UNIVERSITY OF TARTU
Faculty of Social Sciences
School of Economics and Business Administration

Abdullah Cem Açıkgöz

SECURITY ANALYSIS OF OPEN BANKING INTEGRATIONS AND AWARENESS OF ESTONIAN BANK ACCOUNT HOLDERS ON THESE RISKS

Master's thesis

Supervisor: Isaac Nana Akuffo

Tartu 2021

Name and signature of supervisor: Isaac Nana Akuffo

Allowed for defense on ....

I have written this master's thesis independently. All viewpoints of other authors, literary sources and data from elsewhere used for writing this paper have been referenced.

--- (signature of author)

Abstract

This thesis aims to identify the security risks of open banking integrations as well as the awareness level of Estonian bank account holders on these risks. For these purposes, open banking Application Programming Interfaces (APIs) were analyzed, and how Third-Party Providers (TPPs) can create applications by using these APIs was pointed out. For this analysis, a qualitative method was the preference. Confidential data security/privacy and the man-in-the-middle attack were the two essential risks identified. To understand the awareness level of Estonian bank account holders, 202 people were surveyed. As a sampling technique, convenient sampling was used. The quantitative method was employed to analyze the data. The findings indicated that while the vast majority of Estonian bank account holders are more aware of General Data Protection Regulation (GDPR) related concepts, more than half of them do not know what the man-in-the-middle attack is. The results also showed that men are more aware than women in both GDPR and MITM attack. Moreover, there was a positive and significant correlation between awareness in GDPR and MITM attack. The further analysis of the unaware group for MITM showed that they might be the potential victims for man-in-the-middle.

Table of Contents

List of acronyms

TPP – Third Party Provider

AIS – Account Information Service

PIS – Payment Initiation Service

MITM – Man in the Middle Attack

API – Application Programming Interface

PSD – Payment Service Directive

AISP – Account Information Service Provider

PISP – Payment Initiation Service Provider

GDPR – General Data Protection Regulation

PSU – Payment Service User

OB – Open Banking

IT – Information Technology

1. Introduction

Today, with the rapid development of technology in every field, as in many industries, breakthroughs are made in the finance sector to modernize, digitalize and, provide quality and innovative services. The finance sector's digitalization finds its roots in the early 80s with internet banking's introduction by the Bank of Scotland (Tait & Davis, 1989). However, in the 80s, since the vast majority of customers were not fully aware and ready for internet banking, internet banking was interrupted (ibid). In the 90s, the fast pace in information technology's development encouraged banks to launch internet banking onto the market again (ibid). After the second launch's success and the trend in using the internet bank among customers, the banking industry organically redefined its standards (ibid). As years passed, the number of internet bank users increased to a great extent. Therefore, to stay in the competition, having an internet bank became necessary for the banks.

After internet banking became mainstream in the early 21st century, physically linked traditional banking activities started to leave their place to electronic-based service channels (Omarini, 2018). Digitalization went beyond internet banking and, the concept of mobile banking has been also a part of everyday life. Banks invested more in digitalization and innovation. However, their complex architectures and slow speed of development positioned banks to not meeting customer demands (Omarini, 2018). Businesses seeking to become a part of banking activities have seen it as a great opportunity (ibid). These businesses formed a new industry named fintech or financial technology.

Fintech or financial technology, refers to a cross-disciplinary industry that aims to give fast, simple, and improved financial services (Leong, 2018). Competing with traditional financial services with their technological power, fintech firms act with the philosophy of facilitating their customers' lives over the world (ibid). Fintech firms, with their practicality, price advantage, customized user experience and, innovative services, have a prominent effect beyond expectations (Zveryakov et al., 2019).

For the benefit of the European fintech industry, the most recent regulation is the implementation of the new EU Payment Service Directive (PSD2). Open Banking (also called API Banking), which is seen as an integral part of the developments taking place with PSD2, is defined as banks and their affiliates opening their data to the third parties via API (Zachariadis & Ozcan, 2017). European Union targeted increasing competition, transparency, innovation, and creating new opportunities for potential businesses with open banking. The power of accessing core bank services leads new third-party providers (TPP) to emerge to build a sophisticated user experience (Gozman et al., 2018). With a more digitalized way, the usage of traditional banking continues to decrease. People start using the new platforms which use the banks' services. At this phase, the matter of trust and convenience plays a significant role. In the battle between the new service providers, the ones that can build the feeling of security and practicableness will gain a victory (Dratva, 2020).

Despite the many benefits of open banking, the emergence of new fintech companies brings along some concerns. Particularly the access of third parties to core banking services raises security concerns. The security part, which was previously only under the control of banks, will be a prominent matter for TPPs.

