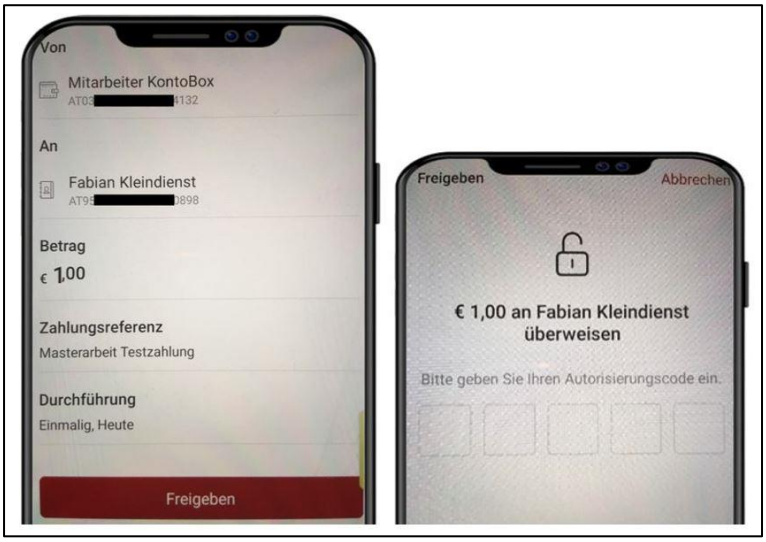


Abbildung 12: Transaktionsübersicht und -kontrolle sowie Freigabe mit dem Autorisierungscode

Im Schritt zur Freigabe erfolgt der Aufruf zur Eingabe eines selbst definierten fünfstelligen Autorisierungscodes (Abbildung 12, rechtes Bild). Mit der Kombination aus der Verknüpfung der App mit dem Smartphone – der „Besitz" – und dem Autorisierungscode – das „Wissen" – werden die Vorgaben für die SCA erfüllt. Diese Variante hat den Vorteil, dass die gesamte Transaktion innerhalb einer App abgewickelt werden kann.

3.4.7 Transaktion über die N26 App

Die N26 Bank unterscheidet sich in der Nutzung von der Web-Oberfläche minimal zur Erste Group Bank. Um die Sicherheit zu erhöhen, wird die Eingabe eines Verfügers, eines Passwortes und die Freigabe des Zugriffes in der, mit einem Smartphone verknüpften, App verlangt.

In der Abbildung 13 ist von links nach rechts die Transaktion mit der N26 App dargestellt. Durch die Verknüpfung der App mit einem Smartphone, das Öffnen der App mit einem persönlichen Passwort oder dem Fingerabdruck und die Bestätigung der Transaktion mit dem selbst definierten Bestätigungs-PIN wird eine Transaktion abgewickelt. Ein Vorteil gegenüber anderer Lösungen ist, dass die Freigabe zum Login und die Authentifizierung zur Freigabe einer Transaktion innerhalb einer App abgewickelt wird. Des Weiteren sind in diesem Testbeispiel 3 Kriterien bis zur Zahlungsfreigabe zu erfüllen.

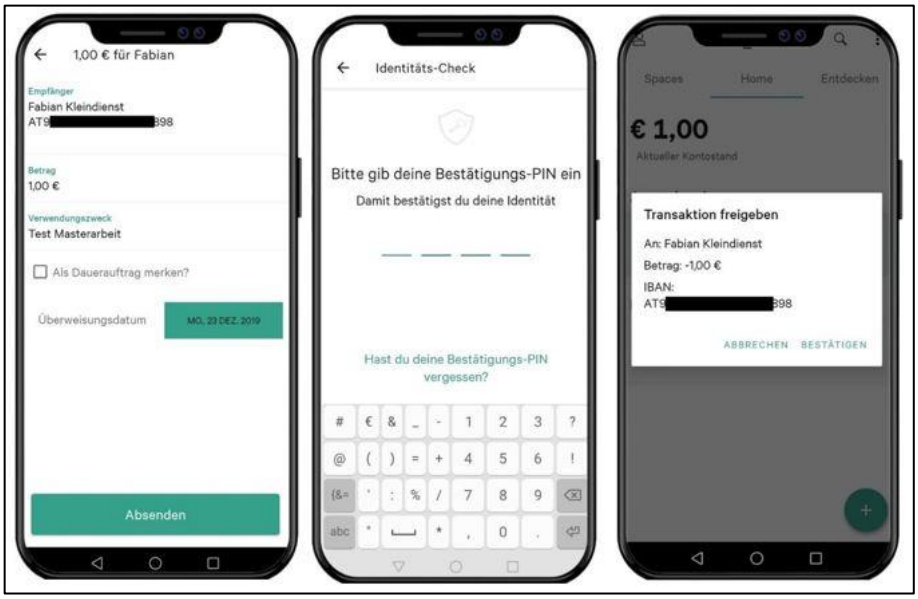


Abbildung 13: Transaktionsauftrag, -bestätigung mit dem PIN und -abschluss

3.4.8 Transaktion aus der ELBA-App

Im Beispiel der ELBA-App von der Raiffeisenbank wird eine pushTAN zur Zahlungsfreigabe erzeugt. Zum Öffnen der pushTAN muss ein fünfstelliger Code eingegeben oder die Einsicht per Fingerprint ermöglicht werden. Bevor die Transaktion durchgeführt wird, ist diese nochmals zu kontrollieren und zu bestätigen. Wie bei allen App-Lösungen ist beim pushTAN Verfahren der Kommunikationskanal vom Zahlungsdienstleister kontrollierbar.

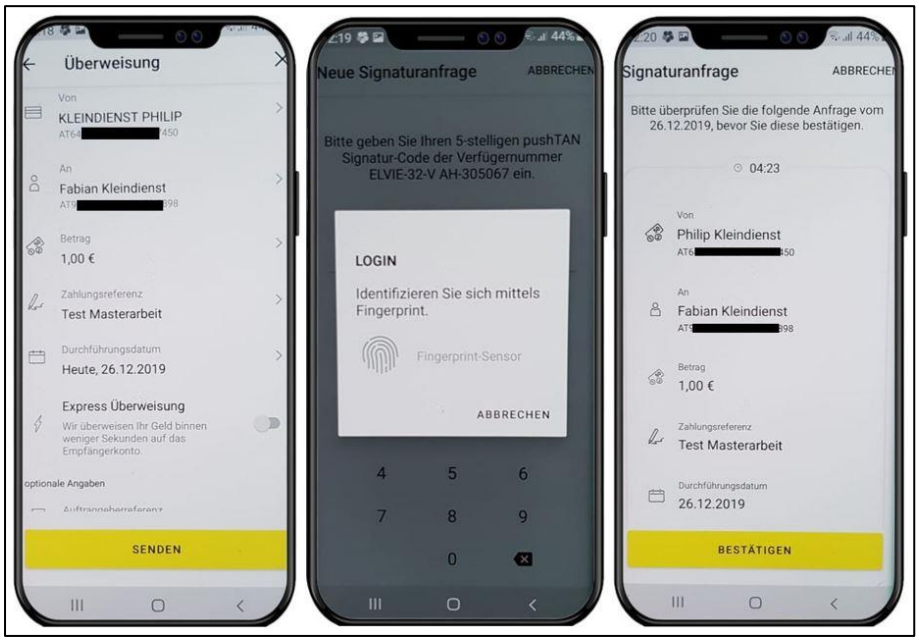


Abbildung 14: Transaktionsauftrag, Login nach push-TAN und Bestätigung

Die Raiffeisenbank bietet als **Alternative** zur Smartphone oder Tablet gebundenen Variante auch eine Desktop Variante an. Dies ist eine Applikation, welche die pushTAN zur Login- oder Transaktionsbestätigung auf den Desktop übermittelt. Der Ablauf ist analog zur App auf dem Smartphone und sieht diesem sehr ähnlich. (Raiffeisen, o. J.)

3.4.9 Beispiel für Open Banking

In Tabelle 4 werden Beispiele für Open Banking angeführt. Nachdem die API Schnittstelle für alle Zahlungsdienstleister seit September 2019 gemäß der PSD2 verpflichtend ist, wurde analysiert, welche Zahlungsdienstleister aktiv als „Drittanbieter“ in den Markt eintreten.

Kontoinformationsdienst	**Zahlungsauslösedienst**
Die **Erste Group Bank** bietet die Möglichkeit, Zahlungskonten anderer Zahlungsdienstleister in George einzubinden. Dazu muss bei der Einrichtung die Verfügernummer und die PIN des einzubindenden Zahlungskontos angegeben werden. Mit der Bestätigung der Zugangsdaten sind am Dashboard bereits die Informationen des neuen Zahlungskontos ersichtlich. Die Funktion befindet sich zum Zeitpunkt der Erstellung der Masterarbeit seitens der Erste Group Bank in Überarbeitung und kann daher nicht demonstriert werden. Weitere Zahlungsdienstleister, welche das Einbinden von Fremdkonten anbieten: • Die alles direkt Bank (DADAT) • Volksbank	Die Zahlungsauslösedienste werden vorrangig von FinTechs entwickelt. Beispiele für einen Zahlungsauslösedient sind: • PayPal • Google Pay • Apple Pay

Tabelle 4: Zahlungsauslöse und Kontoinformationsdienste in der Praxis

3.4.10 Übersichtsmatrix der Möglichkeiten

In nachfolgender Tabelle 5 sind die verschiedenen Möglichkeiten der Kapitel 3.4.1 bis 3.4.9 übersichtlich dargestellt. Daraus geht hervor, dass die Erste Group Bank, die Raiffeisenbank und die N26 nicht auf mobileTANs setzt. Die Erste Group Bank bietet als einziger Zahlungsdienstleister in dieser Testmenge die Möglichkeit zu Multibanking. Alle vier analysierten Zahlungsdienstleister ermöglichen einen App-basierten Login oder eine App-basierte Transaktion. Alternativen für jene NutzerInnen, welche keine App-fähigen Devices besitzen, bieten die Erste Group Bank und die Raiffeisenbank an. Hinzuzufügen ist, dass die BAWAG P.S.K dafür die mobileTAN anbietet. Zusätzlich unterscheidet die Zahlungsdienstleister voneinander, ob Prozesse in einer App oder mit einer zusätzlichen „Freigabe"-App abgewickelt werden.

Zahlungsdienstleister	Möglichkeit zu Open Banking	mobileTAN	Freigabe-App	„all-in-one" Lösung bei Transaktionen mit der App	Alternativen zu Mobiletelefon abhängigen Lösungen
Erste Group Bank	✓	✗	✓	✓	✓
BAWAG P.S.K	✗	✓	✓	✓	✗
N26	✗	✗	✓	✓	✗
Raiffeisenbank	✗	✗	✓	✓	✓

Tabelle 5: Übersicht der Lösungsvarianten zur PSD2 konformen Transaktionsfreigabe (Stand der Erhebung Dezember 2019)

3.5 Vorteile und Nachteile sowie Chancen und Risiken der SCA

In folgendem Abschnitt sind die Betrachtungen der Auswirkungen auf KundInnen in Bezug zur SCA dargestellt.

Haftung: VerbraucherInnen haften bei nicht autorisierten Zahlungen mit einem Höchstbetrag von € 50. Dies gilt nur, wenn die VerbraucherInnen die missbräuchliche Verwendung bemerkt und verhindern hätten können. Wird VerbraucherInnen eine grobe Fahrlässigkeit in der Verwendung ihrer Instrumente nachgewiesen, gilt die Grenze von € 50 nicht. Die Beweispflicht, eine missbräuchliche Verwendung und grobe Fahrlässigkeit nachzuweisen, liegt in der Verantwortung der Zahlungsdienstleister. (Fletzberger, o. J.)

Sicherheit: Die BAWAG P.S.K sowie die N26, um Beispiele zu nennen, empfehlen zur sicheren Verwendung und Einhaltung der Verpflichtungen seitens der NutzerInnen folgendes: (bawaggroup, 2019b; N26, o. J.)

- Nutzung von vertrauenswürdigen Devices und Netzwerken für die Installation und Verwendung von z.B. Banking Apps
- Apps und Devices vor allem im Bezug zur geladenen Software aktuell halten
- Keine Deaktivierung von standardmäßig vorgegebenen Sicherheitsmaßnahmen wie z.B. die Anzeige von PIN Eingaben im Klartext
- Download von Banking Apps ausschließlich aus den offiziellen App Stores
- Niemals PIN, Passwörter, Einmalpasswörter oder Benutzernamen an unbefugte Dritte weitergeben

Sicherheit der mobileTAN: Wie im Kapitel 4.3.3 erkennbar wird, hält die mobileTAN einen entsprechend großen Verwendungsanteil. Einzelne Zahlungsdienstleister haben derzeit einen Schwerpunkt in der Verwendung von Lösungen in der Kombination mit der mobileTAN. In verschiedenen Medien bekommt man die Information, dass die mobileTAN dennoch ein Auslaufmodell sein

könnte, da mobileTAN Lösungen nicht PSD2 konform sein könnten. Die mobileTAN wird dabei in Form eines Klartexts über unverschlüsselte Kanäle an die KundInnen versendet. (Härtel, 2019; Dax, 2016) Im Rahmen der sicheren Kommunikation beschreibt die Delegierte Verordnung (EU) 2018/389, dass die Zahlungsdienstleister die Verantwortung für eine sichere Kommunikation tragen und alle Ereignisse zu jedem Zeitpunkt des Transaktionsprozesses rückverfolgbar sein müssen. (siehe Kapitel 3.3) Im Rahmen der mobileTAN Lösung besteht die Möglichkeit, dass BetrügerInnen die mobileTAN zur Authentifizierung an andere Devices weiterleiten. Eine Risikominimierung zu diesem genannten Angriff bietet Dynamic Linking, welche im Transaktionsfreigabeprozess den Betrag und das Zielkonto in den Freigabeprozess einbezieht. Damit kann zumindest verhindert werden, dass das Konto der EmpfängerInnen nachträglich geändert wird. Ansonsten würde der Authentifizierungscode ungültig werden (siehe Kapitel 3.2.2) (Bundesamt für Sicherheit in der Informationstechnik, o. J.)

In einer Stellungnahme der EBA wird erläutert, dass die mobileTAN als Freigabefaktor erlaubt ist. Der Faktor zähle zum Kriterium „Besitz“. Es ist jedoch nicht die mobileTAN der „Besitz“, sondern die SIM-Karte an welche die mobileTAN versendet wird. Die Mobilnummer ist in der Regel einer SIM-Karte zugeordnet. Laut EBA ist der Zahlungsdienstleister dafür zuständig, Daten, in einer nach anerkannten Sicherheitsstandards, sicheren Umgebung zu transferieren. Ob der Transfer einer mobileTAN einen sicheren Kanal darstellt, geht aus der Stellungnahme nicht hervor. (Europäische Bankenaufsichtsbehörde, 2018a)

Sicherheit von Fingerprint und Gesichtsscans: Selbst entwickelte Apps für die Zahlungsfreigabe oder die Zahlungsfreigabe innerhalb der Banking App können, entgegengesetzt der mobileTAN, vom Zahlungsdienstleister kontrolliert werden. Der Fingerprint und der Gesichtsscan sind vor allem für NutzerInnen ein komfortables Mittel als Freigabefaktor. Sicherer als ein gut gewähltes Passwort ist diese Methode jedoch nicht. BetrügerInnen schaffen es durch spezielle Fotos oder nachgebildete Fingerabdrücke die Methoden zu manipulieren. (Deutsche Telekom,

o. J.) Es gibt Tests in welchen sich auch die neuesten Handymodelle mit Fotoausdrucken entsperren lassen. Diese Modelle leiten die Gesichter zur Freigabe bereits aus einem zweidimensionalen Bild ab. (computerbild, 2020) Da es sich jedoch nur um einen Faktor handelt und jeweils der zweite Faktor im Besitz von BetrügerInnen sein muss, kann die Transaktion dadurch nicht manipuliert werden.

Usability: Für die Erhöhung der Sicherheit und Erschwernis von Hacker Angriffen müssen NutzerInnen künftig bei ihren Transaktionen und Zugriffen zu Zahlungskonten bei der Authentifizierung einen Schritt mehr anwenden. Dies ist auf die SCA zurückzuführen. In Zuge dessen ist der Besitz eines Smartphones in den meisten Anwendungen Voraussetzung. (Javaid, 2019)

3.6 Vorteile und Nachteile sowie Chancen und Risiken von Open Banking

In folgendem Abschnitt sind die Betrachtungen der Auswirkungen auf KundInnen in Bezug zu Open Banking dargestellt.

Qualitätssicherung: Die in der RTS festgelegten Kommunikationsstandards fordern eine sichere Kommunikation zwischen Zahlungsdienstleistern und Drittanbietern. Dies wird sichergestellt indem Zahlungsdienstleister die gleichen Leistungsindikatoren wie für deren eigene online Services einhalten müssen. Zudem besteht die Anforderung die Schnittstellen einem Prototyptest und Realitätstest von jeweils drei Monaten zu unterziehen. Dabei können sich MarktteilnehmerInnen unter Marktbedingungen ein Bild von der Schnittstelle machen. Um dies zu kontrollieren, befürwortet die EU Kommission die Zusammensetzung einer Marktgruppe aus VertreterInnen von Zahlungsdienstleistern, von Drittanbietern und Service NutzerInnen. (Europäische Kommission, 2017)

Datenschutz: Sowie innerhalb der Datenschutzrichtlinie vorgesehen, gilt auch gemäß der PSD2 die Regelung, dass VerbraucherInnen die Weitergabe der Daten kontrollieren können. Solange die VerbraucherInnen keine ausdrückliche

Zustimmung zur Datenverarbeitung erteilen, dürfen diese nicht verarbeitet werden. Zudem dürfen nur jene personenbezogenen Daten weitergegeben und verarbeitet werden, welche für die Erbringung der zugestimmten Services notwendig sind. Die VerbraucherInnen haben gemäß der Datenschutzrichtlinie die Rechte auf den Zugriff und die Löschung ihrer Daten. (Europäische Kommission, 2017)

4. Empirische Datenerhebung

Wie bereits zur methodischen Vorgehensweise in Kapitel 1 erwähnt, werden durch eine empirische Datenerhebung mittels eines online Fragebogens die Auswirkungen der PSD2 auf die Zahlungsdienst NutzerInnen erhoben. Diese Befragung bildet den zweiten Teil zur Beantwortung der Forschungsfrage. Der online Fragebogen unterteilt sich in die vier Bereiche „Payment Service Directive 2“, „Strong Customer Authentification“, „Open Banking“ und „allgemeine Informationen“. Innerhalb des ersten Bereichs liegt der Fokus auf eine Einleitung und allgemeine Informationen zur PSD2. In den Bereichen zwei und drei, SCA und Open Banking, liegt der Fokus auf die Sicherheit, das Vertrauen, die Benutzerfreundlichkeit und deren Einschätzungen, Reaktionen und Wahrnehmungen aus Sicht der NutzerInnen. Im vierten Bereich werden demographische Informationen erhoben, um Auswirkungen in regionaler-, altersbedingter- und beruflicher Hinsicht zu evaluieren. Die in Kapitel 3 gewonnenen Erkenntnisse fließen in den online Fragebogen ein.

4.1 Aufbau des Fragebogens

Aufgrund der Komplexität sind zu Beginn des Fragebogens die Eckdaten der PSD2 näher beschrieben. Da sich der Fragebogen in verschiedene Bereiche aufteilt, ist die jeweils notwendige Einleitung und Erklärung unmittelbar vor den entsprechenden Bereichen eingegliedert. Dies hat den Hintergrund, dass alle Informationen zu spezifischen Details unmittelbar vor den entsprechenden Fragen zur Verfügung stehen. Darüber hinaus wurde versucht die Sprache und Erklärung für den Fragebogen einfach zu halten und nur die notwendigsten Informationen in Bezug zum Fragebogen zu erwähnen.

Der Fragebogen enthält 21 geschlossene Fragen, wobei unter Anwendung verschiedener Regeln nicht allen TeilnehmerInnen dieselben 21 Fragen gestellt werden. Bei der Erstellung des Fragebogens wurde darauf geachtet, alle Fragen als Pflichtfragen zu definieren. Die ausschließliche Anwendung von Pflichtfragen

steigert zwar das Risiko, dass TeilnehmerInnen vor dem erfolgreichen Abschluss abbrechen, schafft jedoch Klarheit bei der Auswertung.

Die Antworten des Online Fragebogens lassen sich im Wesentlichen in eine Klassifizierungsform – das Skalenniveau – unterteilen.

- Die **Nominalskala**, diese umfasst qualitative Variable, welche unterschiedliche Bezeichnungen darstellen, jedoch keine Anordnung ermöglichen (z.B. die Auswahl des verwendeten Bankkontos).
- Die **Ordinalskala**, diese umfasst Ausprägungen, welche eine Rangordnung ermöglichen können (z.B. die Bewertung der Zwei-Faktor-Authentifizierung von sehr gut bis nicht gut).
- Die **Verhältnisskala**, das sind metrische Variablen, welche in Verhältnissen zueinander dargestellt werden können (z.B. das Alter). (Alt, 2013, S. 7f.)

Bei den TeilnehmerInnen handelt es sich um eine Zufallsstichprobe, die nicht in Bereiche z.B. Bevölkerungsschichten, Alter oder Bildungsabschluss, vordefiniert wurde.

Der Fragebogen ist mit Screenshots im Anhang C und D dargestellt. Das verwendete Tool für die Durchführung der Befragung und die erste Aufbereitung der Daten stammt von https://www.umfrageonline.com/s/Auswirkungen_der_PSD2. Die weitere Aufbereitung erfolgt mit Microsoft Excel. Die Bewerbung des Fragebogens hat über Beiträge in Facebook, LinkedIn, Xing, über das Teilen in themenspezifischen Foren und durch persönliche Kontaktaufnahmen stattgefunden.

4.2 Signifikanzniveau der Stichprobe

Als Grundgesamtheit für die Befragung im Rahmen dieser Masterarbeit werden alle NutzerInnen von online Services im österreichischen Zahlungsverkehr definiert. Im Jahr 2019 nutzten 63% der österreichischen Bevölkerung Online-Banking. Daher beläuft sich die Grundgesamtheit, bei 8,8 Millionen österreichischen

StaatsbürgerInnen im Jahr 2019, auf 5,5 Millionen Personen, die Online-Banking nutzten. (statista, 2020a; statista, 2020b)

Vor der Durchführung der Befragung wurde eine repräsentative Stichprobengröße der NutzerInnen von online Services im österreichischen Zahlungsverkehr berechnet. Dafür wurde die Grundgesamtheit von 5,5 Millionen Personen herangezogen. Als Fehlermarge, das ist die Abweichung zwischen dem Ergebnis der Stichproben und dem der Grundgesamtheit, wurden 5% definiert. Als Konfidenzniveau, dieses zeigt die Sicherheit, dass die Fehlermarge eingehalten wird, wurden 90% definiert. Nachdem nicht vorherzusehen war, wie sich die Antworten verteilen, wurde eine Standardabweichung von 50% definiert. Das ist jener Wert, der den schlimmsten Fall darstellt und genügend Sicherheit bringt, dass die Stichprobengröße repräsentativ zur Grundgesamtheit ist. Aus diesen Parametern ließ sich eine Stichprobe von mindestens 271 TeilnehmerInnen errechnen. (qualtrics, 2020)

4.3 Auswertung und statistische Erkenntnisse

Mithilfe der deskriptiven statistischen Analyse wurden die Informationen aus der Stichprobe aller TeilnehmerInnen der online Befragung aufbereitet. „Deskriptiv" bedeutet beschreibend und eignet sich gut für die Beantwortung von Fragestellungen mit dem Typ „Wie", entsprechend der Forschungsfrage „Wie wirken sich die Veränderungen der PSD2 auf die NutzerInnen im österreichischen Zahlungsverkehr aus?". Bei der Auswertung in der deskriptiven Statistik wurde zwischen Analysen eines Merkmals und Analysen von Zusammenhängen mehrerer Merkmale unterschieden.

Nachdem in dieser Forschungsarbeit ausschließlich der österreichische Zahlungsverkehr betrachtet wird, wurden die Datensätze mit „kein österreichischer Zahlungsdienstleister" innerhalb der Analysen aussortiert. Jene Datensätze, die bei den Auswirkungen von SCA mit einer entsprechenden Begründungen sowohl einen Grund für „Ich verwende Online Banking und E-Commerce Transaktionen (Online

Handel) mehr als bisher, weil“ als auch einen Grund für „Ich verwende Online Banking und E-Commerce Transaktionen (Online Handel) weniger als bisher, weil“ angegeben haben, wurden ebenso aussortiert. Es basiert auf der Annahme, dass ein Service nicht zugleich mehr und weniger als bisher benutzt werden kann. Wenn beide Datensätze bei diesen Aussagen „trifft nicht zu“ beinhalten, wird davon ausgegangen das die Verwendung gleichbleibend ist.

Während der Laufzeit der Onlineumfrage zwischen 24.02.2020 und 02.04.2020 konnten 381 TeilnehmerInnen zur Durchführung geworben werden. Von den 381 TeilnehmerInnen haben 330 TeilnehmerInnen den Fragebogen abgeschlossen. Wie bereits im vorhergehenden Absatz erwähnt, wurden Datensätze nach entsprechenden Regeln entfernt, sodass 287 gültig beantwortete Fragebögen für weitere Analysen zur Verfügung stehen. Damit ist die notwendige Anzahl von TeilnehmerInnen für ein repräsentatives Ergebnis, aus statistischer Sicht, erreicht. Die Zahlen sind in der folgenden Tabelle 7 und Tabelle 7 zusammengefasst dargestellt:

Eigenschaft	**Werte**
Österreichische Staatsbürger	8.800.000 Personen
NutzerInnen von online Services im österreichischen Zahlungsverkehr	63%
Grundgesamtheit	5.500.000 Personen
Fehlermarge	5%
Konfidenzniveau	90%
Standardabweichung	50%
Mindestwert für eine repräsentative Stichprobe	**271 Personen**

Tabelle 6: Ausgangspunkt vor der Befragung

Eigenschaft	Anzahl der Personen
durchgeführte Befragungen	381
davon nicht abgeschlossene Befragungen	51
abgeschlossene Befragungen	330
davon gemäß Kriterien ungültige Befragungen	43
gültige abgeschlossene Befragungen	**287**

Tabelle 7: Ausgangspunkt nach der Befragung

4.3.1 Demographische Merkmale

In den drei nachfolgenden Tabellen sind die wichtigsten demographischen Merkmale Alter, Herkunft und berufliches Tätigkeitsfeld der Stichprobe dargestellt.