In the current literature, studies are mostly for the security of open banking APIs. There is no comprehensive study anatomizing these risks, although few papers mention them. For instance, "The security of access to accounts under the PSD2" by Wolters and Jacobs is a study that touches upon the potential danger of TPPs accessing to account information of users theoretically (Wolters & Jacobs, 2019). However, this study is not clarifying the risks thoroughly.

Understanding the possible security risks of open banking integrations is quite crucial. This cruciality arises from TPP access to customers` financial data. The more worrying part is TPPs can initiate a payment on behalf of their customers. Therefore, any misbehavior or vulnerability of TPPs can cause the leakage of confidential information and financial loss for customers.

As mentioned earlier, most studies theoretically mention the risk of TPPs accessing financial data. The worse is none of the current studies focuses on the risk of financial loss. This study targets to shed light on these risks and explain them step by step.

The essential purpose of this study is to point out the security risks of open banking integrations and to show the awareness level of Estonian bank account holders regarding this matter. For this purpose, open banking APIs are analyzed and Estonian bank account holders are surveyed.

1.1. Research Questions

In this thesis, the effort goes to find the answers to the following research questions:

1. What are the security risks of open banking integrations?
2. To what extent Estonian bank account holders are aware of security risks?

The rest of the paper consists of literature review, methods and data, data analysis and interpretation, discussion of findings, conclusion, references and appendices.

2. Literature Review

This part of the thesis overviews related scientific articles to create a basic understanding of open banking and security concepts. It is vital to explain respecting concepts to make readers more familiar with the research topic. Additionally, this part makes readers comprehend the absence of extensive study on this topic by reviewing related work.

2.1. General Concepts

As mentioned before, explaining necessary concepts is important for readers of the thesis. So, this part focuses on creating a basis for readers to understand the background of the research topic.

2.1.1. PSD2

PSD2 - Payment Service Directive is a revolutionary set of legal infrastructure rules that determine the method and functioning of new applications to be developed between institutions and third-party service providers in the UK and the European Union as of January 13, 2018 (Scheja & Machielse, 2019). It is the second version of the Payment Services Directive designed by the European Union countries. It covers various topics from online payment methods to the information needed during payment for 28 EU member states (ibid). In essence, PSD2 expands the scope of PSD. For example, PSD2 opens the way to make transactions in third countries for a payment service provider in any country of the EU (Yawe & Mukisa, 2020). It also defines the cooperation and sharing between financial institutions and third-party payment service companies (ibid). To make electronic payments more secure, PSD2 offers advanced security measures to be implemented by all payment service providers, including banks (ibid). Moreover, PSD2 encourages the development of innovative applications with low costs (Haubrich, 2018).

2.1.2. The notion of Open Banking

Open banking -the essential component of PSD2- stands for a system that allows third-party service providers to access users' financial information and transactions within their consents (Farrow, 2020). In parallel to PSD2's objectives, the development of new financial products, increasing the transparency and competition in the finance sector, improving user experience, increasing users' control on their data and, enabling banks to reach a broader client base are the open banking's targets (Premchand & Choudhry, 2019).

There are three main actors in open banking services. The first party is the customer that refers to payment service user (PSU) in payment systems literature. PSU is a natural or legal entity initiating the payment order or benefiting from the payment service. The second party is the banks where the customer's payment account is available and the last party is the third-party providers where the customer's data is shared.