Die Stichprobe enthält eine Ausgeglichenheit bei den 29- bis 58-Jährigen, mit jeweils knapp einem Viertel. Die unter 18-Jährigen und über 58-Jährigen sind weniger repräsentativ in der Stichprobe enthalten und die 14- bis 17-Jährigen sowie die über 70-Jährigen sind für diese Auswertung nicht repräsentativ genug. (siehe Tabelle 8)

Alter	Anzahl	Anteil
14-17	1	0%
18-28	51	18%
29-38	66	23%
39-48	66	23%
49-58	64	22%
59-69	30	11%
ab 70	9	3%
Summe	**287**	**100%**

Tabelle 8: Verteilung des Alters der Stichprobe (Frage 18)

Regional richtet sich der Schwerpunkt auf die Landeshauptstädte mit 37% und ländliche Regionen mit 45%. Die Bezirkshauptstädte befinden sich mit 16% zwischen diesen beiden Regionen. (siehe Tabelle 9)

Herkunft	**Anzahl**	**Anteil**
Landeshauptstadt	106	37%
Bezirkshauptstadt	45	16%
ländliche Region	129	45%
Keine Angaben	7	2%
Summe	**287**	**100%**

Tabelle 9: Verteilung der Herkunft der Stichprobe (Frage 19)

Insgesamt sind rd. 80% der Stichprobe nicht in der Finanzbranche tätig. Diese rd. 80% verhelfen dabei die Qualität der Ergebnisse in Bezug auf die Auswirkungen der PSD2 zu steigern. Es ist davon auszugehen, dass sich die Wahrnehmung der Auswirkungen, jener in der Finanzbranche tätigen Personen von jenen außerhalb der Finanzbranche tätigen Personen, unterscheidet. (siehe Tabelle 10)

Berufliches Tätigkeitsfeld	**Anzahl**	**Anteil**
Tätigkeitsfeld in der Finanzbranche	56	20%
Tätigkeit mit Berührungspunkten zur Finanzbranche	31	11%
Anderer Tätigkeitsbereich	154	54%
Nicht berufstätig	13	5%
StudentIn	22	8%
Keine Angaben	11	4%
Summe	**287**	**100%**

Tabelle 10: Verteilung des beruflichen Tätigkeitsfeldes der Stichprobe (Frage 21)

4.3.2 PSD2 Allgemein

Um festzustellen, welche Zusammenhänge zwischen den einzelnen Fragen bestehen, wurden zu Beginn alle Ergebnisse der Stichprobe in numerische Werte umgewandelt. Folgend wurde mithilfe von Excel eine Korrelations-Funktion (in der Statistik als „r“ definiert) angewendet. Entsprechend der Richtwerte wann etwas einen kleinen Effekt (r = 0,1), einen mittleren Effekt (r = 0,3) oder einen großen Effekt (r = 0,5) auf die Variablen hat, konnten diese näher betrachtet werden. (Hemmerich, o. J.) Jene Werte, welche zumindest einen Wert von r = 0,4 oder -0,4 erreichten, wurden farblich hervorgehoben. Folgende Zusammenhänge, im Anhang A und B nachzulesen, hoben sich aufgrund der Korrelation von anderen ab und sind unter folgenden Aussagen zusammengefasst:

Korrelationen:

- Personen, die die PSD2 und ihre Inhalte kennen, nutzen Services eines Zahlungsdienstleisters über eine App auf dem Smartphone oder Tablet häufiger
- Personen, die die PSD2 und ihre Inhalte kennen, fühlen sich besser über die Zwei-Faktor-Authentifizierung informiert
- Personen, die die PSD2 und ihre Inhalte kennen, sind beruflich eher an der Finanzbranche ausgerichtet
- Personen, die Services eines Zahlungsdienstleisters über eine App auf dem Smartphone oder Tablet häufiger nutzen, bewerten die Usability eines Zahlungsauslösedienstes besser
- Personen, die Services eines Zahlungsdienstleisters über eine App auf dem Smartphone oder Tablet häufiger nutzen, tendieren zu einem jüngeren Alter
- Personen, die Services eines Zahlungsdienstleisters über eine App auf dem Smartphone oder Tablet häufiger nutzen, sind beruflich an der Finanzbranche ausgerichtet

- Personen, die sich besser über die neuen Zwei-Faktor-Authentifizierungsmethoden informiert fühlen, bewerten die Sicherheit, die Usability und das Vertrauen zum Services besser
- Personen, die sich besser über die neuen Zwei-Faktor-Authentifizierungsmethoden informiert fühlen, bewerten den Informationsgrad zu Open Banking besser
- Personen, die sich besser über die neuen Zwei-Faktor-Authentifizierungsmethoden informiert fühlen, bewerten die Usability von Zahlungsauslösediensten besser
- Bei der Bewertung der Zwei-Faktor-Authentifizierung korrelieren Antworten in Bezug zur Sicherheit und dem Vertrauen höher als in Bezug zur Usability. Eine geringere Korrelation besteht zwischen Sicherheit und Usability. Das bedeutet im Umkehrschluss, dass Sicherheit und Usability nicht gleich gut bewertet werden
- Personen, die Online Services mehr als bisher nutzen, das vor allem aus Gründen der Usability, bewerten auch die Usability der Kontoinformationsdienste besser
- Eine hohe negative Korrelation liegt bei der Reihung von Zwei-Faktor-Authentifizierungen nach der Wichtigkeit von Sicherheit und Usability vor, was bedeutet, dass die Sicherheit und Usability konträr gereiht wurden

Die aussagekräftigsten Korrelationen werden in den folgenden Abschnitten analysiert.

Die Tabelle 11 zeigt, dass zwei Drittel bereits von der Richtlinie gehört haben oder die Inhalte kennen. Rund ein Drittel der Stichprobe kennt die PSD2 und ihre Inhalte nicht.

Wissensstand über die PSD2	**Anzahl**	**Anteil**
Ja, ich kenne die Inhalte der Richtlinie	76	27%
Ich habe davon gehört, kenne aber keine Inhalte	110	38%
Nein, die PSD2 kannte ich bisher nicht	101	35%
Summe	**287**	**100%**

Tabelle 11: Wissensstand über die PSD2 allgemein (Frage 2)

Von den TeilnehmerInnen, welche die Richtlinie inhaltlich kennen, arbeiten rd. 60% in der Finanzbranche. Wohingegen über 70% der TeilnehmerInnen, welche die PSD2 nicht kennen andere Tätigkeitsbereiche verfolgen. (siehe Tabelle 12)

Berufliches Tätigkeitsfeld	**PSD2 bekannt**		**PSD2 teilweise bekannt**		**PSD2 nicht bekannt**	
	Anzahl	**Anteil**	**Anzahl**	**Anteil**	**Anzahl**	**Anteil**
Tätigkeit in der Finanzbranche	45	59%	10	9%	1	1%
Tätigkeit mit Berührungspunkten zur Finanzbranche	11	15%	12	11%	8	8%
Anderer Tätigkeitsbereich	17	22%	65	59%	72	71%
Nicht berufstätig	1	1%	9	8%	3	3%
StudentIn	1	1%	9	8%	12	12%

Berufliches Tätigkeitsfeld	PSD2 bekannt		PSD2 teilweise bekannt		PSD2 nicht bekannt	
	Anzahl	Anteil	Anzahl	Anteil	Anzahl	Anteil
Keine Angaben	1	1%	5	5%	5	5%
Summe	**76**	**100%**	**110**	**100%**	**101**	**100%**

Tabelle 12: Wissensstand zur PSD2 und berufliches Tätigkeitsfeld (Frage 2/21)

Wird der Wissensstand zur PSD2 mit der Herkunft in Bezug gesetzt, ist erkennbar, dass dieser in Landeshauptstädten höher ist. Mit 47% wohnen TeilnehmerInnen, welche die Richtlinie kennen, in einer Landeshauptstadt. Wohingegen jene, welche weniger Wissen über die Richtlinie besitzen, mit jeweils knapp 50%, ländlicher Herkunft sind. (siehe Tabelle 13)

Herkunft	PSD2 bekannt		PSD2 teilweise bekannt		PSD2 nicht bekannt	
	Anzahl	Anteil	Anzahl	Anteil	Anzahl	Anteil
Landeshauptstadt	36	47%	35	32%	35	35%
Bezirkshauptstadt	13	17%	20	18%	12	12%
ländliche Region	27	36%	51	46%	51	51%
Keine Angaben	0	0%	4	4%	3	3%
Summe	**76**	**100%**	**110**	**100%**	**101**	**100%**

Tabelle 13: Wissensstand zur PSD2 und Herkunft (Frage 2/19)

Beim Alter lässt sich im Vergleich dazu, ob innerhalb der Stichproben jemand die Inhalte der Richtlinie besser kennt, nur davon gehört oder diese gar nicht kennt, keine Tendenz erkennen. In den Vergleichsfällen teilen sich die 18- bis 58-Jährigen, das sind vier Gruppen, jeweils rd. 20 bis 30%.

Die höchste abgeschlossene Ausbildung trägt keinen essentiellen Beitrag dazu bei, ob TeilnehmerInnen mehr oder weniger mit der Richtlinie vertraut sind. Die Stichprobe zeigt, dass rd. 87% der TeilnehmerInnen, welche inhaltlich mit der Richtlinie vertraut sind, eine Matura oder einen akademischen Abschluss haben. TeilnehmerInnen mit Matura oder akademischen Abschluss, welche weniger oder nicht mit der Richtlinie vertraut sind, haben mit jeweils rd. 70% einen geringfügig kleineren Anteil. Da gesamtheitlich in der Stichprobe mit anteilig rd. 45% einen akademischen Abschluss haben, ist die höchst abgeschlossene Ausbildung weniger repräsentativ. Eine Lehre oder Berufsausbildung sowie Fachschulabschlüsse nehmen in der Stichprobe nur einen Anteil von rd. 16% ein.

Bezugnehmend auf Kapitel 3.4, in welchem verschiedene PSD2 konforme Lösungen dargestellt sind, wird im Rahmen der Stichprobe auf die verschiedenen österreichischen Zahlungsdienstleister eingegangen, da verschiedene Lösungen verschiedene Auswirkungen ermöglichen können. Die Bankkonten, welche von den TeilnehmerInnen als Hauptkonto angegeben wurden, verteilen sich wie folgt:

Zahlungsdienstleister	**Anzahl**	**Anteil**
Erste Group Bank (inklusive. Sparkasse)	101	35%
Raiffeisenbank	88	31%
BAWAG P.S.K	34	12%
UniCredit Bank Austria	30	11%
Sonstiger österreichischer Zahlungsdienstleister	34	12%
Summe	**287**	**100%**

Tabelle 14: Verteilung der Zahlungsdienstleister auf die Stichrobe (Frage 1)

In der Tabelle 14 zeigt sich ein großer Anteil der Raiffeisenbank und Erst Group Bank KundInnen mit jeweils mehr als 30%. Die BAWAG P.S.K und die UniCredit Bank Austria sind in der Stichprobe anteilig mit jeweils knapp über 10% enthalten.

Um das Verhältnis der Anzahl von KundInnen im österreichischen Zahlungsverkehr in einem Vergleich mit der Stichprobe darzustellen, nachfolgend einige Daten:

Rund 12 Millionen KundInnen werden am österreichischen Markt von genannten vier Zahlungsdienstleistern angegeben. Dabei ist zu beachten, dass Mehrfachkonten bei verschiedenen Zahlungsdienstleistern möglich sind. Anteilig davon haben

- die Raiffeisenbank und die Erste Group Bank mit jeweils rd. 4 Millionen KundInnen (33%) den größten Anteil,
- folgend die BAWAG P.S.K mit 2,5 Millionen KundInnen (21%)
- und die UniCredit Bank Austria mit knapp über 1,5 Millionen KundInnen (13%).

Ausgenommen der BAWAG P.S.K nähert sich die Stichprobe dem Verhältnis der tatsächlichen Anzahl von KundInnen der österreichischen Zahlungsdienstleister an. (UniCredit Bank Austria, 2018; erstegroup, o. J.; Österreichischer Raiffeisenverband, 2018; bawaggroup, o. J.)

Überleitend zur Auswirkung der Inhalte, SCA und Open Banking, spielt die Frage zur Häufigkeit der Benutzung von Services eines Zahlungsdienstleisters über den Computer oder über die App auf dem Smartphone oder dem Tablet eine Rolle. In der Tabelle 15 ist die Häufigkeit der verwendeten Services dargestellt. Anhand der arithmetischen Mittelwerte ist erkennbar, dass innerhalb der Stichprobe die Häufigkeit der Benutzung eines Services mittels Apps steigt. Jene Befragten, die online Services benutzen, nutzen diese durchschnittlich einmal wöchentlich mit dem Computer und mehrmals wöchentlich mit einer App.

Entsprechend Tabelle 15 zeigt sich, dass das arithmetische Mittel bei der Häufigkeit der Nutzung von online Services mit dem Computer 3,7 ergibt. Das ist eine Häufigkeit der Benutzung von zumindest einmal wöchentlich. Das arithmetische Mittel bei der Häufigkeit der Nutzung von online Services mit der App über das Smartphone oder Tablet liegt bei 2,9. Das ist eine Häufigkeit der Nutzung von

zumindest mehrmals wöchentlich. Auf jene, die solch ein online Service nutzen wirkt sich die SCA und Open Banking aus.

Häufigkeit	**Servicenutzung mit dem Computer**		**Servicenutzung mit der App**	
	Anzahl	**Anteil**	**Anzahl**	**Anteil**
mehrmals täglich (1)	13	5%	41	14%
Einmal täglich (2)	14	5%	26	9%
Mehrmals wöchentlich (3)	74	26%	82	29%
Einmal wöchentlich (4)	82	29%	39	14%
Einmal monatlich (5)	66	23%	25	9%
Nie (6)	38	13%	74	26%
Summe	**287**	**100%**	**287**	**100%**
Gewichteter Mittelwert inklusive „nie“	**4,0**		**3,7**	
Gewichteter Mittelwert exklusiver „nie“	**3,7**		**2,9**	

Tabelle 15: Häufigkeit der Nutzung von Services eines Zahlungsdienstleisters (Frage 3)

Zur besseren Übersicht ist dies in einem Balkendiagramm, siehe Abbildung 15, aufbereitet. Einerseits werden die Zugriffe auf online Services mit dem Computer dargestellt, andererseits werden die Zugriffe auf online Services über eine App dargestellt. TeilnehmerInnen, welche mehrmals wöchentlich zugreifen, teilen sich die Häufigkeit der Verwendung von online Services mit der App oder dem Computer. Bei den Zugriffen mittels Apps ist ersichtlich, dass diese häufiger benutzt werden, wohingegen die Zugriffe mittels Computer im Vergleich zur App seltener benutzt werden. Gesamt nutzen 74 % der TeilnehmerInnen Apps für Services der Zahlungsdienstleister.

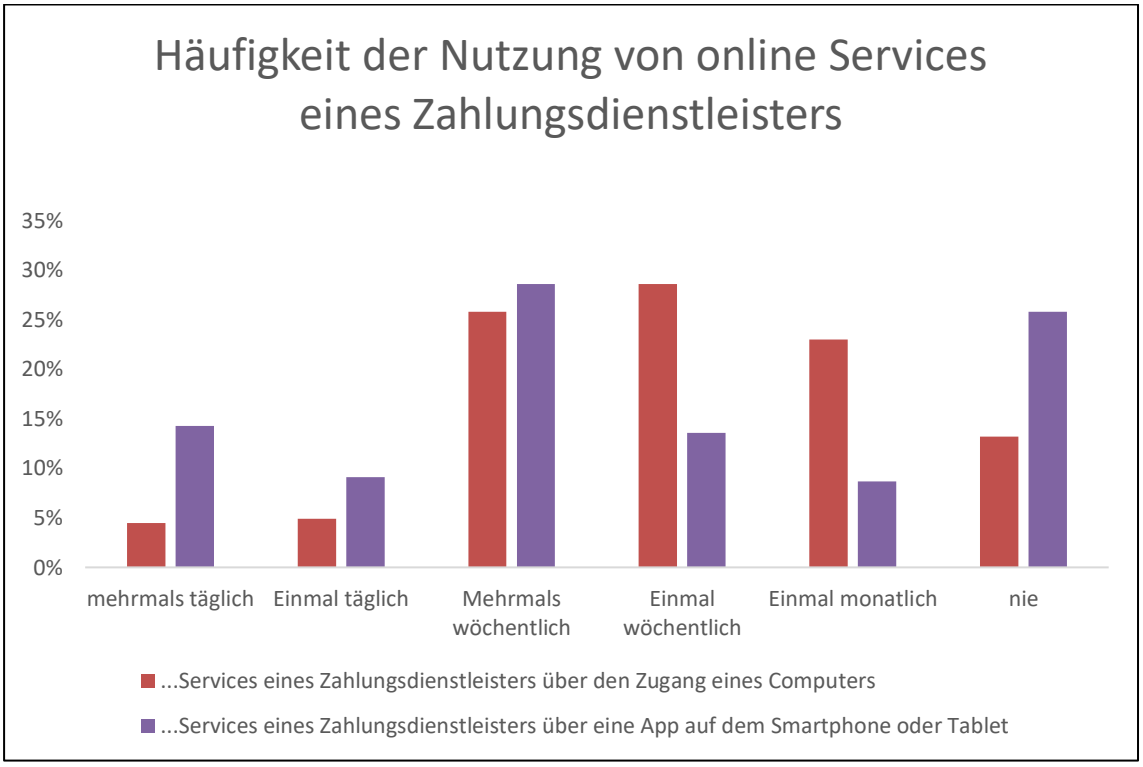


Abbildung 15: Häufigkeit der Nutzung von online Services eines Zahlungsdienstleisters (Frage 3)

Die Stichprobe zeigt, dass 5% nie auf die online Services der Zahlungsdienstleister zugreifen. Eine Auswirkung der PSD2 auf diese Gruppe ist daher nur geringfügig vorhanden. Auf folgende Merkmale begrenzt sich diese Gruppe:

- von SCA ist diese Gruppe nur bei kartenbasierten Transaktionen betroffen
- 73% kannte die PSD2 bisher nicht
- 73% fühlt sich nicht gut über die Möglichkeiten von Open Banking informiert
- 93% nimmt seit September 2019 keine Veränderung im Bereich Open Banking war
- 60% befinden sich im Alter zwischen 49 und 69 Jahren
- 67% haben keinen beruflichen Berührungspunkt in die Finanzbranche
- 60% kommen aus dem ländlichen Bereich

4.3.3 Strong Customer Authentication

Auf die gesamte Stichprobe gesehen, fühlen sich 95%, das sind 272 TeilnehmerInnen, welche online Services nutzen, mit 70% sehr gut oder gut über die neuen SCA-Lösungen informiert. (siehe Abbildung 16)

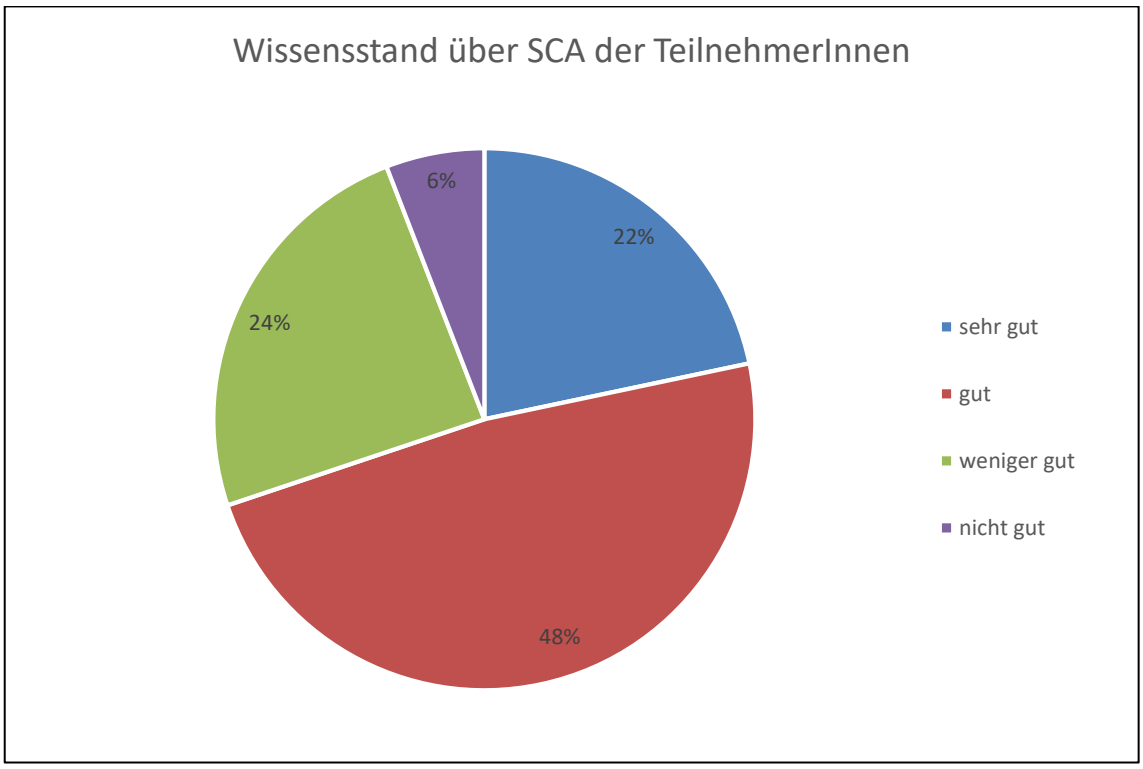


Abbildung 16: Wissensstand über SCA (Frage 4)

Verteilung der SCA Lösungen aus verschiedenen Blickwinkeln

In der Tabelle 16 wird die Wahrnehmung darüber, ob sich TeilnehmerInnen besser oder schlechter über die SCA-Lösungen informiert fühlen, dargestellt und in Bezug zur verwendeten SCA-Lösung gesetzt. Die meist verbreiteten SCA-Lösungen sind Freigaben mit einer App und einem Fingerprint, Gesichtsscan oder Passwort und die Freigabe mit einer mobileTAN, welche als SMS übermittelt wird. Ein geringfügiger Anteil verwendet die Alternativen SCA-Methoden, wo kein Smartphone benötigt wird und einzelne haben angegeben eine andere SCA-Methode zu verwenden.

SCA-Methode	**Wissensstand über SCA-Methode sehr gut/gut**		**Wissensstand über SCA-Methode weniger gut/nicht gut**	
	Anzahl	**Anteil**	**Anzahl**	**Anteil**
mobileTAN per SMS	49	26%	25	31%
App mit Passwort oder Code/PIN	56	30%	23	28%
App mit Fingerprint/Gesichtsscan	72	38%	20	24%
App via Desktopversion	3	2%	2	2%
cardTAN Generator	4	2%	4	5%
Verwenden eine andere SCA	5	3%	2	2%
Wissen nicht welche SCA	1	1%	6	7%
Summe	190	100%	82	100%

Tabelle 16: Wissensstand über SCA-Methoden in Bezug zur verwendeten 2FA-Methode (Frage 4/5)

In der Abbildung 17 ist ersichtlich, dass TeilnehmerInnen, die sich sehr gut oder gut informiert fühlen von einer mobileTAN in Richtung App-basierten Lösung tendieren und jene sich weniger gut oder nicht gut informiert fühlenden von der App-basierten Lösung zur mobileTAN Lösung tendieren.

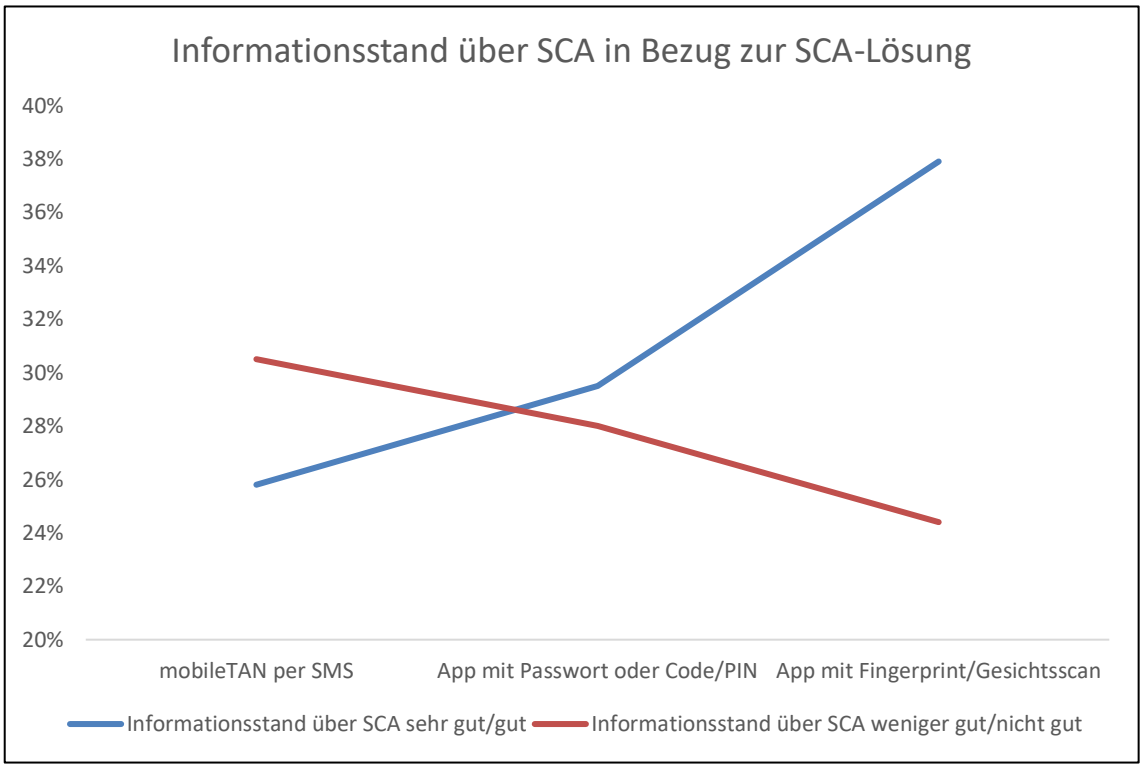


Abbildung 17: Wissensstand über SCA in Bezug zur verwendeten SCA-Lösung (Frage 4/5)

Eine weitere Sichtweise ist der Vergleich von SCA-Lösungen mit den Altersgruppen. Jüngere TeilnehmerInnen tendieren vermehrt zu SCA Lösungen mittels Apps. Wohingegen bei älteren TeilnehmerInnen die mobileTAN Lösungen den größeren Verwendungsanteil zeigt. Die 59- bis 69-Jährigen zeigen einen Ausreißer in Richtung der SCA Lösung mittels App und einem Passwort sind jedoch in dieser eingeschränkten Stichprobe mit knapp 50% weniger Anteil vertreten. (siehe Abbildung 18)

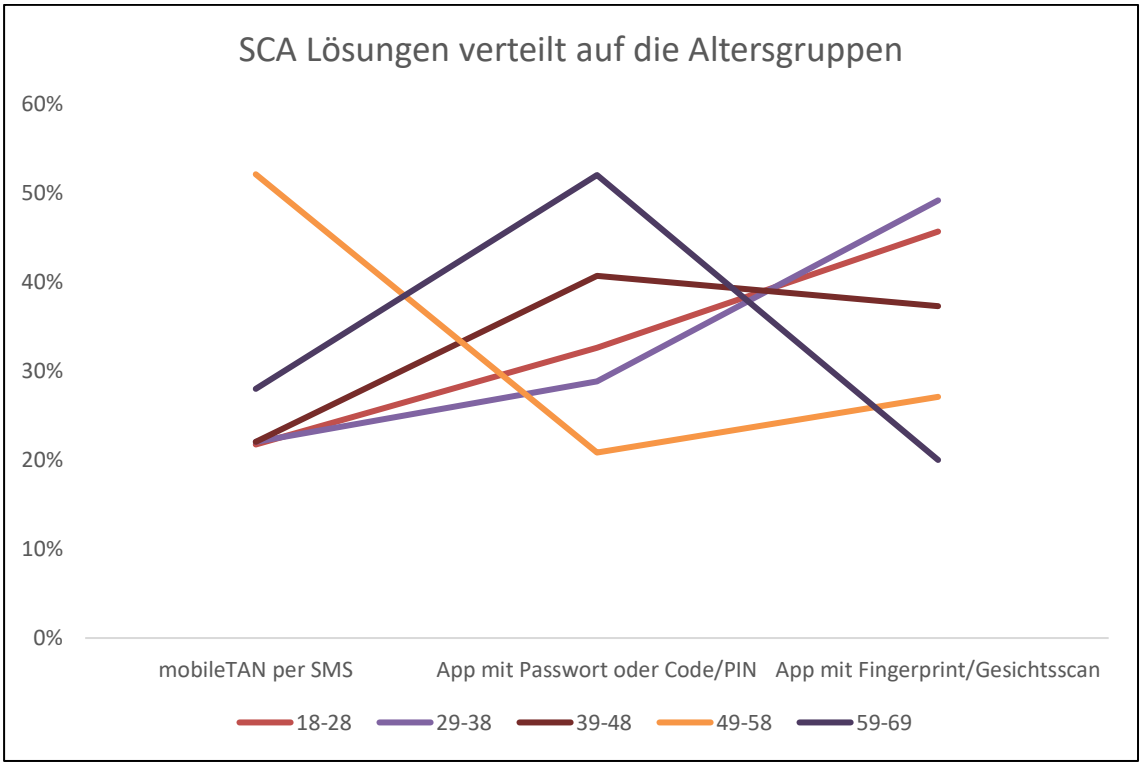


Abbildung 18: SCA Lösungen verteilt auf die Altersgruppen (Frage 4/18)

In den folgenden Abbildungen wird das Empfinden der Sicherheit, der Usability und des Vertrauens der verschiedenen SCA Lösungen näher betrachtet. Das Hauptaugenmerk dabei liegt auf das arithmetische Mittel der Bewertung von den jeweils selbst verwendeten SCA Methoden und das arithmetische Mittel der Reihung nach der Wichtigkeit von den Kriterien Sicherheit, Usability und Vertrauen. Zunächst eine Darstellung, welche die Verteilung der SCA Lösungen auf die Zahlungsdienstleister zeigt.

Die Abbildung 19 zeigt, dass jeweils über 60% der KundInnen der BAWAG P.S.K und der UniCredit Bank Austria mobileTAN Freigabemethoden verwenden. Die Raiffeisenbank und die Erste Group Bank haben zusammen über 80% ihrer KundInnen im Bereich der App-Lösungen. (siehe auch Abbildung 20) Die Freigabevarianten „App via Desktopversion“ und „cardTAN Generator“ sind schwindend gering in Verwendung und nur von der Raiffeisenbank und der Erste Group Bank angeboten.

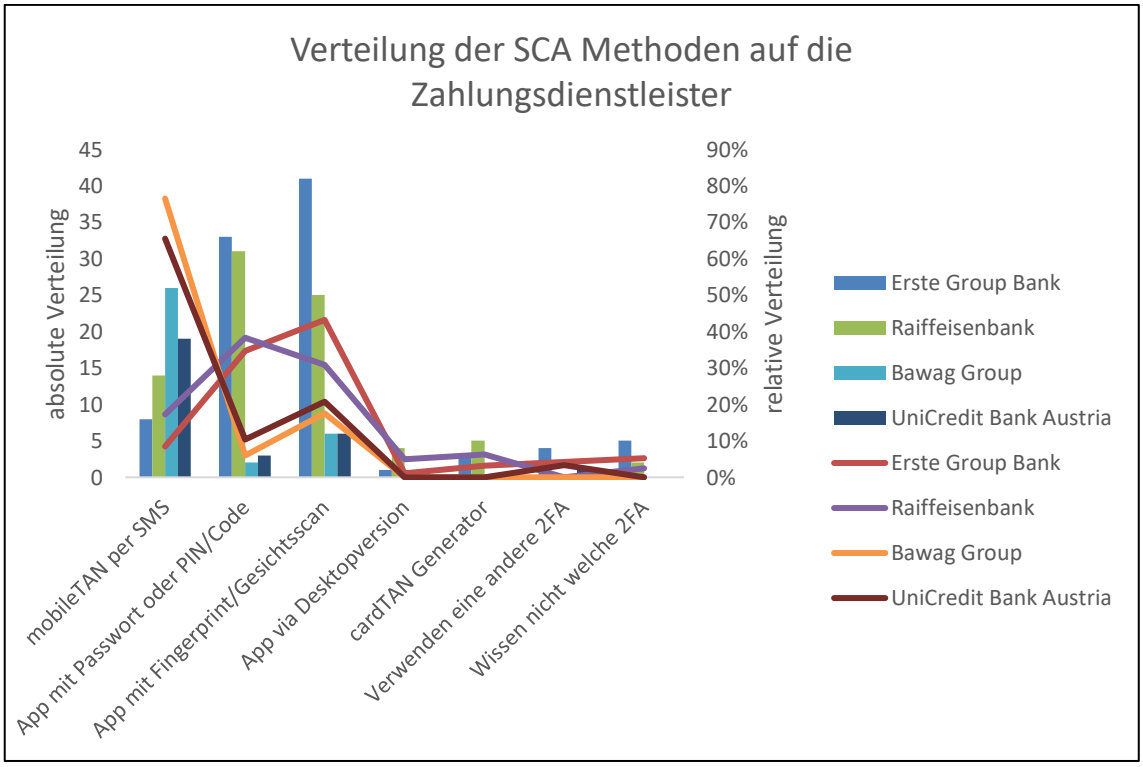


Abbildung 19: Verteilung der SCA Lösungen auf die Zahlungsdienstleister (Frage 1/5)

Ein Hauptgrund dafür ist, dass die KundInnen, welche keine App-fähigen Devices für eine Authentifizierung besitzen, bei der Erste Group Bank und die Raiffeisenbank als Alternative die App als Desktopversion oder einen cardTAN Generator verwenden können. Umgekehrt ist die verstärkte Anwendung der SCA Methoden mittels mobileTAN, erhalten durch eine SMS, eine Alternative für KundInnen ohne App-fähige Devices.

Innerhalb der drei meistgenutzten Methoden zur Authentifizierung verteilen sich die Anteile der Banken wie in Abbildung 20. Dies zeigt den deutlichen Schwerpunkte der SCA Lösungen der Zahlungsdienstleister.

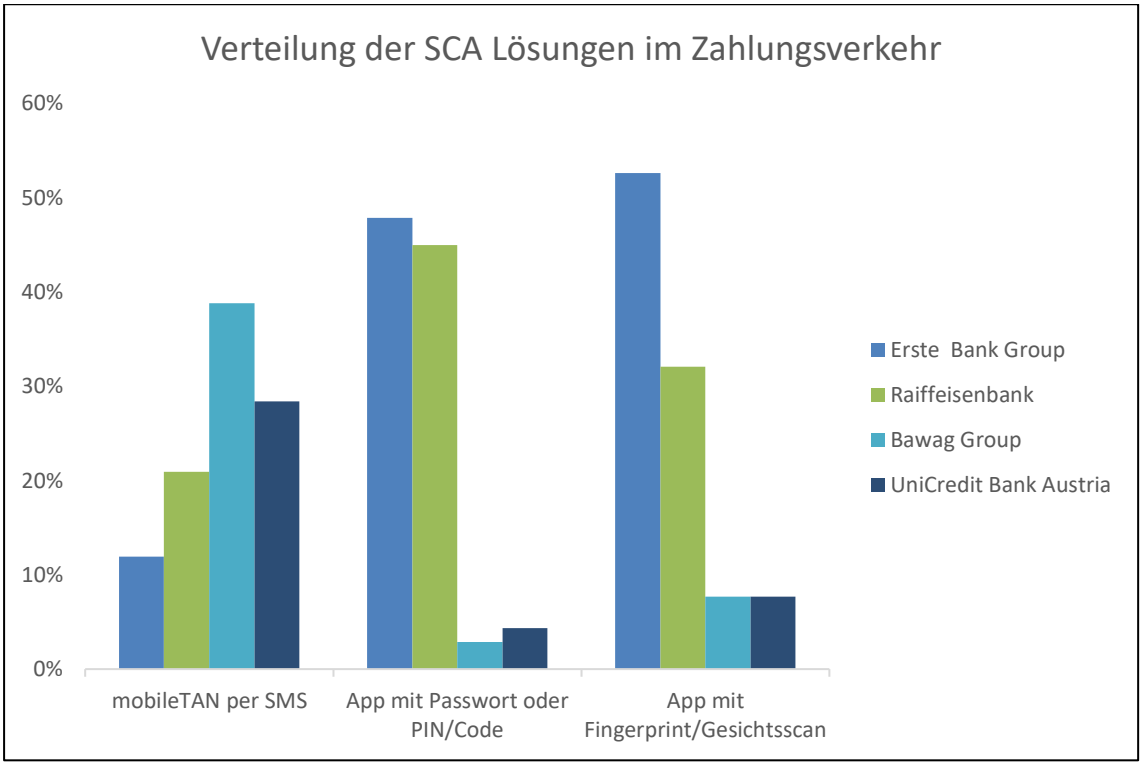


Abbildung 20: Verteilung der 2FA-Methoden auf die Zahlungsdienstleister (Frage 1/5)

SCA Lösungen mit dem Blick auf die Sicherheit, die Usability und das Vertrauen

Mit der Sicht auf die Sicherheit, das Vertrauen und die Usability zeigt sich in Abbildung 21, dass die Sicherheit bei allen drei verwendeten SCA Lösungen am wichtigsten erscheint. Gefolgt wird die Sicherheit von Usability und dem Vertrauen. Bei der Zufriedenheit sind keine Tendenzen erkennbar. Mit einer sehr guten Bewertung (annähernd durchschnittlich 1,8) bewerten die NutzerInnen ihre verwendete Lösung. Mit einem Wert (annähernd durchschnittlich 1,6) ist die Bewertung für die SCA Lösung mit der App und dem Fingerprint oder Gesichtsscan am besten. Die Bewertung der Sicherheit bei der SCA Lösung mit einer App und einem Passwort ist ungleich der Wichtigkeit des Faktors Sicherheit. In dieser Hinsicht ist Verbesserungsbedarf vorhanden.

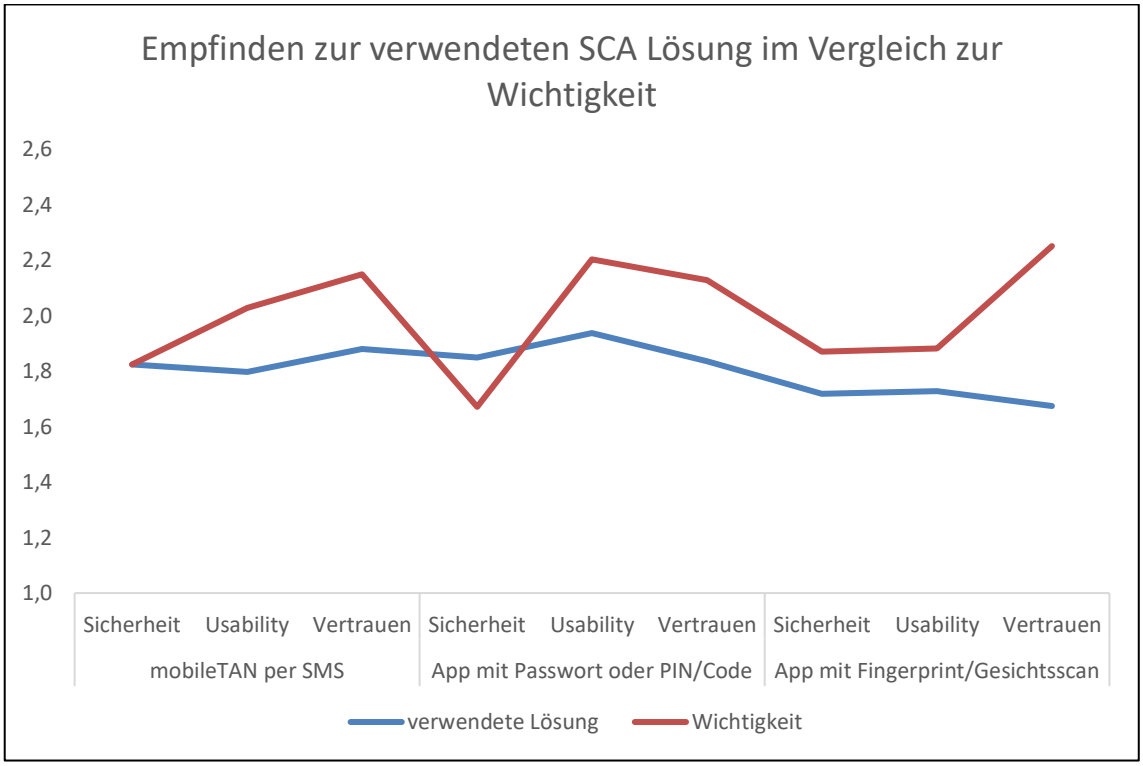


Abbildung 21: Empfinden der Sicherheit, Usability und dem Vertrauen der verwendeten SCA Lösung im Vergleich zur Wichtigkeit (Frage 5/6/9)

In der Abbildung 22 wird zum Vergleich der Bewertung mit der Wichtigkeit der einzelnen Faktoren, der Faktor Wissensstand über SCA Lösungen hinzugefügt. Es ist ein Unterschied anhand des Wissensstandes erkennbar. Jene TeilnehmerInnen, die sich besser über SCA informiert fühlen, bewerten diese Lösungen grundsätzlich besser. Ein markanter Punkt ist jedoch, dass jene, die sich weniger gut über SCA informiert fühlen, die App mit dem Passwort aus Sicht der Sicherheit besser bewerten. Aus Sicht der Wichtigkeit wird bei der Freigabe mit einer mobileTAN von den Befragten mit weniger Information über SCA die Usability an die erste Stelle gereiht. Jene, die sich besser informiert fühlen reihen bei allen SCA-Lösungen die Sicherheit an erste Stelle.

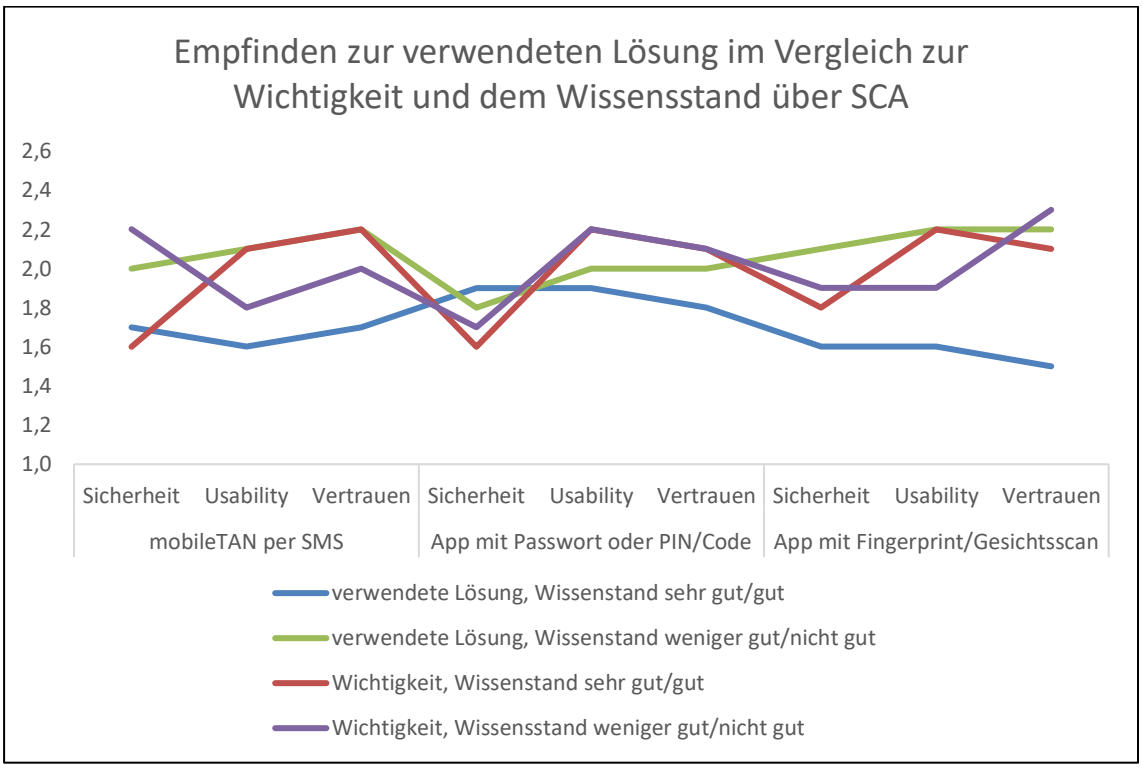


Abbildung 22: Empfinden der Sicherheit, Usability und dem Vertrauen zur verwendeten Lösung im Vergleich zur Wichtigkeit auf Basis des Wissensstandes (Frage 4/5/6/9)

Nachdem die Lösungen mit Apps vor allem bei der Erste Group Bank und bei der Raiffeisenbank in Verwendung sind, wurden diese in Abbildung 23 und Abbildung 24 direkt miteinander verglichen. Bei der App Variante mit dem Passwort ist die Beurteilung der Sicherheit und der Usability bei Erste Group Bank besser beurteilt, wohingegen hier die Raiffeisenbank mehr Vertrauen erhält. (siehe Abbildung 23)

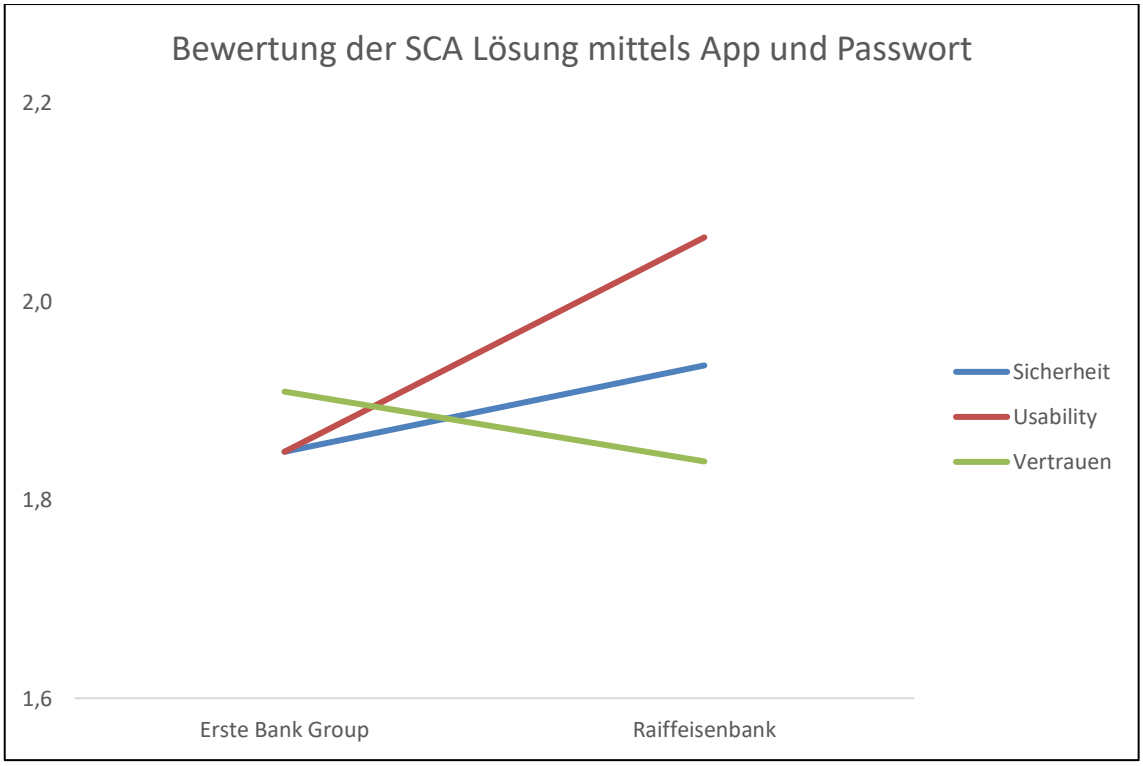


Abbildung 23: durchschnittliche Bewertung der SCA Lösung einer App mit Passwort oder PIN/Code im Vergleich der Zahlungsdienstleister (Frage 5/6)

Die TeilnehmerInnen bewerten die Lösung der Erste Group Bank, der App mit Fingerprint oder Gesichtsscan, in allen drei Merkmalen besser als die TeilnehmerInnen der Raiffeisenbank. (siehe Abbildung 24)

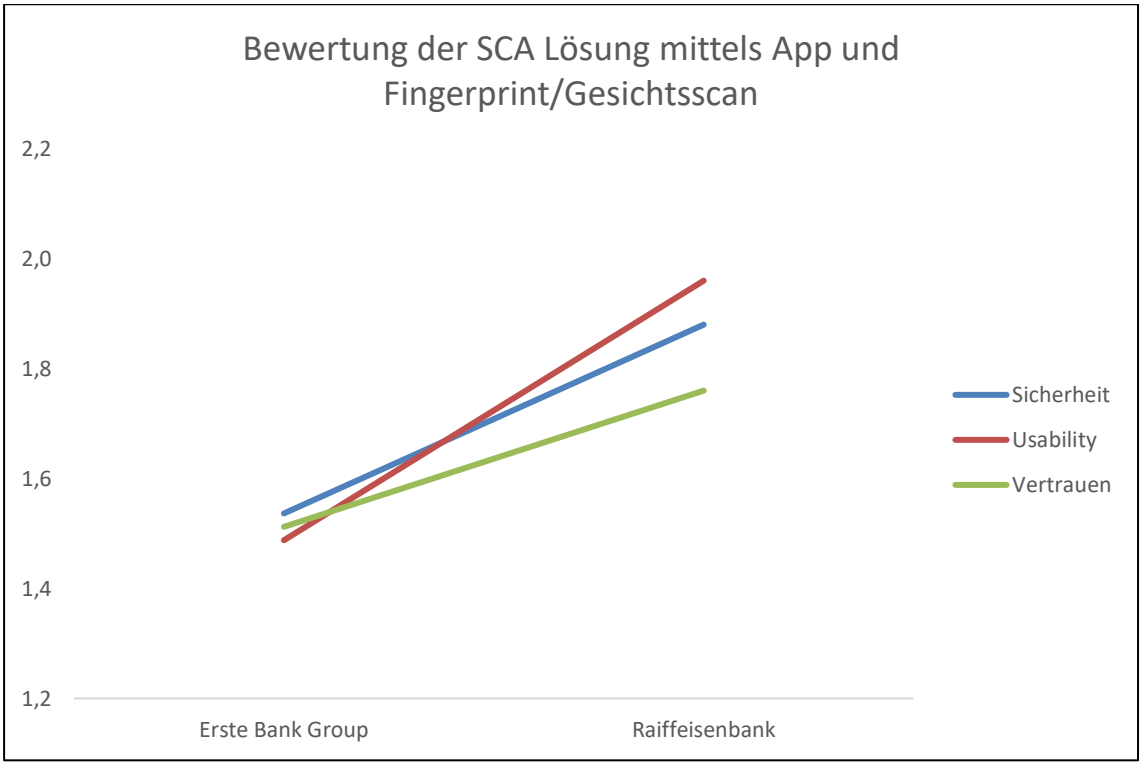


Abbildung 24: durchschnittliche Bewertung der SCA Lösung einer App mit Fingerprint/Gesichtsscan im Vergleich der Zahlungsdienstleister (Frage 5/6)

Die Abbildung 25 zeigt den direkten Vergleich der BAWAG P.S.K und der UniCredit Bank Austria, welche vorrangig die mobileTAN Lösung in Verwendung haben. Es ist ersichtlich, dass die Usability, der mobileTAN AnwenderInnen der BAWAG P.S.K am besten, gefolgt von der Sicherheit, beurteilt wird. Wohingegen die Sicherheit bei der Lösung der UniCredit Bank Austria am besten bewertet wird, gefolgt von der Usability und dem Vertrauen.

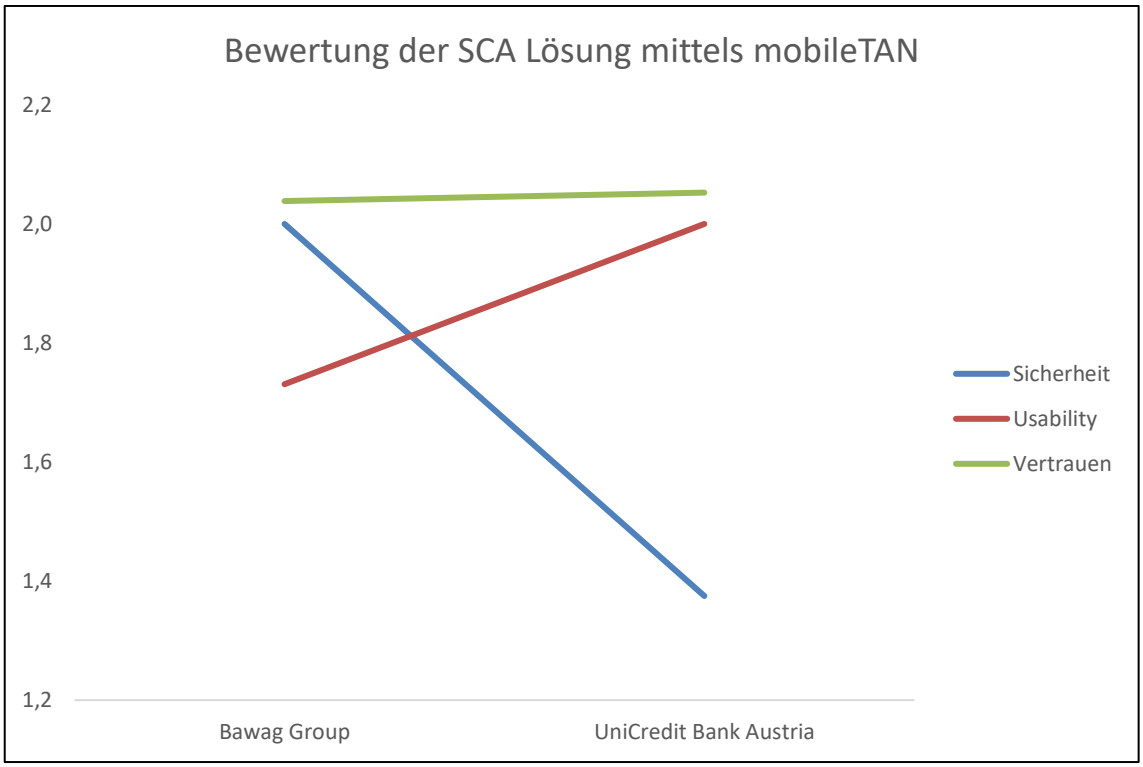


Abbildung 25: durchschnittliche Bewertung der SCA Lösung mit mobileTAN im Vergleich der Zahlungsdienstleister (Frage 5/6)

Hinzuzufügen ist, dass die Vergleiche der Abbildung 23, Abbildung 24 und Abbildung 25 den TeilnehmerInnen nicht möglich ist. Die Bewertungen beruhen auf die Wahrnehmungen der TeilnehmerInnen von 1 – sehr gut bis 4 – nicht gut.