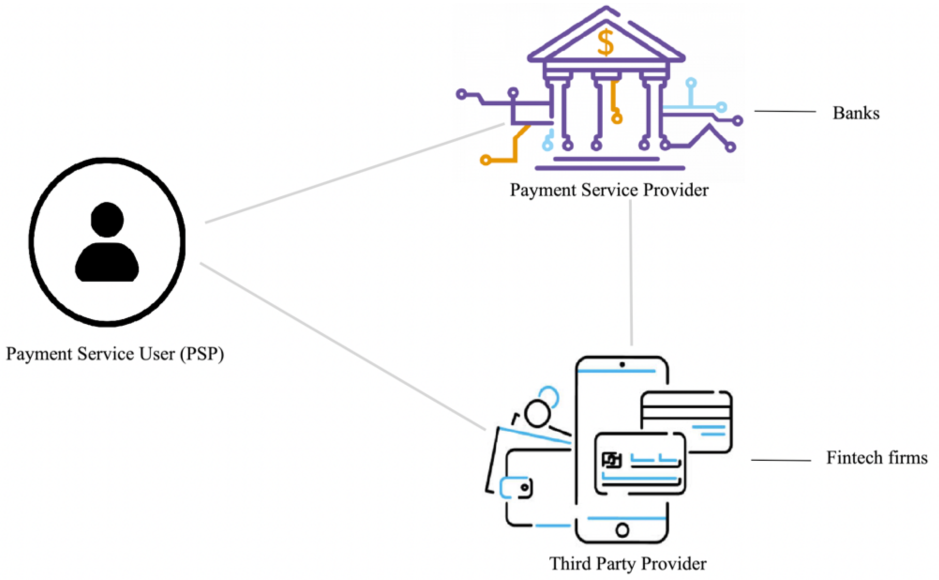


Figure 1: Parties in the open banking ecosystem. Compiled by author

Account information service (AIS) and payment initiation service (PIS) are the two primary open banking categories. These services facilitate the emergence of payment initiation service providers (PISP) and account information service providers (AISP). Third party-providers that obtain AISP and/or PISP license can benefit from AIS and PIS to create applications (Bär & Mortimer-Schutts, 2020).

Open banking services promise to manage accounts in different banks in a single interface, reduce transaction costs, and benefit from an integrated payment market for customers (Dratva, 2020). The benefits of these services for banks are customer intelligence and financial risk management, better targeting on a customer basis, thus generating more revenue from customers (Döderlein, 2018).

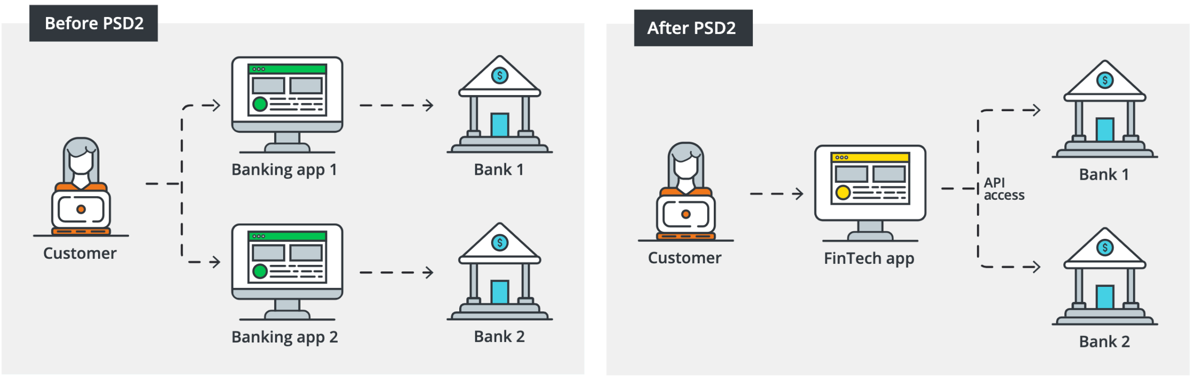


Figure 2: What PSD2 brings with account information service. Compiled by author.

2.1.3. Application Programming Interface (API)

Keeping in mind that another name of open banking is API banking, having at least a basic knowledge about API helps to understand the operating mechanism of open banking.

API is an interface that allows outside/remote access to the functions owned by an application, platform, or service within the permitted limits (Sagdeo, 2018). It is accurate to say API enables two applications to communicate with each other.

The essential purpose of API usage is to open methods of an application to other applications. It eases to meet the remote data and information requests quickly. In this way, remote users who are allowed to operate in a single application can benefit from particular parameters. API generally serves to process real-time data one by one (Meng et al., 2018). The server processes the input with or without parameters sent by the server via the API and returns a result set or just a success notification (ibid). Updates to only a limited part of the data require a parameter. API, on the other hand, ensures that these operations are both fast and practical (ibid).

To make API more understandable for non-technical readers, we can use the classic restaurant example. In a restaurant, we can consider the customer as an information/service requestor and the restaurant as an application that provides the information/service. When the customer requests information/service, the waiter is responsible for delivering this request. The waiter talks with a customer and conveys the customer request to the restaurant. When the service is ready, the waiter brings this service to the customer. So, two parties -customer and restaurant- communicate with the help of the waiter. Here the role of the waiter is the same as API.

2.1.4. Financial Technologies (Fintech)

As the name suggests, fintech, which has become increasingly popular in the 21st century, is the name given to technological solutions/companies in the financial sector (Ryu & Ko, 2020). These companies, combining finance and technology to provide easy and fast financial services, use agile methodologies (ibid). The finance sector is one of the industries that mostly affected by technological developments. This development prompts the finance sector to reshape and create new opportunities. Thanks to these new opportunities, fintech firms enter areas where big players cannot focus much (Llewellyn, 2018).