Veränderung aufgrund der neuen SCA Lösungen

Bei der Fragestellung, in der es darum geht, ob sich NutzerInnen aufgrund der SCA Lösungen im Verhalten verändern würden, werden 75% mit „trifft nicht zu“ beantwortet. Als zweitgrößtes Antwortfeld wird die „Usability“ mit 13% als Begründung zur Veränderung angegeben. Die Sicherheit, das Vertrauen oder andere Gründe sind mit jeweils knapp 5% keine Hauptgründe das Verhalten im Rahmen der Möglichkeiten zu ändern. (siehe Abbildung 26)

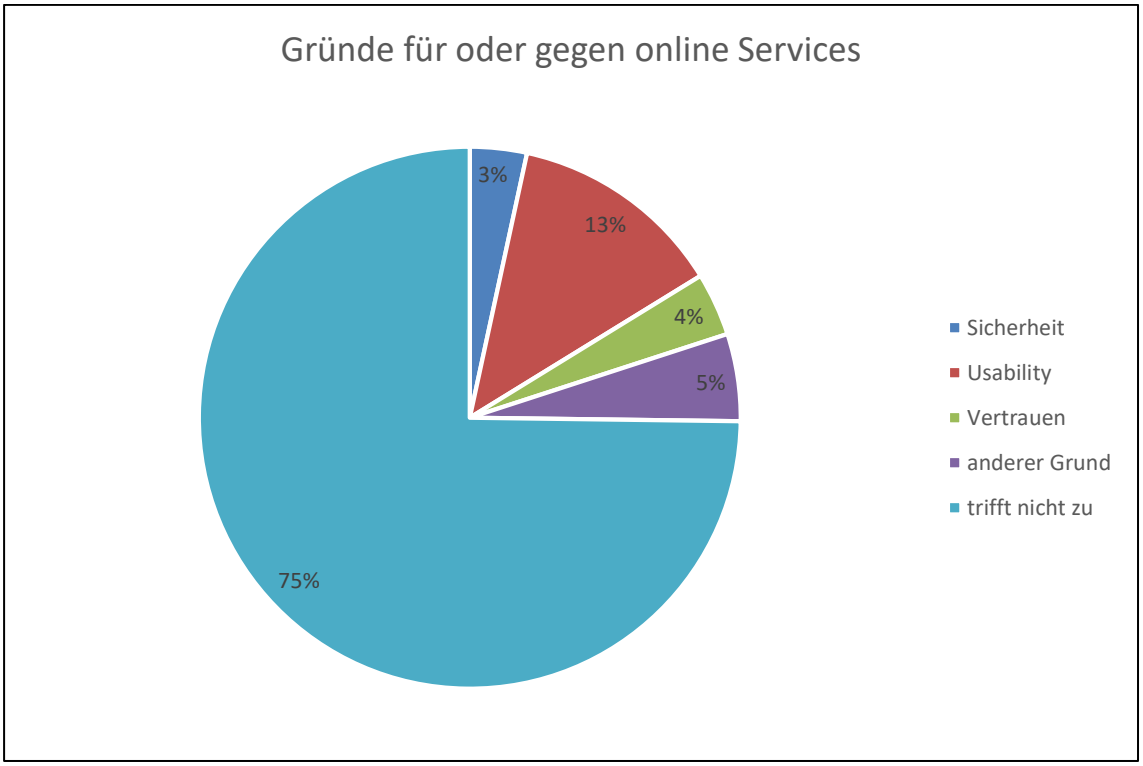


Abbildung 26: Gründe für oder gegen die Verwendung eines online Services (Frage 7)

Die Verteilung der „trifft nicht zu“ Antworten in der Abbildung 27 verteilen sich auf alle zur antwortstehenden Veränderungsmöglichkeiten nicht bedeutend unterschiedlich. Es zeigt sich daraus, dass für dreiviertel der Stichprobe

- weder der Bedarf besteht, sich an einen anderen Zahlungsdienstleister zu wenden,
- noch anstelle des bestehenden Zahlungsdienstleisters über einen Drittanbieter seine Services zu beziehen,
- noch anstelle komplexer Prozesse vermehrt auf Bargeld Transaktionen zu tätigen,
- oder die Services mehr oder weniger zu nutzen.

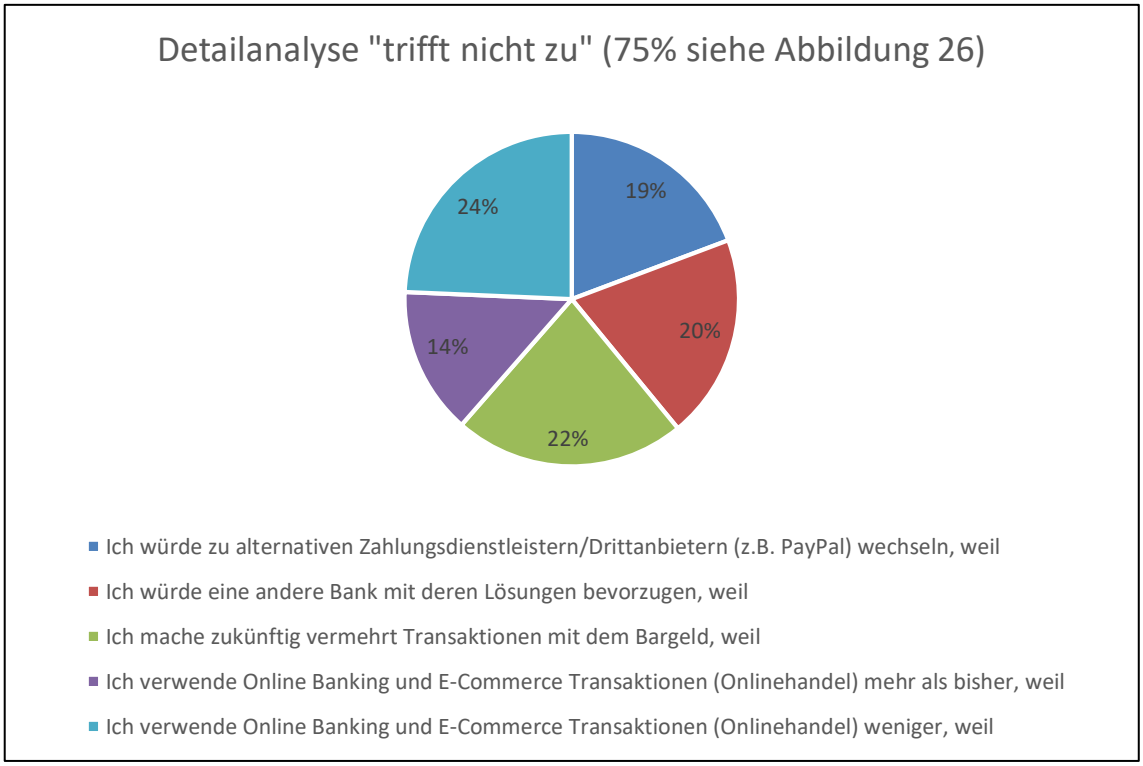


Abbildung 27: Anteile der Beweggründe etwas zu verändern, welche mit "trifft nicht zu" beantwortet wurden (Frage 7)

Im 13% großen Bereich, jener die eine Veränderung aufgrund der „Usability“ durchführen, ist ersichtlich, dass mehr als die Hälfte davon online Services seit den neuen Regelungen vermehrt verwenden. (siehe Abbildung 28)

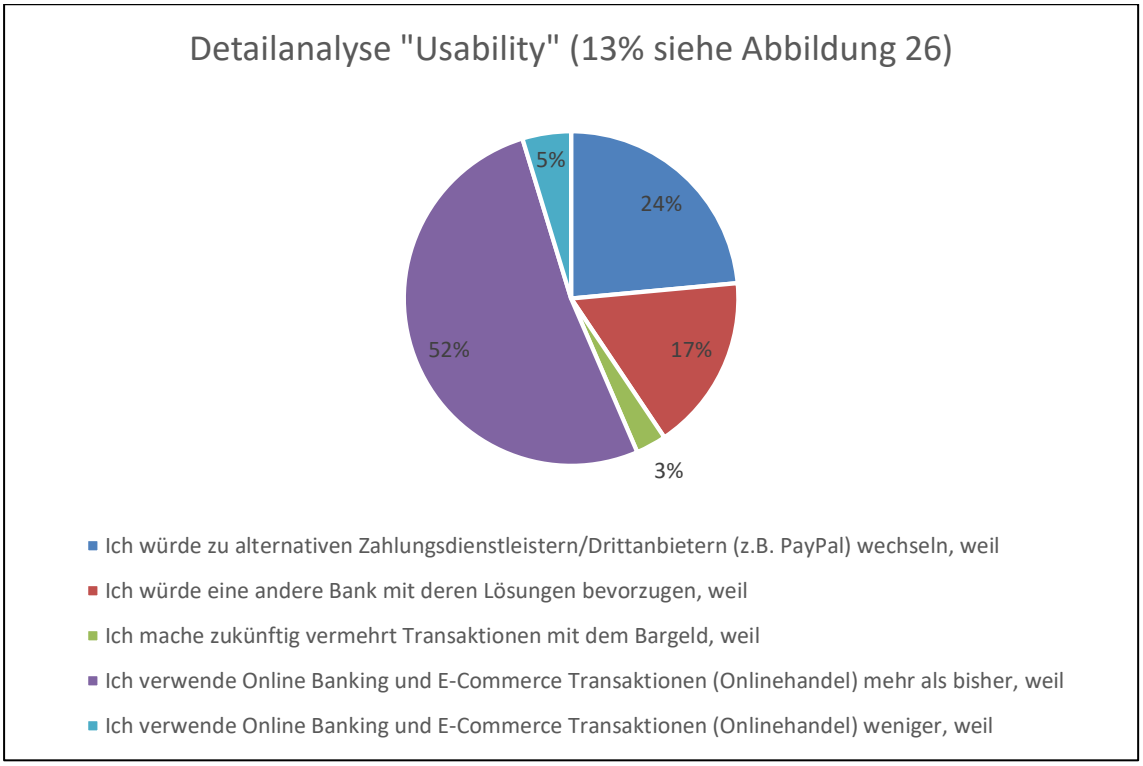


Abbildung 28: Anteile der Beweggründe etwas zu verändern, welche mit "Usability" beantwortet sind (Frage 7)

TeilnehmerInnen, welche Online Banking und E-Commerce Transaktionen aufgrund der Usability jetzt mehr verwenden, bringen folgende Merkmale mit:

- Dreiviertel davon fühlen sich sehr gut oder gut über SCA informiert
- knapp die Hälfte verwendet eine App mit Fingerprint oder Gesichtserkennung
- für diese Stichprobe ist Usability bei einem Service am wichtigsten (Durchschnitt 1,6), danach Vertrauen (1,8), knapp danach Sicherheit (1,9)

Des Weiteren zeigt sich in der Altersstruktur, dass die vermehrte Verwendung von online Services aufgrund der „Usability“ von den 18- bis 28-Jährigen bis zu den 59- bis 69-Jährigen abnimmt. Im Umkehrschluss ist festzustellen, dass die „Usability“ von online Services für eine vermehrte Benutzung in steigendem Alter abnehmenden aber positiven Einfluss hat. (siehe Abbildung 29)

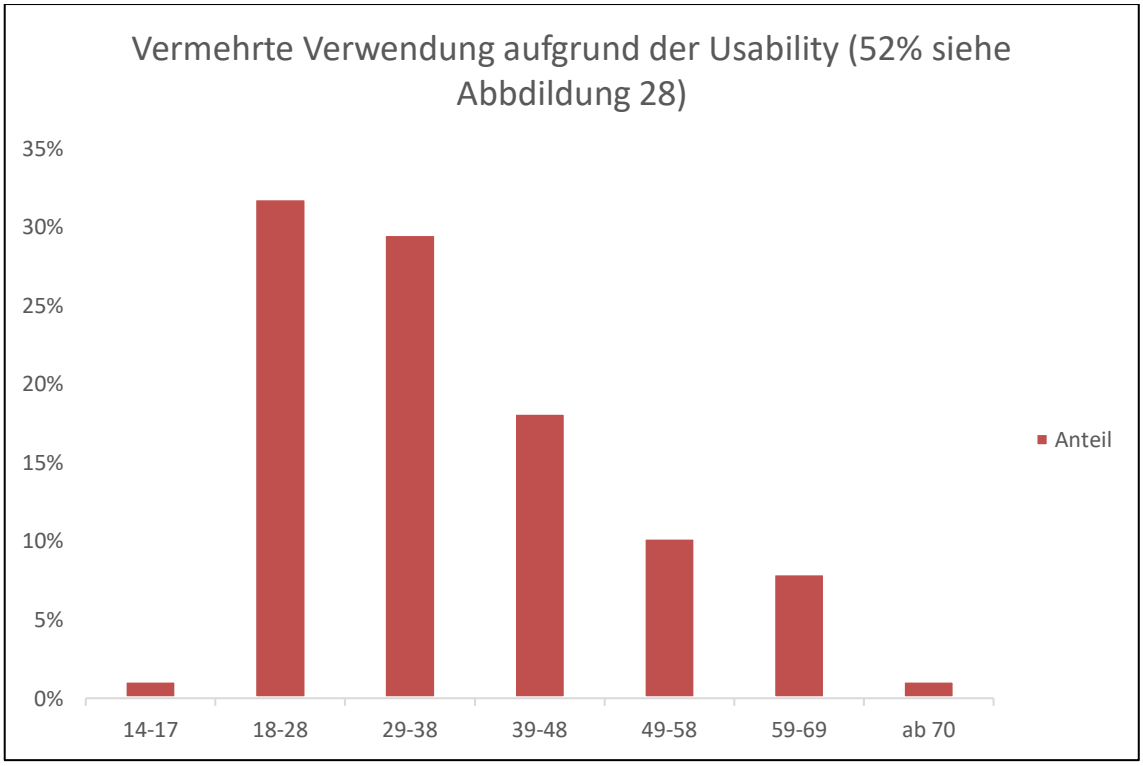


Abbildung 29: Vermehrte Verwendung von online Services, welche mit "Usability" Begründung beantwortet wurden, im Bezug zum Alter (Frage 7/18)

Im Vergleich der verschiedenen Zahlungsdienstleister hat die Erste Group Bank gefolgt von der Raiffeisenbank den größten Zuspruch, wenn es darum geht online Services aus Sicht der „Usability“ mehr als bisher zu nutzen. (siehe Abbildung 30)

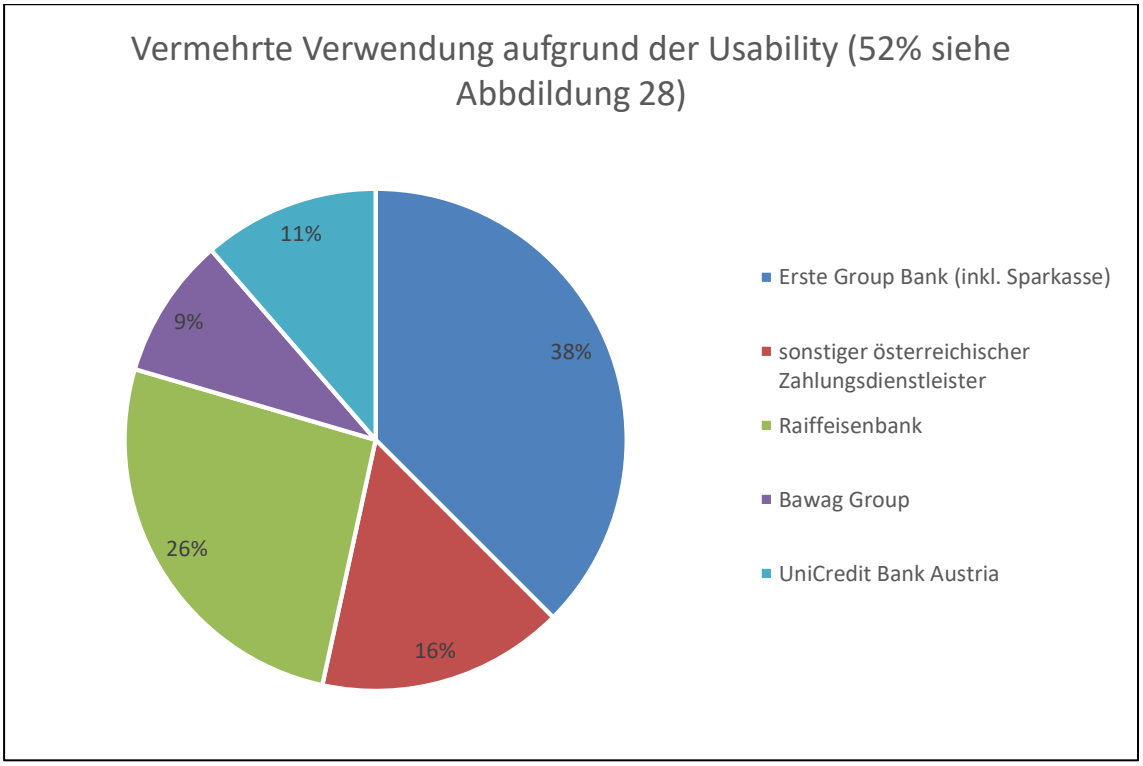


Abbildung 30: Vermehrte Verwendung von online Services, welche mit "Usability" beantwortet wurden, im Bezug zum Zahlungsdienstleister (Frage 1/7)

Jene TeilnehmerInnen, die aus „Usability“ Gründen die online Services mehr nutzen, kommen nicht aus der Finanzbranche sondern mit rd. 50% aus anderen beruflichen Tätigkeitsfeldern. Gefolgt mit rd. 30% jener, welche in der Finanzbranche tätig sind. (siehe Abbildung 31)

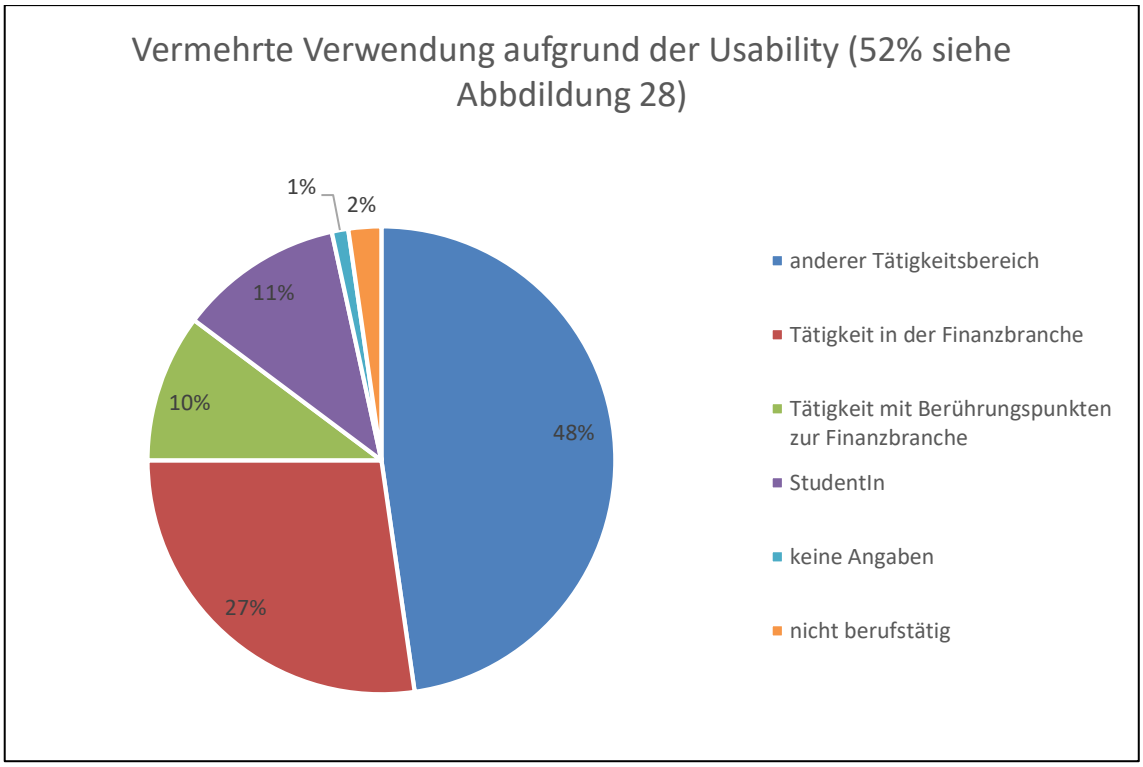


Abbildung 31: Vermehrte Verwendung von online Services, welche mit "Usability" beantwortet wurden, im Bezug zum Tätigkeitsfeld (Frage 7/21)

Die TeilnehmerInnen haben die Ausnahmen wie folgt beurteilt: Rund ein Drittel beurteilt diese als „gut“, um den NutzerInnen den SCA Prozess zu erleichtern. Ein relevanter Teil konnte diese Ausnahmen nicht beurteilen. (siehe Abbildung 32)

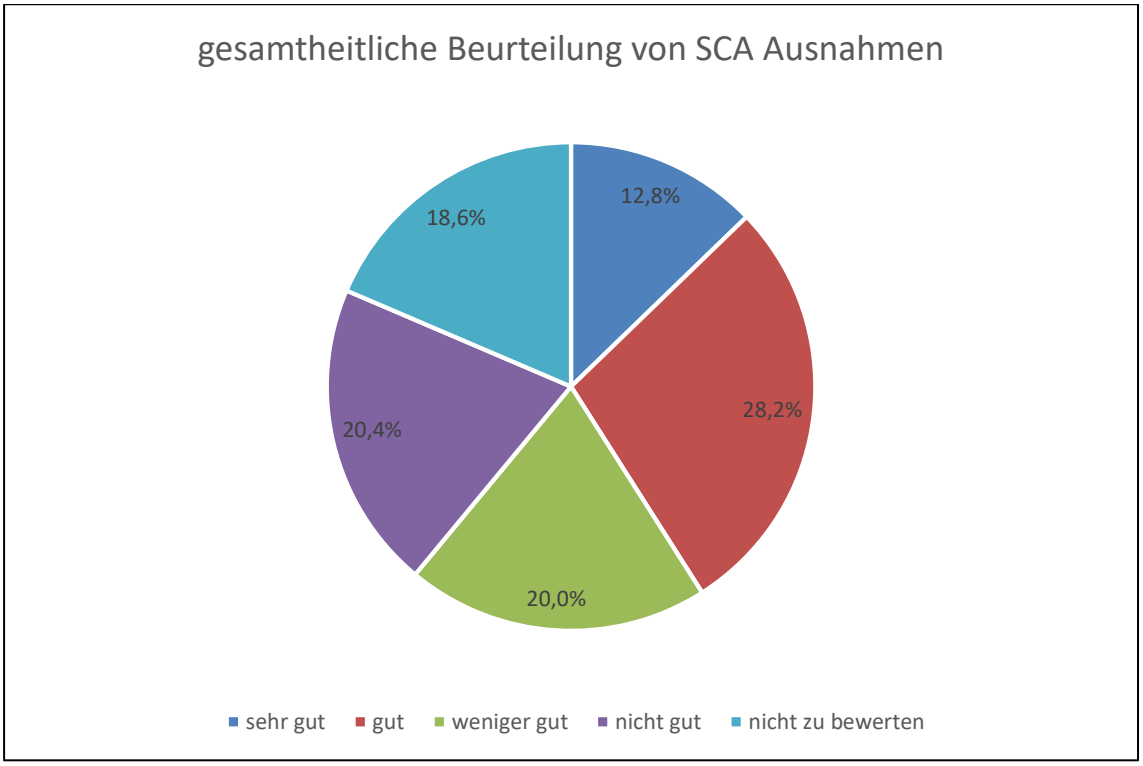


Abbildung 32: Beurteilung von SCA Ausnahmen (Frage 8)

Nachdem 26% einen Entfall von SCA in Form von Whitelisting nicht bewerten können, ist daraus zu schließen, dass hierzu noch keine Erfahrungswerte vorhanden sind. Am besten beurteilt ist der Verzicht von SCA bei gleichbleibenden Folgetransaktionen, gefolgt vom Verzicht auf SCA bei Kleinstbetragszahlungen. Mit 40% ist dennoch fast jeder/jede Zweite gegen eine SCA Ausnahme bei Kleinstbetragszahlungen. Ein Drittel beurteilt die SCA Ausnahme von wiederkehrenden Folgetransaktionen negativ. (siehe Abbildung 33)

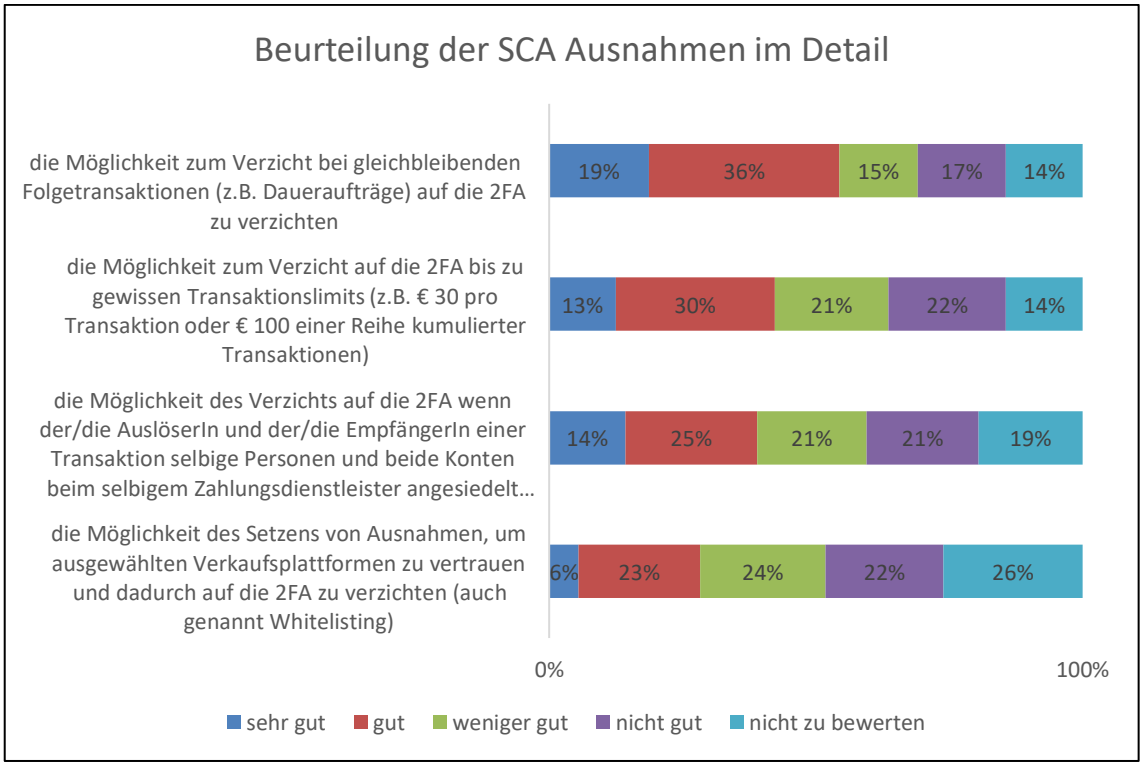


Abbildung 33: Beurteilung der SCA Ausnahmen im Detail (Frage 8)

4.3.4 Open Banking

In der Abbildung 34 ist ersichtlich, dass der überwiegende Teil der Stichprobe sich nicht gut über Open Banking informiert fühlt. Daher liegt der Schwerpunkt der weiteren Analysen in Richtung jener, die sich nicht gut informiert fühlen.

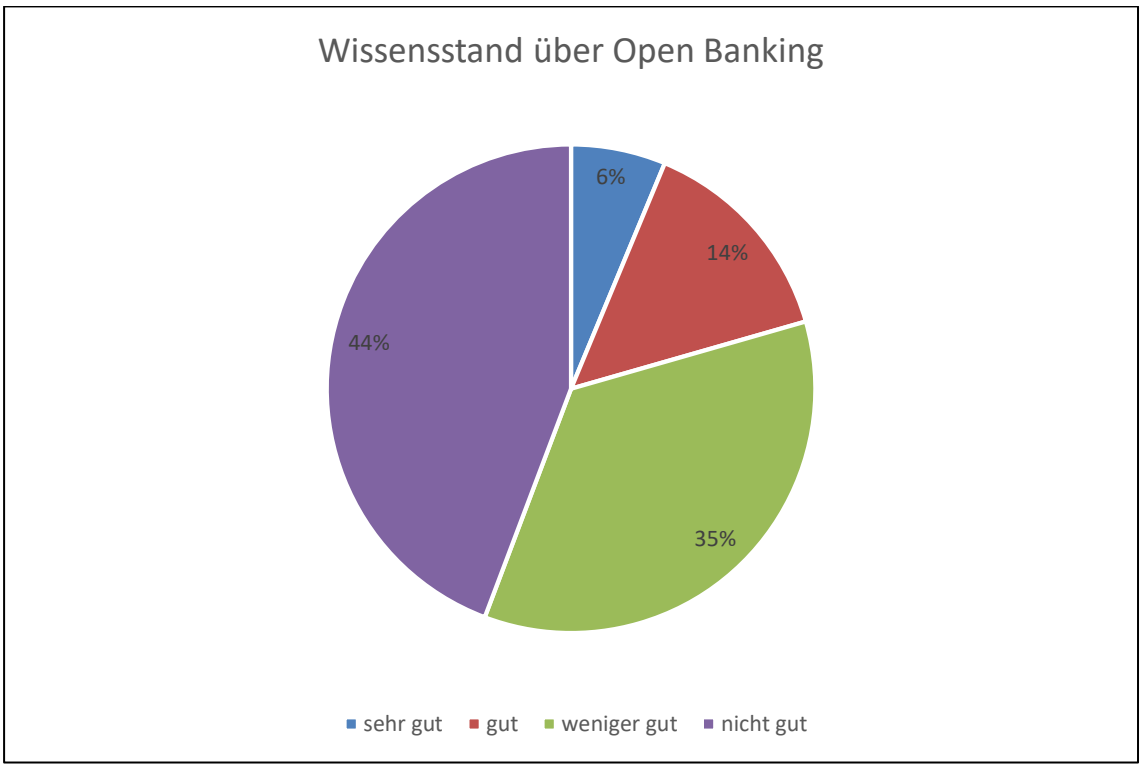


Abbildung 34: Wissensstand über Open Banking (Frage 10)

Zur übersichtlicheren Darstellungen in den Abbildungen und Tabellen wird anstelle der Kontoinformationsdienste die Kurzform AISP und anstelle der Zahlungsauslösedienste die Kurzform PISP verwendet. Auf TeilnehmerInnen mit wenig oder keinem Vorwissen zu Open Banking reduziert, ist ersichtlich, dass trotzdem 49% die Zahlungsauslösedienste im Bereich Open Banking verwenden. Knapp 40% sind an Zahlungsinformationsdiensten interessiert. (siehe Tabelle 16)

Verwendung von Open Banking	**AISP**		**PISP**	
	Anzahl	**Anteil**	**Anzahl**	**Anteil**
Ja, verwende ich	12	6%	104	49%
Nein, bin auch nicht daran interessiert	84	39%	14	7%
Nein, lehne ich ab	118	55%	96	45%
Summe	**214**	**100%**	**214**	**100%**

Tabelle 17: Verwendung von Open Banking, weniger/nicht gut informierter Personen (Frage 10/11/12)

Es zeigt sich, dass die Ablehnungen für Kontoinformationsdienste nicht unmittelbar auf die Sicherheit, die Usability oder das Vertrauen zurückzuführen sind. Über 70% geben auch oder zusätzlich andere Gründe an. Diese Frage ermöglichte eine Mehrfachantwort. (siehe Tabelle 18)

Gründe für keine Verwendung, aber Interesse an AISPs	**Anzahl**	**Anteil**
Sicherheitsgefühl	9	11%
Usability	12	14%
Vertrauen	11	13%
Andere Gründe	60	71%
Summe	**92**	**100%**

Tabelle 18: Gründe gegen die Verwendung, aber Interesse an AISPs (Frage 11/13)

Jener Teil, welcher Zahlungsauslösedienste im Bereich Open Banking nutzt, bewertet die Usability am besten, gefolgt von Vertrauen und Sicherheit. (siehe Tabelle 19)

Ja, ich verwende PISPs	**arithmetisches Mittel**	
	Sehr gut (1)	Nicht gut (4)
Sicherheitsgefühl	2,1	
Usability	1,7	
Vertrauen	2,0	

Tabelle 19: Beurteilung von PISPs (Frage 14/15)

In Tabelle 20 ist zusammengefasst, welche Merkmale die NutzerInnen, welche Services im Bereich des Open Bankings prinzipiell ablehnen, erfüllen.

Verwendung von PISP und AISP abgelehnt	**Anzahl**	**Anteil**
Fühlen sich nicht gut über Open Banking informiert	45	58%
Nehmen kein vermehrtes Angebot seit 2019 war	68	88%
Wohnhaft in ländlicher Region	42	55%
Tätigkeit außerhalb der Finanzbranche	43	56%
Tätigkeit in der Finanzbranche	12	16%

Tabelle 20: Charakterisierung der Open Banking ablehnenden TeilnehmerInnen

Die Abbildung 35 gibt Aufschluss darüber, ob sich die Verwendung im Vergleich zwischen den Zahlungsdienstleistern unterscheiden. Mit knapp 70%, und daher um 20% mehr als alle anderen Zahlungsdienstleister, nutzen KundInnen der UniCredit Bank Austria Zahlungsauslösedienste. Andere Unterscheidungen gibt es im Bereich Open Banking zwischen den Zahlungsdienstleistern nicht.

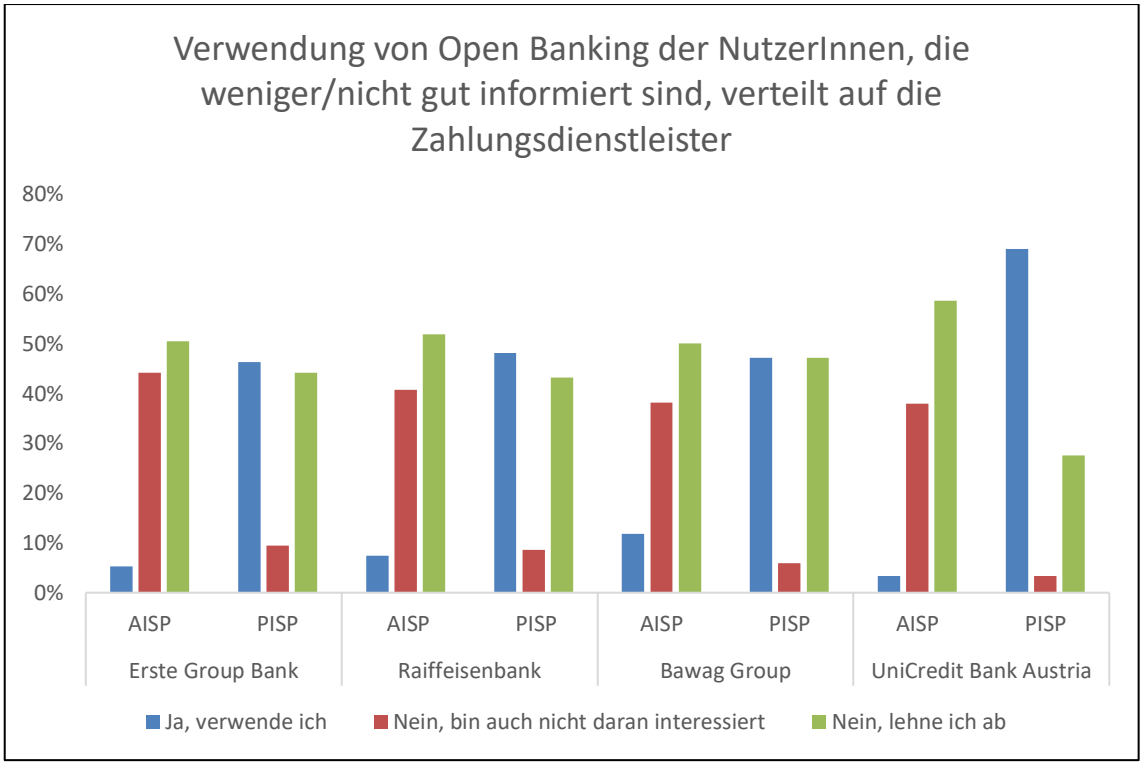


Abbildung 35: Verwendung von Open Banking der NutzerInnen, die weniger/nicht gut informiert sind, verteilt auf die Zahlungsdienstleister (Frage 1/11/14)

5. Erkenntnisse der wissenschaftlichen Arbeit

Aufbauend auf die Ergebnisse der Auswertung in Kapitel 4 werden nachfolgend die Erkenntnisse zusammengefasst. Das Hauptziel dieser Masterarbeit ist die Beantwortung, der an Beginn gestellten Forschungsfrage:

Wie wirken sich die Veränderungen der PSD2 auf die NutzerInnen im österreichischen Zahlungsverkehr aus?

Zunächst wurde die Forschungsfrage zerlegt, um die einzelnen Inhalte hervorzuheben:

- **„Wie“** erfragt einen Grad in dem sich etwas befindet oder etwas geschieht
- **„wirkt sich … aus“** evaluiert die Wahrnehmung, das Empfinden, den Informationsstatus und die Konsequenzen des Themas
- **„Veränderungen“** zeigen einen Wechsel von Anwendungen, eine Weiterentwicklung oder die Notwendigkeit sich an Entwicklungen anzupassen
- **„PSD2“** ist der Begriff für das inhaltliche Kernthema, welches Open Banking und SCA beinhaltet
- **„NutzerInnen“** definieren die Sichtweise, aus welcher auf das Thema Bezug genommen wird
- **„österreichischer Zahlungsverkehr“** ist die örtliche Abgrenzung auf die Bezug genommen wird, nachdem es sich um kein global gleichbehandeltes Thema handelt

5.1 Kaum eine Auswirkungen der PSD2

Für die TeilnehmerInnen, welche keine online Services der Zahlungsdienstleister nutzen, hat die PSD2 kaum Auswirkungen. Diese Personengruppe, von 5% in der Stichprobe, kann nur im Zusammenhang mit kartenbasierten Transaktionen Berührungspunkte haben (z.B. an einem POS Terminal im Supermarkt).

5.2 Auswirkungen der PSD2

Wie: Von TAN-Listen, Zugriffsmöglichkeiten auf Zahlungskonten ohne einem zweiten Faktor, keiner Smartphone Notwendigkeit für Zahlungsfreigaben oder direktem Kontakt mit den Zahlungsdienstleistern, hat sich der Zahlungsverkehr durch Open Banking zu einem umworbenen, für Drittanbieter zugänglichen Markt, weiterentwickelt.

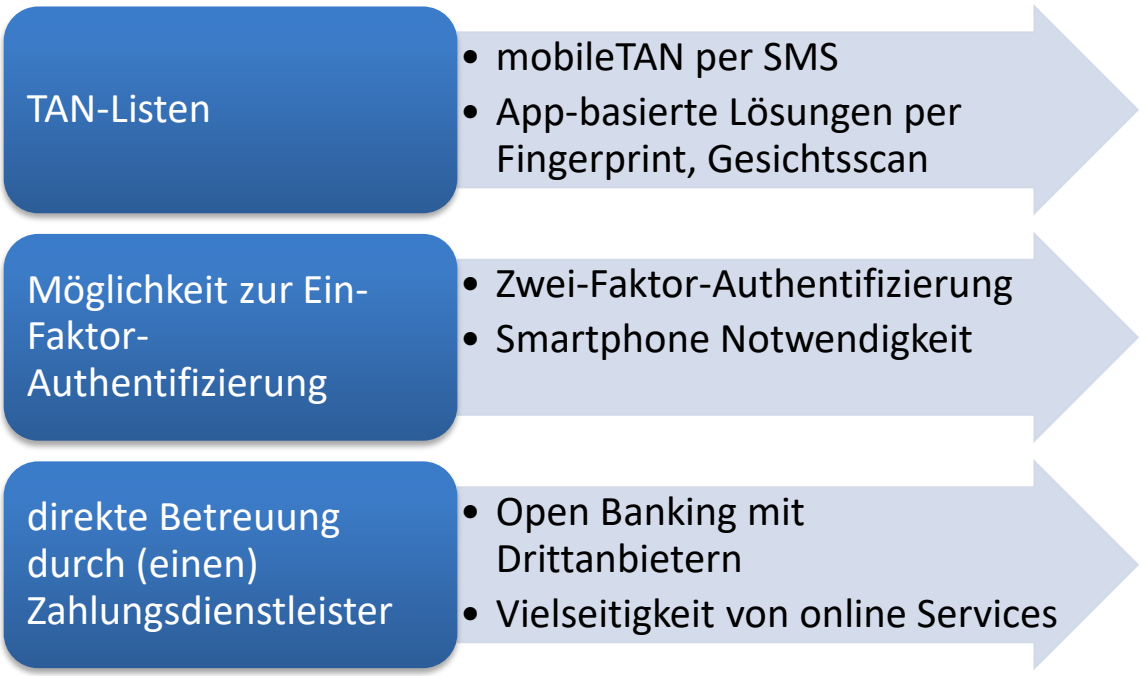


Abbildung 36: Veränderungen im Überblick

Österreichische Zahlungsdienstleister haben bis zum Ende des Jahres 2020 noch Zeit, alle Services, welche Zugriff auf Zahlungskonten, die elektronische

Zahlungsvorgänge auslösen und etwaige Fernzugänge anbieten, SCA Funktionalitäten umzusetzen. Die Stichprobe zeigt, dass der Trend der SCA Lösungen in Richtung App-basierte tendiert. Als zweithäufigste Methode, wird die mobileTAN, die per SMS zugestellt wird, angeboten.

Seitens Open Banking wird das Ziel verfolgt, Drittanbietern den Markt zu öffnen, indem Zahlungsdienstleister API Schnittstellen zur Verfügung stellen müssen. Diese werden durch Drittanbieter für das Auslösen von Zahlungen oder das Einholen von Kontoinformationen genutzt. Dadurch entwickeln sich Möglichkeiten der Vergleichbarkeit, zielgerichteter Angebote und schnellere Abwicklungen für die Stakeholder des Zahlungsverkehrs.

Wirkt sich … aus: Auswirkungen auf die NutzerInnen unterscheiden sich beim Alter, der Herkunft und der Berufstätigkeit. Ein weiterer Unterschied besteht darin, bei welchem Zahlungsdienstleister die NutzerInnen ihre Zahlungsgeschäfte abwickeln.

70% der TeilnehmerInnen haben angegeben, dass sie sich sehr gut oder gut über die SCA Methode ihres Zahlungsdienstleisters informiert fühlen. Daraus ist zu erkennen, dass die Zahlungsdienstleister viel Information und Unterstützung angeboten haben. (siehe Abbildung 16)

Das Gegenteil zeigt sich im Bereich von Open Banking. Es sind über 70% TeilnehmerInnen, die angeben sich wenig oder nicht gut über die Möglichkeiten von Open Banking informiert zu fühlen. In Anbetracht dessen, dass NutzerInnen unter nachweisbarer Fahrlässigkeit einen Teil der Haftung von Geschehnissen übernehmen müssen, nehmen sie dazu verhältnismäßig wenig Informationen wahr. (siehe Abbildung 34)

Veränderungen: Bereits 74% der TeilnehmerInnen nutzen Smartphones oder Tablets für ihre online Services der Zahlungsdienstleister. 87 % nutzen den Computer für ihre Services. Es geben über 25% der TeilnehmerInnen an, ihr

Smartphone oder Tablet sogar mehrmals die Woche für online Services ihres Zahlungsdienstleisters zu nutzen. Entsprechend einer Studie von Eurostat waren es im Jahr 2018 noch 58% der ÖsterreicherInnen, die Online Banking benutzten. (Brandt, 2019) In diesem Zusammenhang zeigt sich ein Verlauf, dass mit der steigenden Häufigkeit, der mobilen Zugriffe auf online Services, die Zugriffe über den PC sinken. (siehe Abbildung 15)

Die mobileTAN Lösungen sind vorrangig bei der BAWAG P.S.K und der UniCredit Bank Austria in Verwendung. Diese Lösung ist vor allem bei älteren Altersgruppen und Personen, welche weniger über die PSD2 sowie SCA informiert sind, in Verwendung. Wenn hier das Bestreben der Zahlungsdienstleister vollständig auf App-basierte Lösungen umzusteigen vorhanden ist, muss dieser Zielgruppe besondere Unterstützung zukommen. Nachdem die TeilnehmerInnen, welche sich besser über SCA informiert fühlen bereits App-basierte Lösungen nutzen und jene, die sich weniger informiert fühlen mobileTAN Lösungen bevorzugen, ist der Wissensstand ein wichtiges Thema in einer möglichen Ablöse der mobileTAN.

In der Theorie ist ein Versand einer mobileTAN jedoch nicht sicherer als App-basierte Lösungen. Es kann jedoch die PSD2 Konformität, die Kommunikationsprozesse zu jederzeit kontrollieren zu können, bei App-basierten Lösungen eingehalten werden. (siehe Kapitel 3.5)

Das Empfinden der jeweils verwendeten SCA Lösung der TeilnehmerInnen erreicht einen guten Durchschnitt von 1,8, bei Antwortmöglichkeiten von 1 = sehr gut bis 4 = nicht gut. Im Vergleich zur Reihung der Wichtigkeit von Sicherheit, Usability und Vertrauen ist ersichtlich, dass das subjektive Empfinden daher immer vor der Wichtigkeit erscheint. Bei der App-basierten Lösung mit Passwort oder PIN/Code gibt es eine Ausnahme, bei der die Sicherheit am wichtigsten ist und dem Empfinden der TeilnehmerInnen im Vergleich zur Wichtigkeit weniger entspricht. (siehe Abbildung 21)

Wie bei den verschiedenen SCA Lösungen erwähnt, spielt der Wissensstand auch bei der Beurteilung von SCA Lösungen eine wichtige Rolle. Allgemein werden Lösungen besser bewertet, je besser man sich informiert fühlt. Die Auswirkung auf die Sicherheit ist bei höherer Kenntnis über SCA am wichtigsten. Diese TeilnehmerInnen haben bei jeder der drei meistverwendeten SCA Lösungen Sicherheit an erster Stelle gereiht. Bei der mobileTAN, diese wird vermehrt bei weniger Wissensstand über SCA verwendet. Diesen TeilnehmerInnen ist die Usability am wichtigsten. (siehe Abbildung 22)

Zwischen den Zahlungsdienstleistern sind unterschiedliche Auswirkungen ersichtlich. Im Vergleich zwischen der Raiffeisenbank und der Erste Group Bank, welche schwerpunktmäßig dieselben Lösungen verwenden und eine ähnliche Stichprobengröße aufweisen, ist das Empfinden der TeilnehmerInnen bezüglich Sicherheit, Usability und Vertrauen allgemein besser beurteilt als bei der Raiffeisenbank. Sowohl bei Apps in Passwort Kombinationen als auch bei Fingerprint/Gesichtsscan wird bei der Raiffeisenbank das Vertrauen am besten beurteilt. Wohingegen in beiden App-basierten Varianten die Usability bei der Erste Group Bank am besten beurteilt wird. (siehe Abbildung 23 und Abbildung 24) Die mobileTAN ist vermehrt bei der BAWAG P.S.K und der UniCredit Bank Austria in Verwendung. Aus Sicht der BAWAG P.S.K beurteilen die TeilnehmerInnen die Usability besser. Hingegen die TeilnehmerInnen der UniCredit Bank Austria die Sicherheit deutlich besser beurteilen. (siehe Abbildung 25) Die Beurteilungen wirken gesamtheitlich besser als Medial angedeutet. (siehe Einleitung Kapitel 3) Die Auswirkung der SCA hat gute Bewertungen. Es gibt keinen Durchschnitt mit der Tendenz zu weniger gut oder nicht gut.

Interessanterweise werden die SCA Ausnahmen, welche den KundInnen den Transaktionsprozess erleichtern, nicht mit voller Überzeugung positiv bewertet. Sie werden mit bis zu 40% als weniger oder nicht gut beurteilt. Und das obwohl der Zahlungsdienstleister für Transaktionen unter SCA Ausnahmen haftet, also das Risiko im Betrugsfall übernimmt.

Im Rahmen von Open Banking ist auffällig, dass sich 75% der NutzerInnen wenig bis gar nicht gut informiert fühlen. Insgesamt nutzen 55% der TeilnehmerInnen kein Kontoinformationsservice und 45% der TeilnehmerInnen kein Zahlungsauslöseservice. Der Zusammenhang zwischen subjektiven Informationsstand und Häufigkeit der Nutzung ist offensichtlich. Jene TeilnehmerInnen, die keine Kontoinformationsdienste nutzen, aber Interesse daran hätten, haben andere Gründe als die Sicherheit, die Usability oder das Vertrauen, dies nicht zu verwenden. Eine andere Begründung könnte z.B. fehlende Information über das Angebot sein. (siehe Kapitel 4.3.4) Zum Schutz der VerbraucherInnen gibt die Richtlinie vor, dass eine Beweislast für Reklamations- oder Betrugsfälle, die den VerbraucherInnen schaden können, immer beim Zahlungsdienstleister und Drittanbieter liegt.

Wie das Kapitel 3.4.9 zeigt, sind Kontoinformationsdienste sowie Zahlungsauslösedienste noch nicht bekannt. Es ist trotzdem wichtig zu beachten, dass bei Open Banking von den NutzerInnen immer zugestimmt werden muss, bevor Zahlungsauslösedienste und Kontoinformationsdienste Transaktionen durchführen. Drittanbieter dürfen nur die für Transaktionen notwendigen sensiblen Daten verarbeiten. Für diese gilt die DSGVO.

6. Conclusio und Ausblick

Im ersten Abschnitt dieser Masterarbeit wurde eine umfassende Literatur Recherche vorgenommen. Dabei wurde die Problemstellung mit der Einführung der PSD2 erläutert. Die mit der PSD2 in Verbindung stehenden Auswirkungen, SCA und Open Banking, wurden in den Kapiteln 3.1 bis 3.3 aufgearbeitet. Im Kapitel 3.4 wurde anhand von Testtransaktionen der Ablauf verschiedener SCA-Freigabemethoden beschrieben. Abschließend wurden in diesem Abschnitt die Erkenntnisse der Theorie und der Testtransaktionen zusammengefasst.

In weiterer Folge wurde ein online Fragebogen erstellt, in welchem Teile der Erkenntnisse aus der Theorie eingeflossen sind. Dieser Fragebogen evaluierte die Auswirkungen der PSD2 auf die NutzerInnen. Er besteht aus vier Teilen: ein „PSD2-Allgemein"-Teil, ein „SCA"-Teil, ein „Open Banking"-Teil und ein „Demographie"-Teil.

Die Stichprobe, welche ein repräsentatives Ergebnis abbildet, besteht aus 271 Personen. Zwei Drittel haben zumindest von der PSD2 gehört oder kennen diese und zwei Drittel fühlen sich über die SCA Methoden gut bis sehr gut informiert.

Open Banking ist unter den NutzerInnen noch nicht sehr verbreitet, dreiviertel kennen sich damit wenig bis nicht gut aus. Hinzugefügt sei, dass Open Banking nicht den standardmäßigen Gebrauch von online Services darstellt, da hier eine aktive Nutzung von NutzerInnen vorausgesetzt wird, wohingegen SCA den Alltag im Zahlungsverkehr begleitet.

Die einleitenden Artikel am Beginn von Kapitel 3, von welchen die Mehrheit in den Medien Befürchtungen zur Usability und die Kritik der NutzerInnen zu den neuen Lösungen hervorheben, können zum Stand der Umfrage im Frühjahr 2020 nicht bestätigt werden. Die Absichten der EBA, die Services im Zahlungsverkehr sicherer zu machen, wurden auch von dieser Stichprobe so empfunden. Durch die Öffnung von Konten den Wettbewerb zu erhöhen, ist derzeit noch nicht wahrzunehmen, da

der überwiegende Teil der Stichprobe die Möglichkeiten von Open Banking noch nicht kennt.

Was in dieser Forschungsarbeit in Bezug auf Open Banking und SCA nicht bearbeitet wurde, jedoch Material für eine zukünftige Forschung bieten würde:

- Wollen die Zahlungsdienstleister Open Banking in dieser Art und Weise fördern? Die Angebote dazu sind zum Zeitpunkt der Erstellung der Masterarbeit sehr sparsam.
- In wie weit fördern diese Maßnahmen der Richtlinie vor allem FinTechs wie Google, Apple oder Amazon?
- Sind die Betrugsfälle mit SCA jetzt fallend, steigend oder das Verhältnis von Betrugsfällen im Vergleich zu den NutzerInnen gleichbleibend?
- Wie wirken sich die Entwicklungen auf die vieldiskutierte DSGVO aus?