Fintechs mainly operate in the field of payment systems. Besides, they provide services like lending, personal finance, retail and corporate investments, crowdfunding, asset management, and money transfer (Imerman & Fabozzi, 2020). Fintechs mainly (Knewtson & Rosenbaum, 2020):

- create digital products in the banking sector with personalized solutions
- offer more technological and innovative products and services by focusing on more customer experience
- provide a competitive price advantage
- offer alternative services in the finance sector.

As of 2019 April, the estimated number of fintech firms in the world is more than 3850 (European Parliament. Directorate General for Internal Policies of the Union., 2019). Only in the European Union, the number of fintech companies exceeds 1000 (ibid). In the EU, it should not be a surprise to see an increase in the number of these companies due to the charm of this industry and open banking implementation.

2.1.5. GDPR and Data Security

The General Data Protection Regulation (GDPR) is a regulation created across Europe to protect the personal data of EU citizens (McDowell, 2019). GDPR, which has entered into force in European Union member countries since 25 May 2018, is about ensuring the security of personal data existing in large institutions and organizations in the European Union member countries within the framework of the rules specified in the regulation (Li & Saxunová, 2020). The GDPR covers all businesses that host the personal data of their citizens within the borders of the European Union (Hsu, 2018). Even if the company's location is not located within the European Union, it is held responsible for the regulation because it collects the citizens' data (ibid).

It is not allowed to process personal data unless it is done as specified in the regulation or has explicit consent from the data subject (data owner). The person concerned has the right to revoke this consent at any time. The GDPR also includes data stored in the past (Hernández et al., 2019). Harsh penalties and sanctions await businesses that do not comply with the GDPR. If the company does not comply with GDPR regulations, it has to pay up to 20 million Euros or 4% of its revenue depending on which one is higher (Skendzic et al., 2018).

For companies, complying with GDPR is not sufficient to become trustable. Another important concept for them is data security. Data security is defined as the protection of data against unauthorized access (Kumar et al., 2018). The most important focus in data security is to protect personal or corporate data while ensuring its privacy and verifying its integrity (ibid). Data comes first among the assets owned by institutions (Mukherjee, 2019). Institutions can compile, change, acquire value, sell, turn into a product/service, or share their data (ibid). In this way, they earn income. As always, cyber attackers try to access this data and illegally earn revenue from this data (ibid). Unauthorized access to data causes many problems for companies or individual users (Kamiya et al., 2018). The most common cyber-attacks are theft of bank account information, theft of customer information in the database, and the encryption of data to demand a ransom (ibid).

2.1.6. Man in the Middle Attack

Man in the middle attack is an attack method that includes listening to the communication between two connections and capturing various data or changing data (Jain et al., 2016). In MITM, communication between the two parties may be interrupted. Moreover, misleading communication may be created. Capturing and manipulating packets on the network can summarize this attack type (ibid).

In wireless networks, sheer broadcasted packets lead attackers to intercept packets without any preprocessing (Mallik, 2018). For this reason, areas that provide free Wi-Fi are the most suitable areas for MITM attacks (ibid). The contents of unencrypted packages can be easily read. Attackers in Wi-Fi areas direct network traffic to pass over them. Thus, the traffic of the people on that network starts to flow through the attacker (ibid). The attacker who captured this traffic can achieve many personal data like login credentials.

We can give a postman example to explain it better. When someone wants to send a letter to his friend, he puts the letter in a mailbox. Later on, the postman who received the letter can read it or even change it. However, neither person nor his friend knows about this situation since the postman ensures communication. In this example, the MITM is the postman, and reading or changing the letter is the attack.

Considering the hazardous results of the MITM attack, companies must secure their web applications (Imerman & Fabozzi, 2020). It is also significant for users to be aware of this threat and take precautions.

2.2. Related Work

In this part, we overview the studies which mention the security concerns of open banking integrations. When discussing open banking security, studies mostly focus on open banking itself, not the integration part. Therefore, the number of studies in the current literature is not satisfying enough to attract attention to integrations' security concerns. Additionally, these studies mostly touch upon the GDPR related issues theoretically.

The structure of open banking security itself covers access to APIs, authentication, and authorization. In addition to licenses, third parties need to have related certificates to access the APIs. Besides, since the customers need to use two factor authentication for authentication and authorization, open banking looks secure from its perspective(Basel Committee, 2019). However, as explained before, to say using open banking is secure, we should also be certain about TPPs' security and how they build applications.