Nachdem dieser Bereich im Zahlungsverkehr sehr vielseitig, komplex und sehr fortschrittlich ist, gibt es weiterhin Bedarf die Vorschriften und deren Lösungen zu bearbeiten.

Literaturverzeichnis

Alt, Raimund (2013). Statistik: eine Einführung für Wirtschaftswissenschaftler 2. Aufl., Wien: Linde.

Al-Youssef, Muzayen (2019). Neues Online-Banking: Sicherer, aber für viele Nutzer ärgerlich. Online: https://www.derstandard.at/story/2000107402983/neues-online-banking-sicherer-aber-aergerlich-fuer-viele-nutzer [Abruf am 18.10.2019].

bawaggroup (2019a). Berlin Group NextGenPSD2. Online: https://developer.bawaggroup.com/#/apis/25/136 [Abruf am 15.12.2019].

bawaggroup (2019b). Empfehlungen zur Sicherheit beim Internet-/Mobilebanking. Online: https://www.bawagpsk.com/BAWAGPSK/Sicherheit/479496/empfehlungen-zur-sicherheit-beim-internet--mobilebanking.html [Abruf am 29.03.2020].

bawaggroup (o. J.). BAWAG P.S.K im Überblick. Online: https://www.bawagpsk.com/BAWAGPSK/Ueber_uns/%C3%9Cber%20Uns/Unsere_Bank/291150/ueberblick.html [Abruf am 04.04.2020].

Bendel, Prof Dr Oliver (o. J.). Definition: QR-Code. Online: https://wirtschaftslexikon.gabler.de/definition/qr-code-53515 [Abruf am 31.03.2020].

Berlin Group (o. J.). The Berlin Group - Über. Online: https://www.berlin-group.org [Abruf am 30.03.2020].

Brandt, Mathias (2019). So verbreitet ist Online-Banking in Europa. Online: https://de.statista.com/infografik/965/nutzung-von-online-banking-in-der-eu/ [Abruf am 18.04.2020].

Bundesamt für Sicherheit in der Informationstechnik (o. J.). Digitale Gesellschaft. Sicherheit im Online-Banking. Das mTAN-Verfahren - TAN-Versand per SMS. Online: https://www.bsi-fuer-buerger.de/BSIFB/DE/DigitaleGesellschaft/OnlineBanking/SoFunktioniertDasOnlineBanking/Sicherheit/PIN-TAN-Schutzverfahren.html?nn=6596940&cms_pos=3 [Abruf am 13.04.2020].

computerbild (2020). Schockierend einfach: Gesichtserkennung auch beim S20, P40 Pro & Co geknackt. Online: https://www.computerbild.de/artikel/cb-Tests-Handy-Gesichtserkennung-mit-Foto-geknackt-24910985.html [Abruf am 13.04.2020].

Dax, Patrick (2016). Mobile Banking: „Mobile TANs sind ein Auslaufmodell“. Online: https://futurezone.at/digital-life/mobile-banking-mobile-tans-sind-ein-auslaufmodell/226.405.978 [Abruf am 13.04.2020].

derstandard (2019). App statt SMS: Warum es jetzt Neuerungen beim Online-Banking gibt. Online: https://www.derstandard.at/story/2000107469526/app-statt-sms-warum-es-jetzt-neuerungen-beim-online-banking [Abruf am 18.10.2019].

Deutsche Telekom (o. J.). Fingerabdruck und Gesichtserkennung statt Passwort? Online: https://www.telekom.com/de/verantwortung/datenschutz-und-datensicherheit/sicher-digital/details/fingerabdruck-und-gesichtserkennung-statt-passwort-538744 [Abruf am 13.04.2020].

erstegroup (2019). Bereit für PSD2 und Open Banking: Erste Group schafft einheitlichen Zugang zu den digitalen Schnittstellen all ihrer Tochterbanken im östlichen Teil der EU. Online: https://www.erstegroup.com/de/news-media/presseaussendungen/2019/06/07/psd2-schnittstellen [Abruf am 18.10.2019].

erstegroup (o. J.). Erste Group im Überblick. Online: https://www.erstegroup.com/de/news-media/erste-group-ueberblick [Abruf am 04.04.2020].

Europäische Bankenaufsichtsbehörde (2017a). Final Report. Draft Regulatory Technical Standards on Strong Customer Authentication and common and secure communication under Article 98 of Directive 2015/2366 (PSD2). Online: https://eba.europa.eu/documents/10180/1761863/Final+draft+RTS+on+SCA+and+CSC+under+PSD2+%28EBA-RTS-2017-02%29.pdf [Abruf am 18.10.2019].

Europäische Bankenaufsichtsbehörde (2017b). Opinion of the European Banking Authority on the European Commission’s intention to partially endorse and amend the EBA’s final draft regulatory technical standards on strong customer authentication and common and secure communication under PSD2. Online: https://eba.europa.eu/sites/default/documents/files/documents/10180/1894900/df60c6ac-a284-4772-b1d5-66c7073d28af/EBA%20Opinion%20on%20the%20amended%20text%20of%20the%20RTS%20on%20SCA%20and%20CSC%20(EBA-Op-2017-09).pdf [Abruf am 12.03.2020].

Europäische Bankenaufsichtsbehörde (2018a). Qualification of SMS OTP as an authentication factor. Online: https://eba.europa.eu/single-rule-book-qa/-/qna/view/publicId/2018_4039 [Abruf am 13.04.2020].

Europäische Bankenaufsichtsbehörde (2018b). Auftrag und Aufgaben. Online: https://eba.europa.eu/languages/home_de [Abruf am 29.12.2019].

Europäische Bankenaufsichtsbehörde (2019a). Opinion of the European Banking Authority on the elements of strong customer authentication under PSD2. Online: https://eba.europa.eu/documents/10180/2622242/EBA+Opinion+on+SCA+elements+under+PSD2+.pdf [Abruf am 18.10.2019].

Europäische Bankenaufsichtsbehörde (2019b). EBA publishes Opinion on the deadline and process for completing the migration to strong customer authentication (SCA) for e-commerce card-based payment transactions. Online: https://eba.europa.eu/-/eba-publishes-opinion-on-the-deadline-and-process-for-completing-the-migration-to-strong-customer-authentication-sca-for-e-commerce-card-based-payment [Abruf am 18.10.2019].

Europäische Kommission (2015). Europäische Kommission. Vertretung in Österreich. Über uns. Online: https://ec.europa.eu/austria/about-us_de [Abruf am 29.12.2019].

Europäische Kommission (2017). Richtlinie über Zahlungsdienste (PSD2): Technische Regulierungsstandards bieten Verbrauchern mehr Sicherheit und Innovation bei elektronischen Zahlungen. Online: https://ec.europa.eu/commission/presscorner/detail/de/MEMO_17_4961 [Abruf am 17.11.2019].

eurostat (2019). E-banking and e-commerce. Online: https://appsso.eurostat.ec.europa.eu/nui/show.do?query=BOOKMARK_DS-125107_QID_1E5F8402_UID_-3F171EB0&layout=TIME,C,X,0;GEO,L,Y,0;INDIC_IS,L,Z,0;IND_TYPE,L,Z,1;UNIT,L,Z,2;INDICATORS,C,Z,3;&zSelection=DS-125107IND_TYPE,IND_TOTAL;DS-125107UNIT,PC_IND;DS-125107INDIC_IS,I_IUBK;DS-125107INDICATORS,OBS_FLAG;&rankName1=UNIT_1_2_-1_2&rankName2=INDICATORS_1_2_-1_2&rankName3=INDIC-IS_1_2_-1_2&rankName4=IND-TYPE_1_2_-1_2&rankName5=TIME_1_0_0_0&rankName6=GEO_1_2_0_1&sortC=ASC_-1_FIRST&rStp=&cStp=&rDCh=&cDCh=&rDM=true&cDM=true&footnes=false&empty=false&wai=false&time_mode=FIXED&time_most_recent=false&lang=EN&cfo=%23%23%23%2C%23%23%23.%23%23%23&lang=en [Abruf am 18.10.2019].

Fletzberger, Bernd (2018). PSD2 - alle wichtigen Infos zusammengefasst. Online: https://www.pfr.at/de/psd2-zusammenfassung [Abruf am 16.11.2019].

Fletzberger, Bernd (2019). PSD2 - Stand der EBA-Regulierungsstandards und Leitlinien. Online: https://www.pfr.at/de/rts-und-leitlinien-der-eba [Abruf am 16.11.2019].

Fletzberger, Bernd (o. J.). Zahlungsdienstgesetz 2018 (ZaDIG 2018). Online: https://www.pfr.at/de/zahlungsdienstegesetz-2018-zadig-2018 [Abruf am 14.12.2019].

Gabriel, Roland (o. J.). Definition: IT-Sicherheit. Online: https://www.gabler-banklexikon.de/definition/it-sicherheit-70719 [Abruf am 31.03.2020].

Härtel, Uwe (2019). „Auslaufmodell mTAN“?! Warum das mTAN- Verfahren nicht PSD2-konform ist. Online: https://www.der-bank-blog.de/auslaufmodell-mtan/online-banking/37657760/ [Abruf am 13.04.2020].

Hemmerich, Wanja (o. J.). Korrelation, Korrelationskoeffizient. Online: https://matheguru.com/stochastik/korrelation-korrelationskoeffizient.html#Voraussetzungen-2 [Abruf am 08.04.2020].

Javaid, Omar (2019). PSD2 für Online-Shops: Welche Zwei-Faktor-Authentifizierung ist sinnvoll. Online: https://www.computerwoche.de/a/welche-zwei-faktor-authentifizierung-ist-sinnvoll,3547673 [Abruf am 15.12.2019].

Juraforum (o. J.). EU Rechtsakte: Erklärung zum Begriff EU Rechtsakte. Online: https://www.juraforum.de/lexikon/rechtsakte-der-eu [Abruf am 29.12.2019].

Krautkrämer, Stefan (2018). PSD2 gestern, heute und morgen. Die wichtigsten Infos über die Richtlinie für Zahlungsdienste. Online: https://knowledge.fintecsystems.com/blog/psd2-gestern-heute-und-morgen [Abruf am 11.03.2020].

Metzger, Jochen (o. J.). Definition: Zahlungsdienstleister. Online: https://wirtschaftslexikon.gabler.de/definition/zahlungsdienstleister-54175 [Abruf am 29.12.2019].

MoneyToday (o. J.). Banking und Finance im digitalen Alltag. PSD2. Online: https://www.moneytoday.ch/lexikon/psd2/ [Abruf am 29.12.2019a].

MoneyToday (o. J.). Banking und Finance im digitalen Alltag. API Banking. Online: https://www.moneytoday.ch/lexikon/api-banking/ [Abruf am 29.12.2019b].

MoneyToday (o. J.). Banking und Finance im digitalen Alltag. Open Banking. Online: https://www.moneytoday.ch/lexikon/open-banking/ [Abruf am 29.12.2019c].

N26 (o. J.). Sicherheit bei N26. Online: https://n26.com/de-de/sicherheit [Abruf am 29.03.2020].

Österreichischer Raiffeisenverband (2018). Geld und Finanzdienstleistungen. Online: https://www.raiffeisenverband.at/raiffeisen-in-oesterreich/geld-finanzdienstleistungen/ [Abruf am 04.04.2020].

PayLife (o. J.). Mit 3D Secure schützen Sie Ihre Online Zahlungen. Starke Authentifizierung von Internetzahlungen. Online: https://www.paylife.at/paylife/service/3d-secure-index [Abruf am 13.04.2020].

PCI Security Standards Council (2013). Payment Card Industry (PCI). Datensicherheitsstandard. Anforderungen und Sicherheitsbeurteilungsverfahren V3.0. Online: https://de.pcisecuritystandards.org/_onelink_/pcisecurity/en2de/minisite/en/docs/PCI_DSS_v3.pdf [Abruf am 29.03.2020].

qualtrics (2020). Online-Stichproben – die richtige Stichprobengröße bestimmen. Online: https://www.qualtrics.com/de/erlebnismanagement/research-core/online-stichproben/ [Abruf am 07.03.2020].

Raiffeisen (o. J.). Die pushTAN auf Ihrem Computer. Online: https://www.raiffeisen.at/de/online-banking/mein-elba/sicherheit/pushtan-desktop.html [Abruf am 13.04.2020].

red./tirol.ORF (2019). Onlinebanking: Die SMS-TAN hat ausgedient. Online: https://tirol.orf.at/stories/3005004/ [Abruf am 18.10.2019].

Reitbauer, Gerhard (o. J.). Token-Code. Online: https://www.reitbauer.at/elexikon/?qkeyword=Token-Code [Abruf am 31.03.2020].

Sparkasse Bank AG (o. J.). Alternative Login- und Freigabe-Methoden. Nutzen Sie Internetbanking George ohne Smartphone. Online: https://www.sparkasse.at/waldviertler-sparkasse/privatkunden/digitales-banking/alternative-login-methoden [Abruf am 05.01.2020].

statista (2020a). Anteil der Bevölkerung in Österreich, die das Internet für Online-Banking nutzen von 2007 bis 2019. Online: https://de.statista.com/statistik/daten/studie/431727/umfrage/nutzung-des-internets-fuer-online-banking-in-oesterreich/ [Abruf am 07.03.2020].

statista (2020b). Bevölkerung von Österreich von 2010 bis 2020. Online: https://de.statista.com/statistik/daten/studie/19292/umfrage/gesamtbevoelkerung-in-oesterreich/ [Abruf am 07.03.2020].

STUZZA (o. J.). Zahlen mit System - XS2A / API. Online: https://www.stuzza.at/de/xs2a-api.html [Abruf am 15.12.2019].

surveymonkey (2019). Berechnen der Anzahl der benötigten Befragten. Online: https://help.surveymonkey.com/articles/de/kb/How-many-respondents-do-I-need [Abruf am 18.10.2019].

UniCredit Bank Austria (2018). Präsentation für Fixed Income-Investoren. Online: https://www.bankaustria.at/files/Bank_Austria_Investor_Presentation_1Q18_DE.pdf [Abruf am 04.04.2020].

viveum (o. J.). Meteorpay: Häufig gestellte Fragen zu PSD2, SCA und 3DS v2. Online: https://www.viveum.com/faq-psd2-meteorpay/ [Abruf am 17.11.2019].

Walz, Christian (o. J.). Glossar: Limited Network. Online: https://paytechlaw.com/glossary/limited-network/ [Abruf am 16.11.2019].

Rechtsquellen

Delegierte Verordnung (EU) 2018/389 der Kommission vom 27. November 2017 zur Ergänzung der Richtlinie (EU) 2015/2366 des Europäischen Parlaments und des Rates durch technische Regulierungsstandards für eine starke Kundenauthentifizierung und für sichere offene Standards für die Kommunikation

Richtlinie (EU) 2015/2366 des Europäischen Parlaments und des Rates vom 25. November 2015 über Zahlungsdienste im Binnenmarkt, zur Änderung der Richtlinien 2002/65/EG, 2009/110/EG und 2013/36/EU und der Verordnung (EU) Nr. 1093/2010 sowie zur Aufhebung der Richtlinie 2007/64/EG

Abbildungsverzeichnis

Tabellenverzeichnis

Abkürzungsverzeichnis

AISP – Account Information Service Provider

API – Application Interface

App – Application

DelVo – Delegierte Verordnung

DSGVO – Datenschutzgrundverordnung

EBA – Europäische Bankenaufsichtsbehörde

EU – Europäische Union

EZB – Europäische Zentralbank

FMA – Finanzmarktaufsichtsbehörde

HTTPs – Hypertext Transfer Protocol Secure

ISO – Internationale Organisation für Normung

NFC – Near Field Communication

o. J. – ohne Jahr

PC – Personal Computer

PCI DSS – Payment Card Industry Data Security Standard

PIN – Persönliche Identifikationsnummer

PISP – Payment Initiation Service Provider

POS – Point of Sale

PSD2 – Payment Service Directive 2

Rd. – Rund

RL – Richtlinie

RTS – Regulatory Technical Standard

SCA – Strong Customer Authentication

SIM – Subscriber Identity Module

SMS – Short Message Service

TAN – Transaktionsnummer

TPP – Third Party Provider

z.B. – zum Beispiel

Anhang A – Korrelation der beantworteten Fragen

	F1	F2	F3	F3/1	F3/2	F4	F5	F6	F6/1	F6/2	F6/3	F7	F7/1	F7/2	F7/3	F7/4	F7/5	F8	F8/1	F8/2	F8/3	F8/4	F9	F9/1	F9/2	F9/3	F10
F1	1,00																										
F2	-0,01	1,00																									
F3	0,00	0,00	1,00																								
F3/1	-0,02	0,26	0,00	1,00																							
F3/2	0,07	0,32	0,00	0,17	1,00																						
F4	0,03	0,33	0,00	0,16	0,25	1,00																					
F5	-0,24	0,01	0,00	0,02	-0,08	0,11	1,00																				
F6	0,00	0,00	0,00	0,00	0,00	0,00	0,00	1,00																			
F6/1	0,04	0,02	0,00	0,09	0,15	0,30	0,01	0,00	1,00																		
F6/2	0,01	0,06	0,00	-0,04	0,12	0,32	0,05	0,00	0,45	1,00																	
F6/3	0,05	0,06	0,00	0,02	0,21	0,38	0,00	0,00	0,65	0,53	1,00																
F7	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	1,00															
F7/1	0,04	0,06	0,00	0,04	0,03	0,14	-0,10	0,00	-0,02	-0,13	-0,04	0,00	1,00														
F7/2	-0,14	0,05	0,00	0,10	0,02	0,02	0,09	0,00	-0,10	-0,16	-0,08	0,00	0,34	1,00													
F7/3	-0,03	-0,06	0,00	-0,01	-0,16	-0,09	0,05	0,00	-0,07	-0,04	-0,19	0,00	0,04	0,00	1,00												
F7/4	-0,08	0,11	0,00	-0,02	0,26	0,20	-0,02	0,00	0,16	0,22	0,16	0,00	0,17	0,04	-0,13	1,00											
F7/5	0,02	-0,02	0,00	0,02	-0,14	-0,23	0,03	0,00	-0,21	-0,33	-0,24	0,00	0,04	0,09	0,36	-0,25	1,00										
F8	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	1,00									
F8/1	-0,16	0,21	0,00	0,04	0,23	0,21	0,09	0,00	0,15	0,09	0,13	0,00	0,13	0,23	-0,04	0,12	-0,02	0,00	1,00								
F8/2	-0,07	0,17	0,00	0,02	0,20	0,15	0,00	0,00	0,13	-0,07	0,03	0,00	0,13	0,10	0,02	-0,01	-0,02	0,00	0,50	1,00							
F8/3	-0,10	0,16	0,00	0,09	0,09	0,16	0,10	0,00	0,08	-0,17	0,06	0,00	0,17	0,19	-0,10	0,05	0,02	0,00	0,49	0,62	1,00						
F8/4	-0,08	0,23	0,00	0,11	0,22	0,18	0,07	0,00	0,14	-0,04	0,07	0,00	0,18	0,20	-0,12	0,15	-0,04	0,00	0,45	0,55	0,66	1,00					
F9	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	1,00				
F9/1	0,00	-0,07	0,00	0,00	-0,06	0,12	-0,08	0,00	0,11	0,10	0,01	0,00	0,02	0,02	0,01	0,10	-0,05	0,00	-0,05	0,02	-0,09	-0,06	0,00	1,00			
F9/2	-0,02	0,10	0,00	0,04	0,13	0,00	0,08	0,00	0,01	-0,08	0,10	0,00	0,01	-0,09	-0,12	0,07	-0,08	0,00	0,06	0,01	0,14	0,11	0,00	-0,54	1,00		
F9/3	0,02	-0,03	0,00	-0,03	-0,07	-0,12	0,00	0,00	-0,12	-0,02	-0,11	0,00	-0,02	0,07	0,11	-0,18	0,13	0,00	-0,01	-0,03	-0,05	-0,05	0,00	-0,48	-0,49	1,00	
F10	0,02	0,29	0,00	0,09	0,22	0,35	-0,03	0,00	0,09	0,15	0,22	0,00	0,12	0,19	-0,08	0,14	-0,10	0,00	0,28	0,10	0,16	0,19	0,00	0,02	0,03	-0,05	1,00
F11	-0,03	0,12	0,00	-0,07	0,28	0,12	-0,04	0,00	-0,01	-0,07	0,04	0,00	0,14	0,22	-0,17	0,11	-0,10	0,00	0,21	0,08	0,06	0,10	0,00	-0,06	0,06	0,00	0,21
F12	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00
F12/1	-0,16	-0,10	0,00	-0,43	0,21	0,12	0,00	0,00	0,29	0,47	0,52	0,00	-0,22	-0,09	0,00	0,52	-0,33	0,00	0,15	-0,08	-0,26	-0,40	0,00	0,32	0,14	-0,49	0,27
F12/2	0,00	0,02	0,00	-0,35	0,06	0,00	-0,13	0,00	0,25	0,35	0,51	0,00	-0,17	-0,13	0,00	0,30	-0,22	0,00	0,11	-0,03	-0,26	-0,47	0,00	0,15	-0,05	-0,14	0,13

	F1	F2	F3	F3/1	F3/2	F4	F5	F6	F6/1	F6/2	F6/3	F7	F7/1	F7/2	F7/3	F7/4	F7/5	F8	F8/1	F8/2	F8/3	F8/4	F9	F9/1	F9/2	F9/3	F10
F12/3	-0,06	0,07	0,00	-0,26	0,11	0,00	-0,15	0,00	0,30	0,36	0,58	0,00	-0,21	-0,18	0,00	0,36	-0,24	0,00	0,15	0,02	-0,22	-0,42	0,00	0,10	0,01	-0,14	0,12
F13	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00
F13/1	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00
F13/2	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00
F13/3	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00
F13/4	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00
F14	-0,10	0,10	0,00	0,05	0,24	0,12	-0,02	0,00	0,06	0,04	0,10	0,00	0,28	0,12	-0,14	0,11	-0,17	0,00	0,20	0,09	0,12	0,17	0,00	-0,02	0,10	-0,08	0,19
F15	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00
F15/1	0,03	0,12	0,00	0,00	0,36	0,34	0,00	0,00	0,41	0,27	0,33	0,00	0,16	-0,02	0,07	0,20	-0,07	0,00	0,15	0,19	0,14	0,19	0,00	-0,02	0,03	-0,01	0,23
F15/2	0,06	0,05	0,00	-0,03	0,25	0,29	-0,09	0,00	0,37	0,25	0,33	0,00	0,16	0,00	-0,04	0,21	-0,08	0,00	0,11	0,07	0,12	0,21	0,00	0,08	-0,05	-0,02	0,27
F15/3	0,01	0,06	0,00	0,07	0,29	0,20	-0,08	0,00	0,34	0,21	0,27	0,00	0,08	0,08	0,02	0,19	-0,08	0,00	0,09	0,12	0,12	0,23	0,00	0,15	-0,13	-0,01	0,25
F16	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00
F16/1	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00
F16/2	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00
F16/3	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00
F16/4	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00
F17	0,00	0,14	0,00	0,13	0,24	0,14	0,08	0,00	0,10	0,09	0,06	0,00	0,20	0,12	-0,05	0,31	-0,04	0,00	0,10	-0,02	-0,08	0,05	0,00	-0,01	0,06	-0,06	0,22
F18	0,05	0,06	0,00	-0,16	0,40	0,11	-0,10	0,00	0,08	0,12	0,12	0,00	0,09	-0,01	-0,10	0,23	-0,14	0,00	0,28	0,15	0,09	0,21	0,00	0,02	0,04	-0,07	0,11
F19	-0,10	0,13	0,00	0,05	0,13	0,16	0,06	0,00	0,11	0,04	0,11	0,00	0,10	0,11	-0,03	0,05	-0,06	0,00	0,24	0,09	0,16	0,11	0,00	-0,12	0,13	-0,01	0,19
F20	0,09	-0,08	0,00	-0,11	-0,13	-0,04	0,00	0,00	0,01	0,07	-0,05	0,00	-0,03	-0,16	0,20	-0,12	0,02	0,00	-0,11	-0,06	-0,19	-0,18	0,00	0,18	-0,09	-0,10	0,05
F21	-0,03	0,47	0,00	0,19	0,31	0,28	0,01	0,00	0,06	0,05	0,08	0,00	0,01	0,03	-0,10	0,09	-0,09	0,00	0,15	0,14	0,10	0,17	0,00	0,05	0,04	-0,09	0,22

	F11	F12	F12/1	F12/2	F12/3	F13	F13/1	F13/2	F13/3	F13/4	F14	F15	F15/1	F15/2	F15/3	F16	F16/1	F16/2	F16/3	F16/4	F17	F18	F19	F20	F21
F1																									
F2																									
F3																									
F3/1																									
F3/2																									
F4																									
F5																									
F6																									
F6/1																									
F6/2																									
F6/3																									
F7																									

	F11	F12	F12/1	F12/2	F12/3	F13	F13/1	F13/2	F13/3	F13/4	F14	F15	F15/1	F15/2	F15/3	F16	F16/1	F16/2	F16/3	F16/4	F17	F18	F19	F20	F21
F7/1																									
F7/2																									
F7/3																									
F7/4																									
F7/5																									
F8																									
F8/1																									
F8/2																									
F8/3																									
F8/4																									
F9																									
F9/1																									
F9/2																									
F9/3																									
F10																									
F11	1,00																								
F12	0,00	1,00																							
F12/1	0,00	0,00	1,00																						
F12/2	0,00	0,00	0,75	1,00																					
F12/3	0,00	0,00	0,76	0,97	1,00																				
F13	0,00	0,00	0,00	0,00	0,00	1,00																			
F13/1	0,00	0,00	0,00	0,00	0,00	0,00	1,00																		
F13/2	0,00	0,00	0,00	0,00	0,00	0,00	0,00	1,00																	
F13/3	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	1,00																
F13/4	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	1,00															
F14	0,24	0,00	0,05	-0,01	0,03	0,00	0,00	0,00	0,00	0,00	1,00														
F15	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	1,00													
F15/1	0,15	0,00	0,34	0,33	0,29	0,00	0,00	0,00	0,00	0,00	0,00	0,00	1,00												
F15/2	0,19	0,00	0,48	0,39	0,38	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,59	1,00											
F15/3	0,21	0,00	0,45	0,38	0,38	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,55	0,86	1,00										
F16	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	1,00									
F16/1	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	1,00								
F16/2	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	1,00							
F16/3	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	1,00						
F16/4	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	1,00					