2.2.1. Data Privacy and Security in Open Banking

According to Wolters and Jacobs (2019), there are serious concerns regarding open banking security due to the third party's involvement. They claim the protection of personal data is not entirely met (ibid). There are many restrictions on access to accounts, and the GDPR refers to the provision of payment services (ibid). The account information service concept, however, is broad and covers a wide variety of services. Even though it helps the market to grow and provide innovative services for users, there is no clear privacy aftermath that can be originated from the benefiting of a large amount of account information (ibid). For these reasons, they believe the highest priority for PSD2 is the development of the market, not the privacy of the users (ibid). They explicitly mention, security and the privacy of the users are highly dependent on the PISPs and AISPs (ibid). Based on PSD2, TPPs are trustable if they hold the required licenses and certificates. But Wolters and Jacobs believe this might not be enough and result in data leakage (ibid).

In another study, Romānova, et al., (2018) also described their worries that result from the sharing of personal data with third parties. They also believe data protection and privacy are not the top priority of PSD2 (ibid). Unclarity regarding accountability for security issues is another criticism of them for PSD2 (ibid). Thus, the reputation of PSD2 and open banking might fall into disrepute. In their study, together with addressing the security concerns, they also conducted interviews with 263 people to understand the security, risk, and privacy perceptions of users (ibid). The results showed that users care most about security (with a score of 2.11 out of 5). On the other hand, they give the lowest importance to privacy (with a score of 1.91 out of 5).

Kottayil (2020), in his study, also criticizes open banking regarding consumer security. He highlights the absence of a diffusive liability model in case of data leakage. According to Kottayil, PSD2 does not have enough security and privacy protocols (ibid). He suggests PSD2 build a conceptual model to protect the consumers. Otherwise, he believes open banking's potential can be misused and, consumers may encounter new security threats such as fraud and scams (ibid).

2.2.2. Man-in-the-middle Attack and Risk of Unauthorized Payments in Open Banking

Unfortunately, in the current literature, the number of people who see the man in the middle attack risk for open banking is quite limited. For instance, the author checked Business Source Complete, Scopus, Web of Science, ScienceDriect, Google Scholar databases with man-in-the-middle attack and open banking keywords together, results do not provide much study which include these two concepts together and they explain MITM in other fields. For example, one study (Luvanda et al., 2014) focuses on the MITM within the context of mobile applications. Since we are specifically interested in MITM in OB there are not many studies to overview.

Most researchers touched upon only the data security and privacy parts when examining open banking risks. Some of them also see unauthorized transactions as a risk but as mentioned earlier only a few studies discuss man-in-the-middle attack risk. We believe the reason for such scarcity results from the trust in authentication security of open banking. However, only authentication security is not sufficient to secure the transactions.

Steve Mansfield-Devine’s article (2016) is one of the rare studies that address the risk of a man-in-the-middle attack in the open banking system. In his work, benefiting from the interview with Andrew Whaley, he theoretically explains how this type of attack can occur (ibid). Again, the root cause of such a risk is involvement of third parties. Differing from the data security and privacy concerns, when a man-in-the-middle attack occurs, the financial loss is a matter of question. Even though banks check the identity of the third parties with the help of certificates, it does not guarantee the correctness of the data which is assumed to be sent by a particular TPP (ibid). To make it more specific, after authentication of the user, when the third party wants to initiate a payment, it prepares the request and sends it to a corresponding bank. If man-in-the-middle manages to interfere before the request reaches the bank, he will find a chance to edit the request. In this request editing, a man-in-the-middle can change the creditor IBAN to which the money goes and keep the TPP identifier the same. During this process, since a customer is not aware of this change, the money goes to a different IBAN from the one customer/TPP intends to send the money.

In its report (2018), Institute of International Finance points out the risks of the unauthorised payments which may induce financial loss. By unauthorised payments, they refer to the payments which are made without the permission of customers (ibid). They explain that such transactions are most likely to occur if authentication credentials are captured by unwanted parties(ibid). However, this report does not take into account that even if login credentials are accessed by unwanted parties, it is still not possible to complete payment without user confirmation unless the customer's bank exempts this rule.

3. Methods and Data

In this part of the thesis, researcher explains the appropriate methodologies which are used for the analysis. In addition, data that is used for analysis is defined.

There are various methods to carry out researches in the academic world. One of the most prominent matters of research is choosing a suitable research method. Thus, the methodology should be determined first when deciding on research. In the following part three different research methods are evaluated and chosen for the data analysis. The study employed the mixed method research approach (qualitative and quantitative).

3.1. Research Approach

Qualitative research is a method in which qualitative data collection methods such as observation, interview, and document analysis are used (Choy, 2014). Researchers follow the qualitative approach to reveal perceptions and events realistically and holistically in the natural environment (Moffatt, 2015). This approach prioritizes researching and understanding social phenomena within the environment they connect to, with an understanding based on theorizing. In qualitative research, the collected answers are essentially not numerical answers.