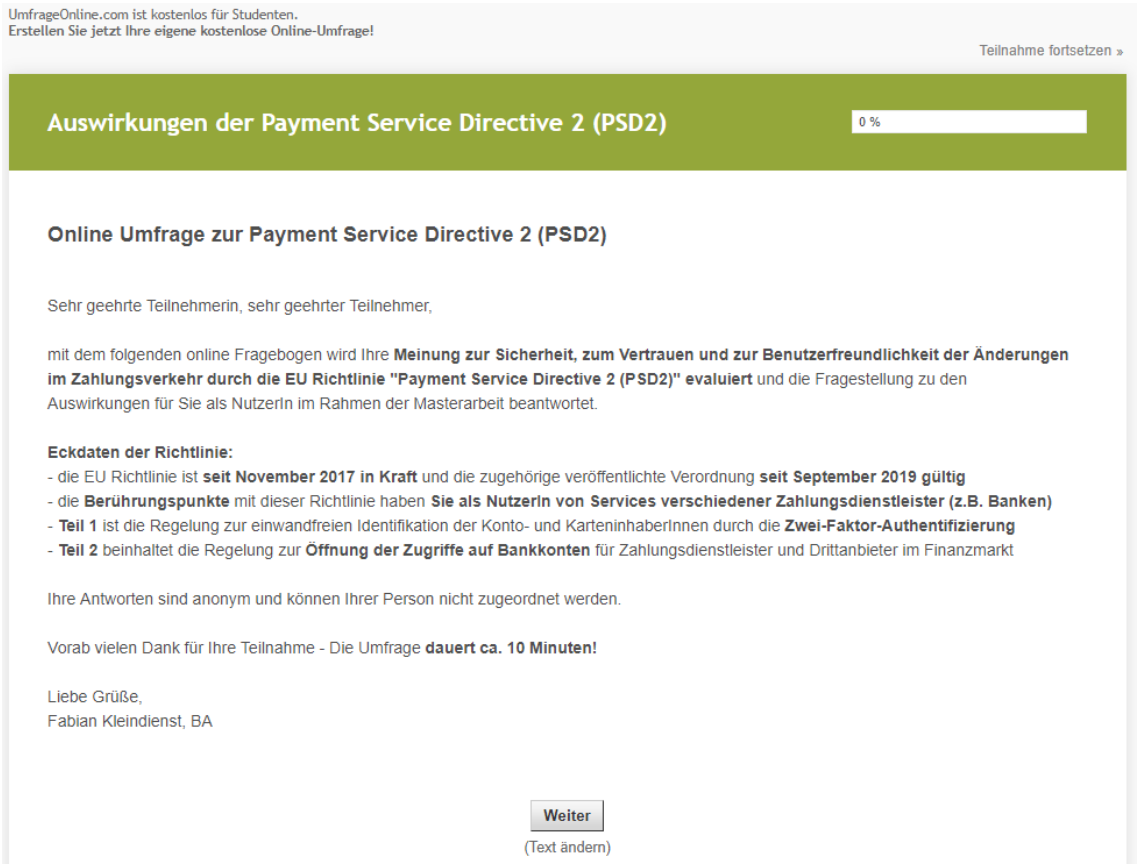
	F11	F12	F12/1	F12/2	F12/3	F13	F13/1	F13/2	F13/3	F13/4	F14	F15	F15/1	F15/2	F15/3	F16	F16/1	F16/2	F16/3	F16/4	F17	F18	F19	F20	F21
F17	0,13	0,00	0,10	0,18	0,14	0,00	0,00	0,00	0,00	0,00	0,16	0,00	0,27	0,23	0,18	0,00	0,00	0,00	0,00	0,00	1,00				
F18	0,19	0,00	0,32	0,09	0,07	0,00	0,00	0,00	0,00	0,00	0,16	0,00	0,20	0,17	0,13	0,00	0,00	0,00	0,00	0,00	0,15	1,00			
F19	0,15	0,00	0,16	0,07	0,12	0,00	0,00	0,00	0,00	0,00	0,19	0,00	0,17	0,11	0,08	0,00	0,00	0,00	0,00	0,00	0,06	0,07	1,00		
F20	-0,14	0,00	0,07	0,11	0,02	0,00	0,00	0,00	0,00	0,00	-0,12	0,00	-0,05	-0,01	-0,02	0,00	0,00	0,00	0,00	0,00	-0,03	-0,10	-0,14	1,00	
F21	0,16	0,00	0,18	0,17	0,22	0,00	0,00	0,00	0,00	0,00	0,02	0,00	-0,01	0,01	0,03	0,00	0,00	0,00	0,00	0,00	0,05	0,22	0,02	0,00	1,00

Anhang B – Legende zur Korrelation

F1	1. Bitte wählen Sie den Zahlungsdienstleister, von dem Sie vorrangig Dienstleistungen beziehen, und beantworten Sie die weiteren Fragen in Bezug auf diesen Zahlungsdienstleister.
F2	2. Haben Sie schon von der EU-Richtlinie „Payment Service Directive 2 (PSD2)“ gehört?
F3	3. Wie häufig benutzen Sie...
F3/1	...Services eines Zahlungsdienstleisters über den Zugang eines Computers
F3/2	...Services eines Zahlungsdienstleisters über eine App auf dem Smartphone oder Tablet
F4	4. Wie gut fühlen Sie sich über die neuen Zwei-Faktor-Authentifizierungsmethoden der Payment Service Directive 2 informiert?
F5	5. Welche Zwei-Faktor-Authentifizierungsmethode verwenden Sie vorrangig für einen Login oder eine Zahlungsfreigabe?
F6	6. Wie bewerten Sie Ihre verwendete Lösung zur Zwei-Faktor-Authentifizierung (Login und Zahlungsfreigabe)?
F6/1	Sicherheitsgefühl (z.B. Umgang mit den Daten)
F6/2	Usability des Services (z.B. Verständlichkeit, Zuverlässigkeit, Schnelligkeit)
F6/3	Vertrauen zum Service (z.B. Glaubwürdigkeit, Seriosität, Überzeugung)
F7	7. Treffen in Bezug auf Ihr verwendetes Service (Login und Zahlungsfreigabe) folgende Aussagen und Gründe zu, wenn Ja welche und mit welchem Hauptgrund?
F7/1	Ich würde zu alternativen Zahlungsdienstleistern/Drittanbietern (z.B. PayPal) wechseln, weil
F7/2	Ich würde eine andere Bank mit deren Lösungen bevorzugen, weil
F7/3	Ich mache zukünftig vermehrt Transaktionen mit dem Bargeld, weil
F7/4	Ich verwende Online Banking und E-Commerce Transaktionen (Onlinehandel) mehr als bisher, weil
F7/5	Ich verwende Online Banking und E-Commerce Transaktionen (Onlinehandel) weniger, weil
F8	8. Wie bewerten Sie folgende Ausnahmemöglichkeiten der Zwei-Faktor-Authentifizierung (in Kurzform: 2FA)?
F8/1	die Möglichkeit des Setzens von Ausnahmen, um ausgewählten Verkaufsplattformen zu vertrauen und dadurch auf die 2FA zu verzichten (auch genannt Whitelisting)
F8/2	die Möglichkeit des Verzichts auf die 2FA wenn der/die AuslöserIn und der/die EmpfängerIn einer Transaktion selbige Person und beide Konten beim selbigem Zahlungsdienstleister angesiedelt sind
F8/3	die Möglichkeit zum Verzicht auf die 2FA bis zu gewissen Transaktionslimits (z.B. € 30 pro Transaktion oder € 100 einer Reihe kumulierter Transaktionen)
F8/4	die Möglichkeit zum Verzicht bei gleichbleibenden Folgetransaktionen (z.B. Daueraufträge) auf die 2FA zu verzichten
F9	9. Reihen Sie folgende Sichtweisen in Bezug zur Zwei-Faktor-Authentifizierung (Login und Zahlungsfreigabe) nach der Wichtigkeit in Ihrem Empfinden.
F9/1	Sicherheitsgefühl (z.B. Umgang mit Authentifizierungs-Daten)
F9/2	Usability des Services (z.B. Verständlichkeit, Zuverlässigkeit, Schnelligkeit)
F9/3	Vertrauen zum Service (z.B. Glaubwürdigkeit, Seriosität, Überzeugung)
F10	10. Wie gut fühlen Sie sich über die Möglichkeiten von Open Banking (Zugriff auf Ihr Konto durch Dritte mit Ihrer Zustimmung) informiert?

F11	11. Verwenden Sie Services, womit Sie Konto- und Transaktionsinformationen verschiedener Zahlungsdienstleister gesammelt in einem Dashboard anzeigen können? (sogenannte: Kontoinformationsdienste)
F12	12. Wie bewerten Sie Services, womit Sie Konto- und Transaktionsinformationen verschiedener Zahlungsdienstleister gesammelt in einem Dashboard anzeigen können?
F12/1	Usability des Services (z.B. Verständlichkeit, Zuverlässigkeit, Schnelligkeit)
F12/2	Sicherheitsgefühl (z.B. Umgang mit Kontoinformationen)
F12/3	Vertrauen zum Service (z.B. Glaubwürdigkeit, Seriosität, Überzeugung)
F13	13. Aus welchen Gründen verwenden Sie Services, wie die Anzeige von Konto- und Transaktionsinformationen verschiedener Zahlungsdienstleister in einem Dashboard, bisher nicht?
F13/1	Sicherheitsgefühl (z.B. Umgang mit Kontoinformationen)
F13/2	Usability der Services (z.B. Verständlichkeit, Zuverlässigkeit, Schnelligkeit)
F13/3	Vertrauen zum Service (z.B. Glaubwürdigkeit, Seriosität, Überzeugung)
F13/4	aus anderen Gründen
F14	14. Verwenden Sie Services, womit Sie Transaktionen durchführen (lassen) können ohne mit Ihrem Zahlungsdienstleister in Kontakt zu treten? (sogenannte: Zahlungsauslösedienste)
F15	15. Wie bewerten Sie Services, womit Sie Transaktionen durchführen (lassen) können ohne mit Ihrem Zahlungsdienstleister in Kontakt zu treten?
F15/1	Usability des Services (z.B. Verständlichkeit, Zuverlässigkeit, Schnelligkeit)
F15/2	Sicherheitsgefühl (z.B. Umgang mit Kontoinformationen)
F15/3	Vertrauen zum Service (z.B. Glaubwürdigkeit, Seriosität, Überzeugung)
F16	16. Aus welchen Gründen verwenden Sie Services, womit Sie Transaktionen durchführen (lassen) können ohne mit Ihrem Zahlungsdienstleister in Kontakt zu treten, bisher nicht?
F16/1	Sicherheitsgefühl (z.B. Umgang mit Kontoinformationen)
F16/2	Usability der Services (z.B. Verständlichkeit, Zuverlässigkeit, Schnelligkeit)
F16/3	Vertrauen zum Service (z.B. Glaubwürdigkeit, Seriosität, Überzeugung)
F16/4	aus anderen Gründen
F17	17. Nehmen Sie seit September 2019 vermehrt diese Art von Services (z.B. Informationsportale, Vergleichsportale, Zahlungsauslöseportale) am Markt wahr?
F18	18. Bitte den zutreffenden Bereich Ihres Alters auswählen
F19	19. Wohnhaft in...
F20	20. Ihre höchste abgeschlossene Ausbildung ist?
F21	21. Ihr berufliches Tätigkeitsfeld ist?

Anhang C – online Fragebogen Fragen



UmfrageOnline.com ist kostenlos für Studenten.
Erstellen Sie jetzt Ihre eigene kostenlose Online-Umfrage!

Teilnahme fortsetzen »

Auswirkungen der Payment Service Directive 2 (PSD2) 0 %

Online Umfrage zur Payment Service Directive 2 (PSD2)

Sehr geehrte Teilnehmerin, sehr geehrter Teilnehmer,

mit dem folgenden online Fragebogen wird Ihre **Meinung zur Sicherheit, zum Vertrauen und zur Benutzerfreundlichkeit der Änderungen im Zahlungsverkehr durch die EU Richtlinie "Payment Service Directive 2 (PSD2)" evaluiert** und die Fragestellung zu den Auswirkungen für Sie als NutzerIn im Rahmen der Masterarbeit beantwortet.

Eckdaten der Richtlinie:
- die EU Richtlinie ist **seit November 2017 in Kraft** und die zugehörige veröffentlichte Verordnung **seit September 2019 gültig**
- die **Berührungspunkte** mit dieser Richtlinie haben **Sie als NutzerIn von Services verschiedener Zahlungsdienstleister (z.B. Banken)**
- **Teil 1** ist die Regelung zur einwandfreien Identifikation der Konto- und KarteninhaberInnen durch die **Zwei-Faktor-Authentifizierung**
- **Teil 2** beinhaltet die Regelung zur **Öffnung der Zugriffe auf Bankkonten** für Zahlungsdienstleister und Drittanbieter im Finanzmarkt

Ihre Antworten sind anonym und können Ihrer Person nicht zugeordnet werden.

Vorab vielen Dank für Ihre Teilnahme - Die Umfrage **dauert ca. 10 Minuten!**

Liebe Grüße,
Fabian Kleindienst, BA

Weiter
(Text ändern)

Teilnahme fortsetzen »

Auswirkungen der Payment Service Directive 2 (PSD2)

5 %

Bitte wählen Sie den Zahlungsdienstleister, von dem Sie vorrangig Dienstleistungen beziehen, und beantworten Sie die weiteren Fragen in Bezug auf diesen Zahlungsdienstleister. *

- ○ Erste Group Bank (inkl. Sparkasse)
- ○ Raiffeisenbank
- ○ Bawag Group
- ○ UniCredit Bank Austria
- ○ sonstiger österreichischer Zahlungsdienstleister
- ○ kein österreichischer Zahlungsdienstleister
- ○ habe kein Bankkonto

Zurück Weiter

(Text ändern)

UmfrageOnline.com ist kostenlos für Studenten.
Erstellen Sie jetzt Ihre eigene kostenlose Online-Umfrage!

Teilnahme fortsetzen »

Auswirkungen der Payment Service Directive 2 (PSD2)

10 %

Haben Sie schon von der EU-Richtlinie „Payment Service Directive 2 (PSD2)“ gehört? *

- ○ Ja, ich kenne die Inhalte der Richtlinie
- ○ Ich habe davon gehört, kenne aber keine Inhalte
- ○ Nein, die PSD2 kannte ich bisher nicht

Zurück Weiter

(Text ändern)

Teilnahme fortsetzen »

Auswirkungen der Payment Service Directive 2 (PSD2)

14 %

Wie häufig benutzen Sie... *

	mehrmals täglich	einmal täglich	mehrmals wöchentlich	einmal wöchentlich	einmal monatlich	nie
...Services eines Zahlungsdienstleisters über den Zugang eines Computers	◯	◯	◯	◯	◯	◯
...Services eines Zahlungsdienstleisters über eine App auf dem Smartphone oder Tablet	◯	◯	◯	◯	◯	◯

Zurück Weiter

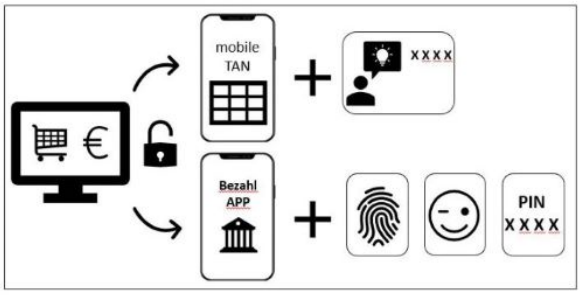
(Text ändern)

Auswirkungen der Payment Service Directive 2 (PSD2)

19 %

Teil 1: Zwei-Faktor-Authentifizierung

Erklärung der Zwei-Faktor-Authentifizierung



Teil 1 der Richtlinie definiert, dass Transaktionen durch eine **„Zwei-Faktor-Authentifizierung (2FA)"** abgesichert werden müssen.

Diese besteht aus zwei der drei Faktoren:
- Wissen (z.B. Passwort oder PIN)
- Besitz (z.B. ein Smartphone und eine verknüpfte App oder ein Passwort per SMS)
- Inhärenz (z.B. ein Fingerabdruck oder Gesichtsscan)

Die häufigsten marktüblichen Zwei-Faktor-Authentifizierungsmethoden sind folgende:
1. Freigabe durch die Eingabe eines Passwortes und einer per SMS zugesendeten Transaktionsnummer (TAN)
2. Freigabe mittels einer mit dem Smartphone verknüpften App in welcher ein Passwort, ein Code oder eine biometrische Eingabe erfolgt
3. Freigabe mithilfe einer zusätzlich zur Banking App verwendeten Security App, welche die Eingabe eines Passwortes oder eines Fingerprints erfordert

Zurück Weiter

(Text ändern)

Teilnahme fortsetzen »

Auswirkungen der Payment Service Directive 2 (PSD2)

24 %

Wie gut fühlen Sie sich über die neuen Zwei-Faktor-Authentifizierungsmethoden der Payment Service Directive 2 informiert? *

- ( ) sehr gut
- ( ) gut
- ( ) weniger gut
- ( ) nicht gut

Zurück Weiter

(Text ändern)

UmfrageOnline.com ist kostenlos für Studenten.
Erstellen Sie jetzt Ihre eigene kostenlose Online-Umfrage!

Teilnahme fortsetzen »

Auswirkungen der Payment Service Directive 2 (PSD2)

29 %

Welche Zwei-Faktor-Authentifizierungsmethode verwenden Sie vorrangig für einen Login oder eine Zahlungsfreigabe? *

- ( ) die Eingabe einer mobile TAN die als SMS zugestellt wird
- ( ) eine App mit Passwort oder Code/PIN
- ( ) eine App mit Fingerprint/Gesichtserkennung
- ( ) eine App, die als Desktopversion auf dem Computer installiert ist
- ( ) einen cardTAN-Generator, welcher ein einmal gültiges Passwort zur Eingabe generiert
- ( ) ich habe eine andere Zwei-Faktor-Authentifizierungsmethode in Verwendung
- ( ) ich weiß nicht welche Zwei-Faktor-Authentifizierungsmethode ich verwende

Zurück Weiter

(Text ändern)

Teilnahme fortsetzen »

Auswirkungen der Payment Service Directive 2 (PSD2)

Wie bewerten Sie Ihre verwendete Lösung zur Zwei-Faktor-Authentifizierung (Login und Zahlungsfreigabe)? *

	sehr gut	gut	weniger gut	nicht gut	keine Bewertung möglich
Sicherheitsgefühl (z.B. Umgang mit den Daten)	○	○	○	○	○
Usability des Services (z.B. Verständlichkeit, Zuverlässigkeit, Schnelligkeit)	○	○	○	○	○
Vertrauen zum Service (z.B. Glaubwürdigkeit, Seriösität, Überzeugung)	○	○	○	○	○

Zurück Weiter

(Text ändern)

Teilnahme fortsetzen »

Auswirkungen der Payment Service Directive 2 (PSD2)

Treffen im Bezug auf Ihr verwendetes Service (Login und Zahlungsfreigabe) folgende Aussagen und Gründe zu, wenn Ja welche und mit welchem Hauptgrund? *

bei keiner Übereinstimmung der Aussage mit Ihrer Haltung "trifft nicht zu" auswählen

	Sicherheitsgefühl (z.B. Umgang mit Daten)	Usability des Services (z.B. Verständlichkeit, Zuverlässigkeit, Schnelligkeit)	Vertrauen zum Service (z.B. Glaubwürdigkeit, Seriösität, Überzeugung)	anderer Beweggrund	trifft nicht zu
Ich würde zu alternativen Zahlungsdienstleistern/Drittanbietern (z.B. PayPal) wechseln, weil	◯	◯	◯	◯	◯
Ich würde eine andere Bank mit deren Lösungen bevorzugen, weil	◯	◯	◯	◯	◯
Ich mache zukünftig vermehrt Transaktionen mit dem Bargeld, weil	◯	◯	◯	◯	◯
Ich verwende Online Banking und E-Commerce Transaktionen (Onlinehandel) mehr als bisher, weil	◯	◯	◯	◯	◯
Ich verwende Online Banking und E-Commerce Transaktionen (Onlinehandel) weniger, weil	◯	◯	◯	◯	◯

Zurück Weiter

(Text ändern)

Auswirkungen der Payment Service Directive 2 (PSD2)

Wie bewerten Sie folgende Ausnahmemöglichkeiten der Zwei-Faktor-Authentifizierung (in Kurzform: 2FA)? *

	sehr gut	gut	weniger gut	nicht gut	nicht zu bewerten
die Möglichkeit des Setzens von Ausnahmen, um ausgewählten Verkaufsplattformen zu vertrauen und dadurch auf die 2FA zu verzichten (auch genannt Whitelisting)	○	○	○	○	○
die Möglichkeit des Verzichts auf die 2FA wenn der/die AuslöserIn und der/die EmpfängerIn einer Transaktion selbige Personen und beide Konten beim selbigem Zahlungsdienstleister angesiedelt sind	○	○	○	○	○
die Möglichkeit zum Verzicht auf die 2FA bis zu gewissen Transaktionslimits (z.B. € 30 pro Transaktion oder € 100 einer Reihe kumulierter Transaktionen)	○	○	○	○	○
die Möglichkeit zum Verzicht bei gleichbleibenden Folgetransaktionen (z.B. Daueraufträge) auf die 2FA zu verzichten	○	○	○	○	○

Zurück Weiter

(Text ändern)

UmfrageOnline.com ist kostenlos für Studenten.
Erstellen Sie jetzt Ihre eigene kostenlose Online-Umfrage!

Auswirkungen der Payment Service Directive 2 (PSD2)

Reihen Sie folgende Sichtweisen in Bezug zur Zwei-Faktor-Authentifizierung (Login und Zahlungsfreigabe) nach der Wichtigkeit in Ihrem Empfinden. *

1 = am wichtigsten, 3 = am unwichtigsten

- ▾ Usability des Services (z.B. Verständlichkeit, Zuverlässigkeit, Schnelligkeit)
- ▾ Vertrauen zum Service (z.B. Glaubwürdigkeit, Seriösität, Überzeugung)
- ▾ Sicherheitsgefühl (z.B. Umgang mit Authentifizierungs-Daten)

Zurück Weiter

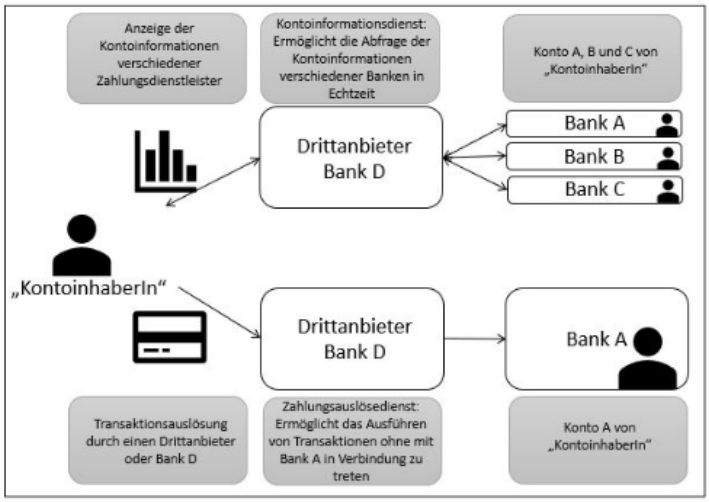
(Text ändern)

Auswirkungen der Payment Service Directive 2 (PSD2)

52 %

Teil 2: Open Banking

Erklärung von Open Banking



Teil 2 der Richtlinie regelt die **Öffnung der Kontoinformationen für Zahlungsdienstleister und Drittanbieter, auch genannt „Open Banking" oder „Access to Account (XS2A)"**. Dies darf **nur mit Ihrer Zustimmung** geschehen.

Die Inhalte von Open Banking sind für Sie als NutzerIn
-) die Möglichkeit verschiedene Konten verschiedener Banken in einer Plattform zusammenzuführen und dadurch alle Kontobewegungen und -stände gesammelt im Überblick zu behalten **(zu sehen in der oberen Hälfte der Abbildung)** oder
-) die Möglichkeit, dass Zahlungsdienstleister und Drittanbieter im Zahlungsverkehr, mittels Zugriffes auf eines Ihrer Konten, Zahlungen für Sie auslösen. **(zu sehen in der unteren Hälfte der Abbildung)**

Zurück Weiter

(Text ändern)

Auswirkungen der Payment Service Directive 2 (PSD2)

57 %

Wie gut fühlen Sie sich über die Möglichkeiten von Open Banking (Zugriff auf Ihr Konto durch Dritte mit Ihrer Zustimmung) informiert? *

- ○ sehr gut
- ○ gut
- ○ weniger gut
- ○ nicht gut

Zurück Weiter

(Text ändern)

UmfrageOnline.com ist kostenlos für Studenten.
Erstellen Sie jetzt Ihre eigene kostenlose Online-Umfrage!

Teilnahme fortsetzen »

Auswirkungen der Payment Service Directive 2 (PSD2)

82 %

Verwenden Sie Services, womit Sie Konto- und Transaktionsinformationen verschiedener Zahlungsdienstleister gesammelt in einem Dashboard anzeigen können? (sogenannte: Kontoinformationsdienste) *

z.B. Multibanking in George

- ● Ja, verwende ich
- ○ Nein, bin jedoch daran interessiert
- ○ Nein, lehne ich ab

Zurück Weiter

(Text ändern)

Teilnahme fortsetzen »

Auswirkungen der Payment Service Directive 2 (PSD2)

67 %

Wie bewerten Sie Services, womit Sie Konto- und Transaktionsinformationen verschiedener Zahlungsdienstleister gesammelt in einem Dashboard anzeigen können? *

	sehr gut	gut	weniger gut	nicht gut	nicht zu beurteilen
Usability des Services (z.B. Verständlichkeit, Zuverlässigkeit, Schnelligkeit)	○	○	○	○	○
Sicherheitsgefühl (z.B. Umgang mit Kontoinformationen)	○	○	○	○	○
Vertrauen zum Service (z.B. Glaubwürdigkeit, Seriösität, Überzeugung)	○	○	○	○	○

Zurück Weiter

(Text ändern)

UmfrageOnline.com ist kostenlos für Studenten.
Erstellen Sie jetzt Ihre eigene kostenlose Online-Umfrage!

Teilnahme fortsetzen »

Auswirkungen der Payment Service Directive 2 (PSD2)

62 %

Verwenden Sie Services, womit Sie Konto- und Transaktionsinformationen verschiedener Zahlungsdienstleister gesammelt in einem Dashboard anzeigen können? (sogenannte: Kontoinformationsdienste) *

z.B. Multibanking in George

- ○ Ja, verwende ich
- ☑ Nein, bin jedoch daran interessiert
- ○ Nein, lehne ich ab

Zurück Weiter

(Text ändern)

Teilnahme fortsetzen »

Auswirkungen der Payment Service Directive 2 (PSD2)

71 %

Aus welchen Gründen verwenden Sie Services, wie die Anzeige von Konto- und Transaktionsinformationen verschiedener Zahlungsdienstleister in einem Dashboard, bisher nicht? *

- [ ] Sicherheitsgefühl (z.B. Umgang mit Kontoinformationen)
- [ ] Usability der Services (z.B. Verständlichkeit, Zuverlässigkeit, Schnelligkeit)
- [ ] Vertrauen zum Service (z.B. Glaubwürdigkeit, Seriösität, Überzeugung)
- [ ] aus anderen Gründen

Zurück Weiter

(Text ändern)

UmfrageOnline.com ist kostenlos für Studenten.
Erstellen Sie jetzt Ihre eigene kostenlose Online-Umfrage!