Qualitative research method has the following limitations (Atieno, 2009). First of all, it does not provide a statistical representation of the collected data (ibid). Responses with this form of research cannot usually be measured. Only comparisons are possible. Secondly, the limited sample size of the research may be problematic in collecting authentic data (ibid). Different viewpoints are also needed to avoid making a costly mistake when making an important decision. Lastly, since qualitative research focuses on individual experiences, the findings are almost impossible to replicate (ibid). Tomorrow, even the same person will have a different viewpoint than they have today (ibid). That implies that it can be tough to verify the data obtained through qualitative research, which can lead some to doubt the conclusions that researchers generate through this method.

Despite its limitations, the author benefits from the qualitative approach in open banking documentation analysis since document analysis is a dimension of qualitative method.

Quantitative research, on the other hand, is a type of research that can make observations, measure, and express them numerically by objectifying the events and facts

(Sukamolson, 2005). The purpose of quantitative research is to observe the behavior of individuals in society, to measure objectively utilizing experiments, and to explain with numbers (ibid). To interpret the connections between the facts, statistical data are taken into consideration and, the results are expressed numerically. Since this method is based on numbers, it is necessary to determine the sample representing the event or phenomenon completely and to ask the right questions.

As in qualitative research approach, quantitative research has some limitations (Queirós et al., 2017). First of all, qualitative research does not care about people's motivation when sharing an opinion or making a decision (ibid). The objective of the information gathering process is to paint a picture of what is happening in the selected demographic at that time. Secondly, quantitative research does not give participants the option to review responses (ibid). Even if the information seems confusing or is invalid, the answers given to researchers must stand alone. The quantitative option has very few opportunities to ask for clarity instead of following a tangent as other methods use. Researchers always face the risk that the responses or features given in a quantitative study are not an accurate representation of the entire population (ibid). Because of the necessary assumptions for this work, it is relatively easy to come to false conclusions or correlations. Even the randomized sampling that takes place is not 100 percent accurate to remove bias from the equation.

Despite the limitations of the quantitative approach, the author benefits from it. This mainly stems from the need of data collection and analyzing the collected data statistically.

A mixed approach is a research approach in which the researcher integrates two data sets collected as quantitative data (closed-ended) and qualitative data (open-ended) to understand research questions and then draws conclusions using the advantages of merging these two data sets (Azorín & Camero, 2010). The basic assumption of this approach is that it has more advantages for the researcher to combine statistical trends (quantitative data) with stories and personal experiences (qualitative data) compared to using any of these methods alone (ibid). Compared to qualitative and quantitative approaches, the mixed approach has fewer limitations.

To sum it up, for this thesis, data is collected in a quantitative way since it allows to collect a good amount of data. Also, to analyze the collected data and generalize the results, the author makes use of the quantitative approach. Since there is also a need for document analysis, the author also draws on a qualitative approach. Therefore, based on the characteristics of the research, it is correct to say that the mixed approach is the selected research approach.

3.2. Questionnaire and Data Collection

This thesis benefits from the book “Research Methods for Business students” to create a questionnaire (Saunders et al., 2009). In the book, it is suggested to have a roadmap to build a well-organized questionnaire. First of all, the researcher should know what kind of data is required and what kind of questions should be asked. Secondly, the researcher needs to determine how he can reach to respondents.

The book states that two types of questionnaire designs decide the way to collect responses from respondents. The first type is interview-administrated, in which the researcher conducts interviews with the respondents one by one. The second type is self-administrated, in which respondents fill the questions by themselves without the researcher's involvement. Considering that reaching out to all the respondents is so time taking and costly, the author decided to choose a self-administrated approach. This approach eases to collect responses from a large number of respondents in a short time. Moreover, this approach lets respondents answer the question without any impact in the absence of the researcher. To expedite the data collection process, the author chose to held the questionnaire online.

In order not to take so much time of the respondents, the author designed the survey with close-ended questions. In the questionnaire, it is decided to have three different types of questions. The first group of questions is demographic questions. With these questions such as age, gender and, country of nationality, understanding the demographic pattern of respondents is aimed. The second group of questions is general questions. These questions are asked to figure out if respondents have Estonian bank account and for how long they are the customer of the bank, how frequently they shop online, which payment methods they prefer and what challenges they face in online shopping. The last group of questions is asked to understand Estonian bank account holders’ security awareness level. If they heard about the man-in-the-middle attack or if they have entered their internet bank login credentials into another website are the example of this group of questions.

The author used google forms to prepare the online questionnaire. After it was created, the author shared it with people.