Teilnahme fortsetzen »

Auswirkungen der Payment Service Directive 2 (PSD2)

76 %

Verwenden Sie Services, womit Sie Transaktionen durchführen (lassen) können ohne mit Ihrem Zahlungsdienstleister in Kontakt zu treten? (sogenannte: Zahlungsauslösedienste) *

z.B. PayPal, GooglePay, etc.

- (●) Ja, verwende ich
- ( ) Nein, bin jedoch daran interessiert
- ( ) Nein, lehne ich ab

Zurück Weiter

(Text ändern)

Auswirkungen der Payment Service Directive 2 (PSD2)

81 %

Wie bewerten Sie Services, womit Sie Transaktionen durchführen (lassen) können ohne mit Ihrem Zahlungsdienstleister in Kontakt zu treten? *

	sehr gut	gut	weniger gut	nicht gut	nicht zu beurteilen
Usability des Services (z.B. Verständlichkeit, Zuverlässigkeit, Schnelligkeit)	○	○	○	○	○
Sicherheitsgefühl (z.B. Umgang mit Kontoinformationen)	○	○	○	○	○
Vertrauen zum Service (z.B. Glaubwürdigkeit, Seriösität, Überzeugung)	○	○	○	○	○

Zurück Weiter

(Text ändern)

UmfrageOnline.com ist kostenlos für Studenten.
Erstellen Sie jetzt Ihre eigene kostenlose Online-Umfrage!

Auswirkungen der Payment Service Directive 2 (PSD2)

78 %

Verwenden Sie Services, womit Sie Transaktionen durchführen (lassen) können ohne mit Ihrem Zahlungsdienstleister in Kontakt zu treten? (sogenannte: Zahlungsauslösedienste) *

z.B. PayPal, GooglePay, etc.

- ○ Ja, verwende ich
- ✓ Nein, bin jedoch daran interessiert
- ○ Nein, lehne ich ab

Zurück Weiter

(Text ändern)

Auswirkungen der Payment Service Directive 2 (PSD2)

86 %

Aus welchen Gründen verwenden Sie Services, womit Sie Transaktionen durchführen (lassen) können ohne mit Ihrem Zahlungsdienstleister in Kontakt zu treten, bisher nicht? *

- [ ] Sicherheitsgefühl (z.B. Umgang mit Kontoinformationen)
- [ ] Usability der Services (z.B. Verständlichkeit, Zuverlässigkeit, Schnelligkeit)
- [ ] Vertrauen zum Service (z.B. Glaubwürdigkeit, Seriösität, Überzeugung)
- [ ] aus anderen Gründen

Zurück Weiter

(Text ändern)

UmfrageOnline.com ist kostenlos für Studenten.
Erstellen Sie jetzt Ihre eigene kostenlose Online-Umfrage!

Auswirkungen der Payment Service Directive 2 (PSD2)

90 %

Nehmen Sie seit September 2019 vermehrt diese Art von Services (z.B. Informationsportale, Vergleichsportale, Zahlungsauslöseportale) am Markt wahr? *

Services, welche für Sie Informationen sammeln und anzeigen oder Transaktionen auslösen ohne direktem Kontakt zu Ihrem Zahlungsdienstleister (Bankkonto)

- ( ) ja
- ( ) nein

Zurück Weiter

(Text ändern)

Auswirkungen der Payment Service Directive 2 (PSD2)

95 %

Abschließend persönliche Informationen

Bitte den zutreffenden Bereich Ihre Alters auswählen *

- ○ 14-17
- ○ 18-28
- ○ 29-38
- ○ 39-48
- ○ 49-58
- ○ 59-69
- ○ ab 70

Wohnhaft in... *

- ○ einer Landeshauptstadt
- ○ einer Bezirkshauptstadt
- ○ einer ländlichen Region
- ○ keine Angaben

Ihre höchste abgeschlossene Ausbildung ist? *

- ○ Pflichtschule
- ○ Fachschulabschluss
- ○ Akademischer Abschluss
- ○ Lehre oder Berufsausbildung
- ○ Matura
- ○ keine Angaben

Ihr berufliches Tätigkeitsfeld ist? *

StudentIn bitte auswählen, wenn dies vergleichsweise zum Beruf die überwiegende Zeit einnimmt

- ○ Tätigkeit in der Finanzbranche
- ○ anderer Tätigkeitsbereich
- ○ StudentIn
- ○ Tätigkeit mit Berührungspunkten zur Finanzbranche
- ○ nicht berufstätig
- ○ keine Angaben

Zurück | Fertig

(Text ändern)

Anhang D – online Fragebogen Antworten

1. **Bitte wählen Sie den Zahlungsdienstleister, von dem Sie vorrangig Dienstleistungen beziehen, und beantworten Sie die weiteren Fragen in Bezug auf diesen Zahlungsdienstleister.** *

.png .pdf .xls .csv

Anzahl Teilnehmer: 287

101 (35.2%): Erste Group Bank (inkl. Sparkasse)

88 (30.7%): Raiffeisenbank

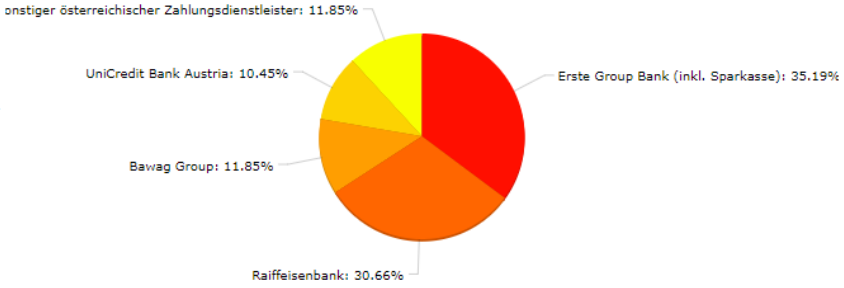
34 (11.8%): Bawag Group

30 (10.5%): UniCredit Bank Austria

34 (11.8%): sonstiger österreichischer Zahlungsdienstleister

- (0.0%): kein österreichischer Zahlungsdienstleister

- (0.0%): habe kein Bankkonto



2. **Haben Sie schon von der EU-Richtlinie „Payment Service Directive 2 (PSD2)“ gehört?** *

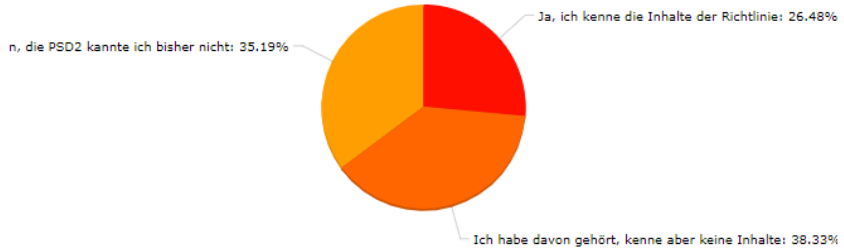
.png .pdf .xls .csv

Anzahl Teilnehmer: 287

76 (26.5%): Ja, ich kenne die Inhalte der Richtlinie

110 (38.3%): Ich habe davon gehört, kenne aber keine Inhalte

101 (35.2%): Nein, die PSD2 kannte ich bisher nicht

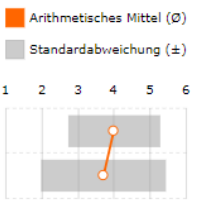


3. **Wie häufig benutzen Sie...** *

.png .pdf .xls .csv

Anzahl Teilnehmer: 287

	mehrmals täglich (1)		einmal täglich (2)		mehrmals wöchentlich (3)		einmal wöchentlich (4)		einmal monatlich (5)		nie (6)			
	Σ	%	Σ	%	Σ	%	Σ	%	Σ	%	Σ	%	Ø	±
...Services eines Zahlungsdienstl...	13x	4,53	14x	4,88	74x	25,78	82x	28,57	66x	23,00	38x	13,24	4,00	1,28
...Services eines Zahlungsdienstl...	41x	14,29	26x	9,06	82x	28,57	39x	13,59	25x	8,71	74x	25,78	3,71	1,73



4. **Wie gut fühlen Sie sich über die neuen Zwei-Faktor-Authentifizierungsmethoden der Payment Service Directive 2 informiert?** *

.png .pdf .xls .csv

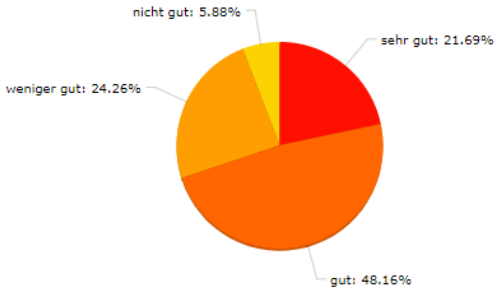
Anzahl Teilnehmer: 272

59 (21.7%): sehr gut

131 (48.2%): gut

66 (24.3%): weniger gut

16 (5.9%): nicht gut



5. **Welche Zwei-Faktor-Authentifizierungsmethode verwenden Sie vorrangig für einen Login oder eine Zahlungsfreigabe?** *

.png .pdf .xls .csv

Anzahl Teilnehmer: 272

74 (27.2%): die Eingabe einer mobile TAN die als SMS zugestellt wird

79 (29.0%): eine App mit Passwort oder Code/PIN

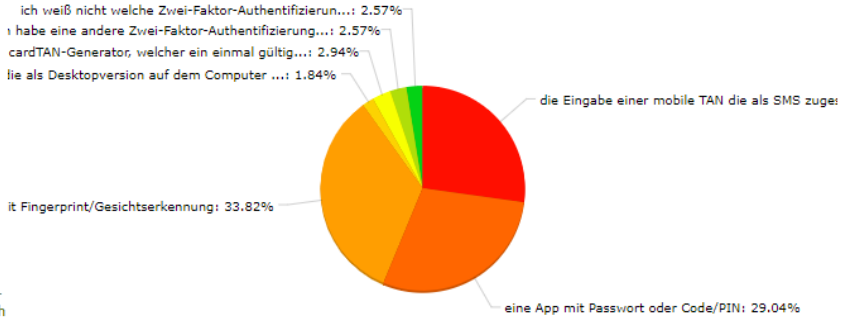
92 (33.8%): eine App mit Fingerprint/Gesichtserkennung

5 (1.8%): eine App, die als Desktopversion auf dem Computer installiert ist

8 (2.9%): einen cardTAN-Generator, welcher ein einmal gültiges Passwort zur Eingabe generiert

7 (2.6%): ich habe eine andere Zwei-Faktor-Authentifizierungsmethode in Verwendung

7 (2.6%): ich weiß nicht welche Zwei-Faktor-Authentifizierungsmethode ich verwende

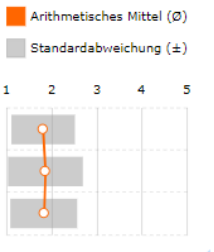


6. **Wie bewerten Sie Ihre verwendete Lösung zur Zwei-Faktor-Authentifizierung (Login und Zahlungsfreigabe)?** *

.png .pdf .xls .csv

Anzahl Teilnehmer: 265

	sehr gut (1)		gut (2)		weniger gut (3)		nicht gut (4)		keine Bewertung möglich (5)			
	Σ	%	Σ	%	Σ	%	Σ	%	Σ	%	Ø	±
Sicherheitsgefühl (z.B. Umgang mi...	84x	31,70	155x	58,49	20x	7,55	4x	1,51	2x	0,75	1,81	0,70
Usability des Services (z.B. Verstän...	101x	38,11	116x	43,77	36x	13,58	11x	4,15	1x	0,38	1,85	0,83
Vertrauen zum Service (z.B. Glaub...	88x	33,21	148x	55,85	22x	8,30	4x	1,51	3x	1,13	1,82	0,74

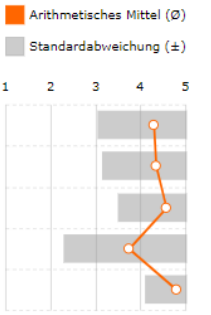


7. Treffen im Bezug auf Ihr verwendetes Service (Login und Zahlungsfreigabe) folgende Aussagen und Gründe zu, wenn Ja welche und mit welchem Hauptgrund? *

.png .pdf .xls .csv

Anzahl Teilnehmer: 265

	Sicherheitsgefühl (z.B. Umgang mit Daten) (1)		Usability des Services (z.B. Verständlichkeit, Zuverlässigkeit, Schnelligkeit) (2)		Vertrauen zum Service (z.B. Glaubwürdigkeit, Seriösität, Überzeugung) (3)		anderer Beweggrund (4)		trifft nicht zu (5)			
	Σ	%	Σ	%	Σ	%	Σ	%	Σ	%	Ø	±
Ich würde zu alternativen Zahlun...	8x	3,02	40x	15,09	10x	3,77	16x	6,04	191x	72,08	4,29	1,25
Ich würde eine andere Bank mit ...	11x	4,15	29x	10,94	12x	4,53	17x	6,42	196x	73,96	4,35	1,22
Ich mache zukünftig vermehrt Tr...	17x	6,42	5x	1,89	6x	2,26	15x	5,66	222x	83,77	4,58	1,08
Ich verwende Online Banking und...	6x	2,26	88x	33,21	18x	6,79	12x	4,53	141x	53,21	3,73	1,44
Ich verwende Online Banking und...	3x	1,13	8x	3,02	4x	1,51	9x	3,40	241x	90,94	4,80	0,71

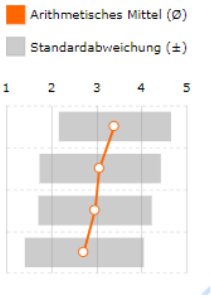


8. Wie bewerten Sie folgende Ausnahmemöglichkeiten der Zwei-Faktor-Authentifizierung (in Kurzform: 2FA)? *

.png .pdf .xls .csv

Anzahl Teilnehmer: 272

	sehr gut (1)		gut (2)		weniger gut (3)		nicht gut (4)		nicht zu bewerten (5)			
	Σ	%	Σ	%	Σ	%	Σ	%	Σ	%	Ø	±
die Möglichkeit des Setzens von Ausn...	15x	5,51	62x	22,79	64x	23,53	60x	22,06	71x	26,10	3,40	1,25
die Möglichkeit des Verzichts auf die ...	39x	14,34	67x	24,63	56x	20,59	57x	20,96	53x	19,49	3,07	1,35
die Möglichkeit zum Verzicht auf die ...	34x	12,50	81x	29,78	58x	21,32	60x	22,06	39x	14,34	2,96	1,26
die Möglichkeit zum Verzicht bei glei...	51x	18,75	97x	35,66	40x	14,71	45x	16,54	39x	14,34	2,72	1,33

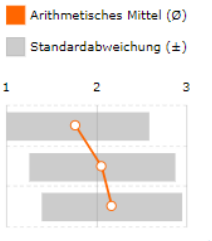


9. Reihen Sie folgende Sichtweisen in Bezug zur Zwei-Faktor-Authentifizierung (Login und Zahlungsfreigabe) nach der Wichtigkeit in Ihrem Empfinden. *

.png .pdf .xls .csv

Anzahl Teilnehmer: 272

	1.		2.		3.			
	Σ	%	Σ	%	Σ	%	Ø	±
Sicherheitsgefühl (z.B. Umgang mit Authentifizierung...	127x	46,69	81x	29,78	64x	23,53	1,77	0,81
Usability des Services (z.B. Verständlichkeit, Zuverlä...	82x	30,15	92x	33,82	98x	36,03	2,06	0,81
Vertrauen zum Service (z.B. Glaubwürdigkeit, Seriösi...	63x	23,16	99x	36,40	110x	40,44	2,17	0,78



10. **Wie gut fühlen Sie sich über die Möglichkeiten von Open Banking (Zugriff auf Ihr Konto durch Dritte mit Ihrer Zustimmung) informiert?** *

.png .pdf .xls .csv

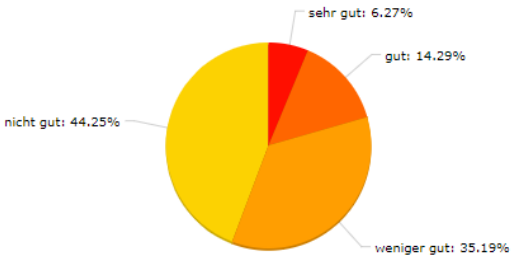
Anzahl Teilnehmer: 287

18 (6.3%): sehr gut

41 (14.3%): gut

101 (35.2%): weniger gut

127 (44.3%): nicht gut



11. **Verwenden Sie Services, womit Sie Konto- und Transaktionsinformationen verschiedener Zahlungsdienstleister gesammelt in einem Dashboard anzeigen können? (sogenannte: Kontoinformationsdienste)** *

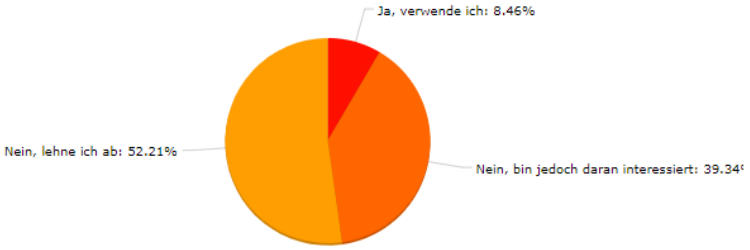
.png .pdf .xls .csv

Anzahl Teilnehmer: 272

23 (8.5%): Ja, verwende ich

107 (39.3%): Nein, bin jedoch daran interessiert

142 (52.2%): Nein, lehne ich ab

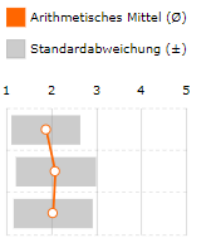


12. **Wie bewerten Sie Services, womit Sie Konto- und Transaktionsinformationen verschiedener Zahlungsdienstleister gesammelt in einem Dashboard anzeigen können?** *

.png .pdf .xls .csv

Anzahl Teilnehmer: 23

	sehr gut (1)		gut (2)		weniger gut (3)		nicht gut (4)		nicht zu beurteilen (5)			
	Σ	%	Σ	%	Σ	%	Σ	%	Σ	%	Ø	±
Usability des Services (z.B. Verständli...	8x	34,78	10x	43,48	5x	21,74	-	-	-	-	1,87	0,76
Sicherheitsgefühl (z.B. Umgang mit K...	5x	21,74	13x	56,52	4x	17,39	-	-	1x	4,35	2,09	0,90
Vertrauen zum Service (z.B. Glaubwü...	5x	21,74	14x	60,87	3x	13,04	-	-	1x	4,35	2,04	0,88



13. **Aus welchen Gründen verwenden Sie Services, wie die Anzeige von Konto- und Transaktionsinformationen verschiedener Zahlungsdienstleister in einem Dashboard, bisher nicht? ***

.png .pdf .xls .csv

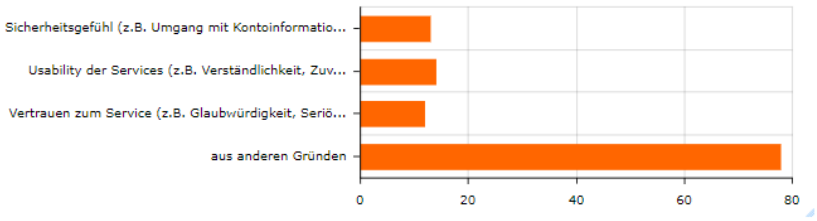
Anzahl Teilnehmer: 107

13 (12.1%): Sicherheitsgefühl (z.B. Umgang mit Kontoinformationen)

14 (13.1%): Usability der Services (z.B. Verständlichkeit, Zuverlässigkeit, Schnelligkeit)

12 (11.2%): Vertrauen zum Service (z.B. Glaubwürdigkeit, Seriösität, Überzeugung)

78 (72.9%): aus anderen Gründen



14. **Verwenden Sie Services, womit Sie Transaktionen durchführen (lassen) können ohne mit Ihrem Zahlungsdienstleister in Kontakt zu treten? (sogenannte: Zahlungsauslösedienste) ***

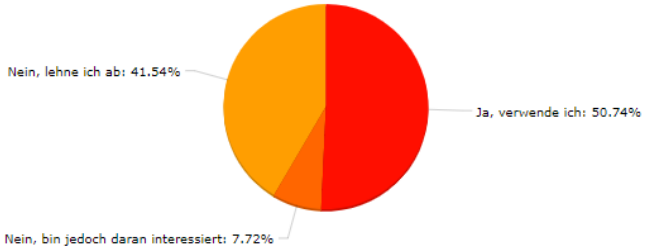
.png .pdf .xls .csv

Anzahl Teilnehmer: 272

138 (50.7%): Ja, verwende ich

21 (7.7%): Nein, bin jedoch daran interessiert

113 (41.5%): Nein, lehne ich ab

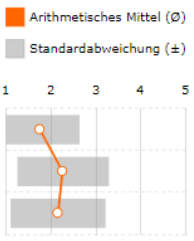


15. **Wie bewerten Sie Services, womit Sie Transaktionen durchführen (lassen) können ohne mit Ihrem Zahlungsdienstleister in Kontakt zu treten? ***

.png .pdf .xls .csv

Anzahl Teilnehmer: 138

	sehr gut (1)		gut (2)		weniger gut (3)		nicht gut (4)		nicht zu beurteilen (5)			
	Σ	%	Σ	%	Σ	%	Σ	%	Σ	%	Ø	±
Usability des Services (z.B. Verständli...	61x	44,20	62x	44,93	8x	5,80	3x	2,17	4x	2,90	1,75	0,89
Sicherheitsgefühl (z.B. Umgang mit K...	28x	20,29	69x	50,00	24x	17,39	10x	7,25	7x	5,07	2,27	1,03
Vertrauen zum Service (z.B. Glaubwü...	37x	26,81	66x	47,83	20x	14,49	7x	5,07	8x	5,80	2,15	1,06



16. **Aus welchen Gründen verwenden Sie Services, womit Sie Transaktionen durchführen (lassen) können ohne mit Ihrem Zahlungsdienstleister in Kontakt zu treten, bisher nicht?** *

.png .pdf .xls .csv

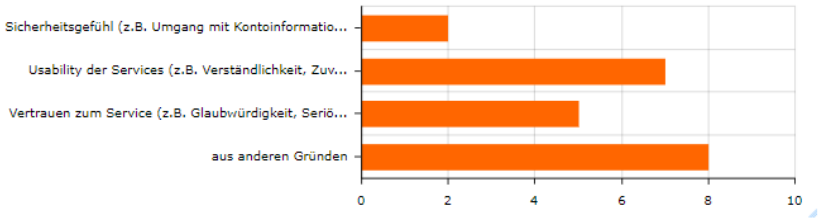
Anzahl Teilnehmer: 21

2 (9.5%): Sicherheitsgefühl (z.B. Umgang mit Kontoinformationen)

7 (33.3%): Usability der Services (z.B. Verständlichkeit, Zuverlässigkeit, Schnelligkeit)

5 (23.8%): Vertrauen zum Service (z.B. Glaubwürdigkeit, Seriösität, Überzeugung)

8 (38.1%): aus anderen Gründen



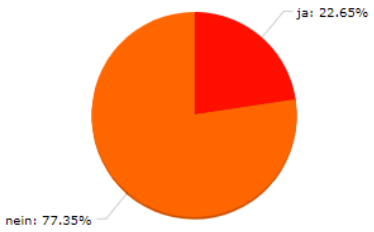
17. **Nehmen Sie seit September 2019 vermehrt diese Art von Services (z.B. Informationsportale, Vergleichsportale, Zahlungsauslöseportale) am Markt wahr?** *

.png .pdf .xls .csv

Anzahl Teilnehmer: 287

65 (22.6%): ja

222 (77.4%): nein



18. **Bitte den zutreffenden Bereich Ihre Alters auswählen** *

.png .pdf .xls .csv

Anzahl Teilnehmer: 287

1 (0.3%): 14-17

51 (17.8%): 18-28

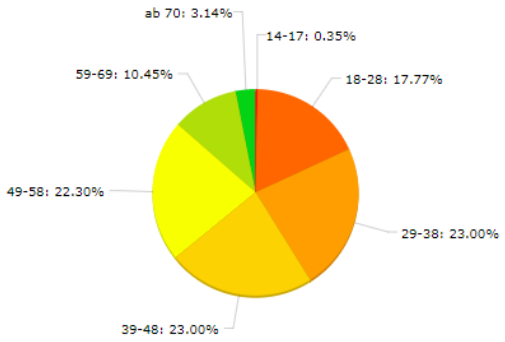
66 (23.0%): 29-38

66 (23.0%): 39-48

64 (22.3%): 49-58

30 (10.5%): 59-69

9 (3.1%): ab 70



19. **Wohnhaft in...** *

.png .pdf .xls .csv

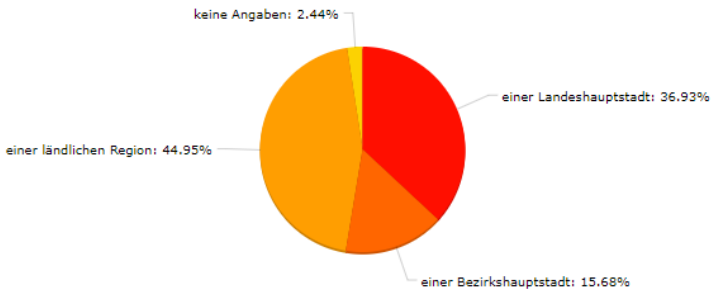
Anzahl Teilnehmer: 287

106 (36.9%): einer Landeshauptstadt

45 (15.7%): einer Bezirkshauptstadt

129 (44.9%): einer ländlichen Region

7 (2.4%): keine Angaben



20. **Ihre höchste abgeschlossene Ausbildung ist?** *

.png .pdf .xls .csv

Anzahl Teilnehmer: 287

8 (2.8%): Pflichtschule

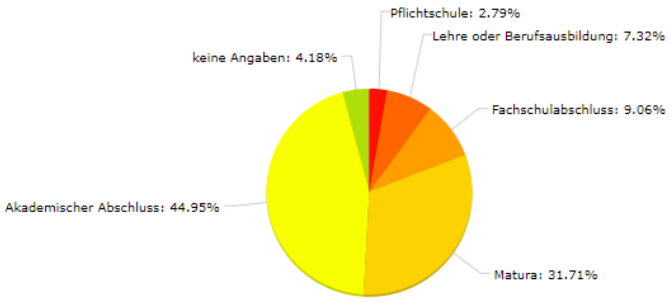
21 (7.3%): Lehre oder Berufsausbildung

26 (9.1%): Fachschulabschluss

91 (31.7%): Matura

129 (44.9%): Akademischer Abschluss

12 (4.2%): keine Angaben



21. **Ihr berufliches Tätigkeitsfeld ist?** *

.png .pdf .xls .csv

Anzahl Teilnehmer: 287

56 (19.5%): Tätigkeit in der Finanzbranche

31 (10.8%): Tätigkeit mit Berührungspunkten zur Finanzbranche

154 (53.7%): anderer Tätigkeitsbereich

13 (4.5%): nicht berufstätig

22 (7.7%): StudentIn

11 (3.8%): keine Angaben