3.3. Sample size and sample technique

The sample of the research consisted of Estonian bank account holders. In the sample there are people from different professions, educational background and social classes. To reach out all the people in the sample, the author used different channels. The survey shared in the social media groups. Also, it was sent in the emails to different companies. The survey was open for answers in Estonia from 1 February 2021 to 5 March 2021. In total, 213 people shared their responses. The number of people who specified that they do not have Estonian bank accounts was 11. Since this survey is only interested in Estonian bank account holders, the number of valid responses for the survey is accepted as 202. Convenient sampling was the sampling technique to reach out all 213 people.

3.4. Ethical standards

To follow the ethical standards, all the participants were communicated that this research is for study purposes and none of their responses are shared with any other individual or institution. None of the respondents were forced to involve in the research. The purpose of the study was shared with the respondents. Thanks to an online questionnaire, respondents were not under the influence of the researcher or any other party. The researcher did not take any action to manipulate the results. Also, while selecting the sample, the author did not intend to find a specific group of people.

3.5. Open Banking Documentations

As mentioned earlier, the author benefits from the publicly available open banking documentations. The reason to examine these documents is because TPPs create the applications based on them. PSD2 mandated banks to create these documentations and share them publicly so that TPPs can benefit. Since PSD2 introduced a standard for these documentations, there is no need to examine the documentation of all banks in Europe. For that reason, the author decided to analyze the documentation of three banks which have operations in Estonia. It is correct to say that for the selection of these banks, purposive sampling is used since these can be considered as the representatives of all banks in Europe. In the analysis, the author explains the usage of APIs and what kind of risks are involved with this usage.

4. Data Analysis and Interpretation

The author divides this part into two categories as the overview of open banking APIs and the evaluation of the online questionnaire. In the first part, the author explains the general structure of open banking APIs and present some visuals for payment flow by using PIS. In the second part, the author displays the results of the questionnaire.

4.1. The Overview of Open Banking APIs

In this part, the author reviews and explains the publicly available open banking APIs of primary banks which operate in Estonia (Swedbank, SEB, and LHV). It is significant to get the readers familiar with APIs to understand the next parts. Because sample models in the empirical presentation are built based on the open banking API. Since the general structure of open banking API is standard for LHV, SEB, and Swedbank, the author does not examine these singly. Instead, the explanation covers the general structure.

Open banking APIs consist of three major parts. These are OAuth, account information services, and payment initiation services.

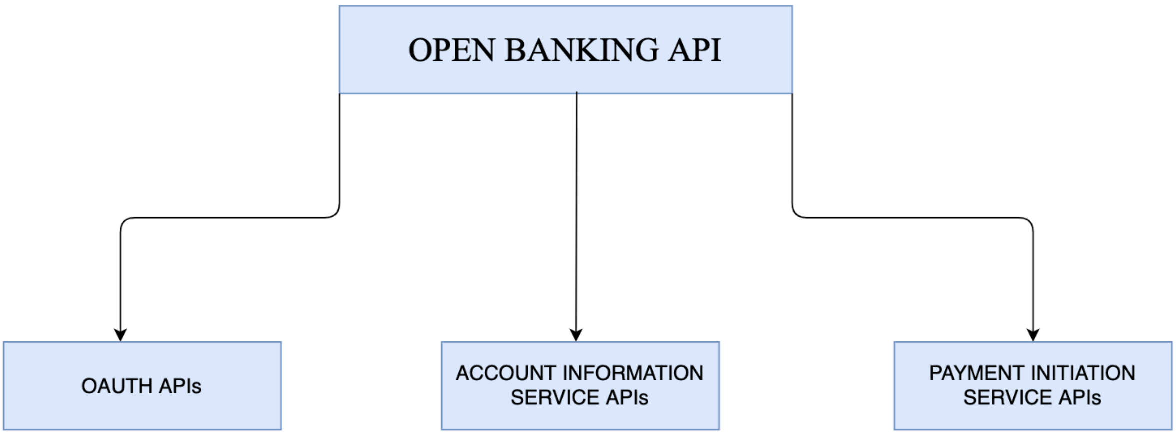
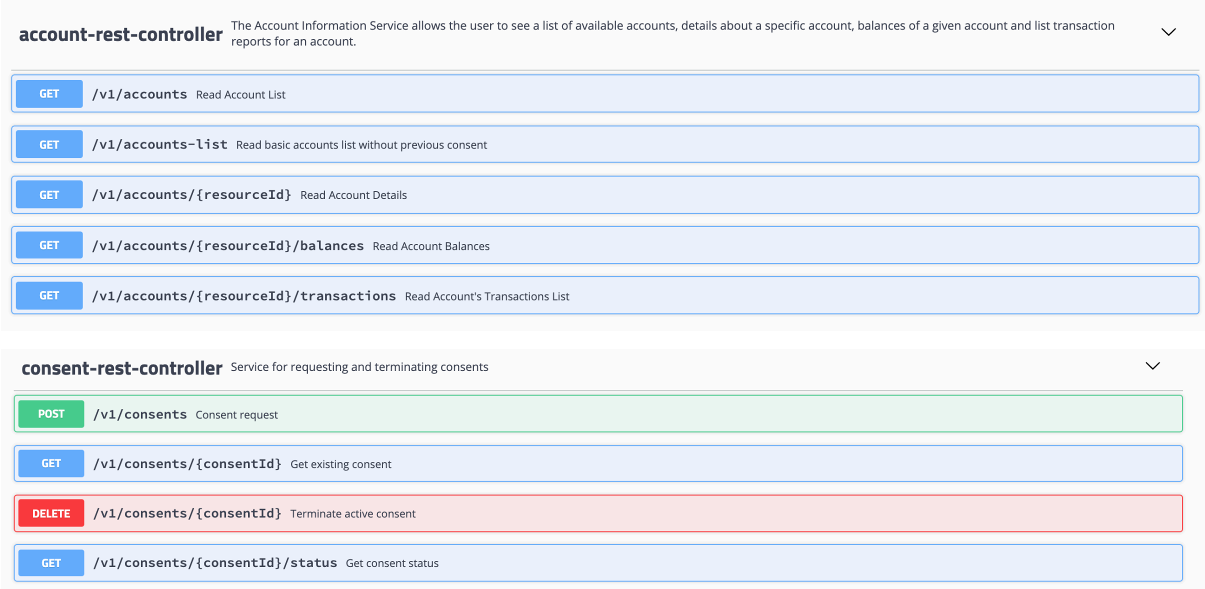

OPEN BANKING API
OAUTH APIs
ACCOUNT INFORMATION SERVICE APIs
PAYMENT INITIATION SERVICE APIs

Figure 3: The overview of open banking API. Compiled by author.

OAuth refers to the authorization. This part is necessary to use the other two services. It lets the user log in as well as checks the identity of TPP. There are two different approaches to log in the user. The first one is the redirect approach, in which the user is redirected to the corresponding bank's page to enter his credentials and confirm the login with a security device. The second approach, named decoupled, allows third parties to collect the user's login credentials and deliver them to the bank. When a third party gets a response from a bank indicating credentials are correct from the bank, it presents confirmation details to the user and, the user completes the authentication. Once the user completes authentication, the third party gets two different tokens: access and refresh tokens. Access token carries the information of the user's identity in a decrypted way and, a refresh token is used to refresh the access token. While the access token is valid for one hour, a refresh token is valid for 90 days. The third-party can use account information and payment initiation services on behalf of the user by using these tokens.

Account information service API, which is a subset of open banking API, consists of several parts. In the current implementation, third parties having the access token can only use an account list endpoint. The account list endpoint only returns the account numbers of the user. However, third parties can request consent from the user to access other details of account information such as transaction history and account balances. If the user grants consent to share his account information details, a third party can access these details for 90 days unless the user terminates the consent. At the end of 90 days, the user needs to grant a new consent. As long as there is active consent, the third-party can access the user's all transaction history and account balances.



account-rest-controller The Account Information Service allows the user to see a list of available accounts, details about a specific account, balances of a given account and list transaction reports for an account.

- GET `/v1/accounts` Read Account List
- GET `/v1/accounts-list` Read basic accounts list without previous consent
- GET `/v1/accounts/{resourceId}` Read Account Details
- GET `/v1/accounts/{resourceId}/balances` Read Account Balances
- GET `/v1/accounts/{resourceId}/transactions` Read Account's Transactions List

consent-rest-controller Service for requesting and terminating consents

- POST `/v1/consents` Consent request
- GET `/v1/consents/{consentId}` Get existing consent
- DELETE `/v1/consents/{consentId}` Terminate active consent
- GET `/v1/consents/{consentId}/status` Get consent status

Figure 4: The account information and consent service endpoints. (LHV Open Banking PSD2 REST API)

Payment initiation service API is evident from its name allows initiating a payment on behalf of the service user. Saying this service will be used by payment service providers is not a surprise. In payment initiation service API, all the necessary endpoints which complete a transaction are available. As in the account information service, the prerequisite to use this service is to have an access token that indicates the user logged in previously. When the user wants to make a payment for a service, a third party initiates the payment. The correctness of the details such as access token, payer's account number, format of the currency, receiver name and, receiver's account number is controlled by the bank. If payment initiation details are correct, the bank validates the payment initiation request and allows TPP to get the confirmation from the user. Again, as in the OAuth process, the user can confirm the payment on the bank's page (redirect approach) or the third party's page (decoupled approach). Finally, when all the other checks such as fraud and balance are completed by the bank, the transaction takes place.

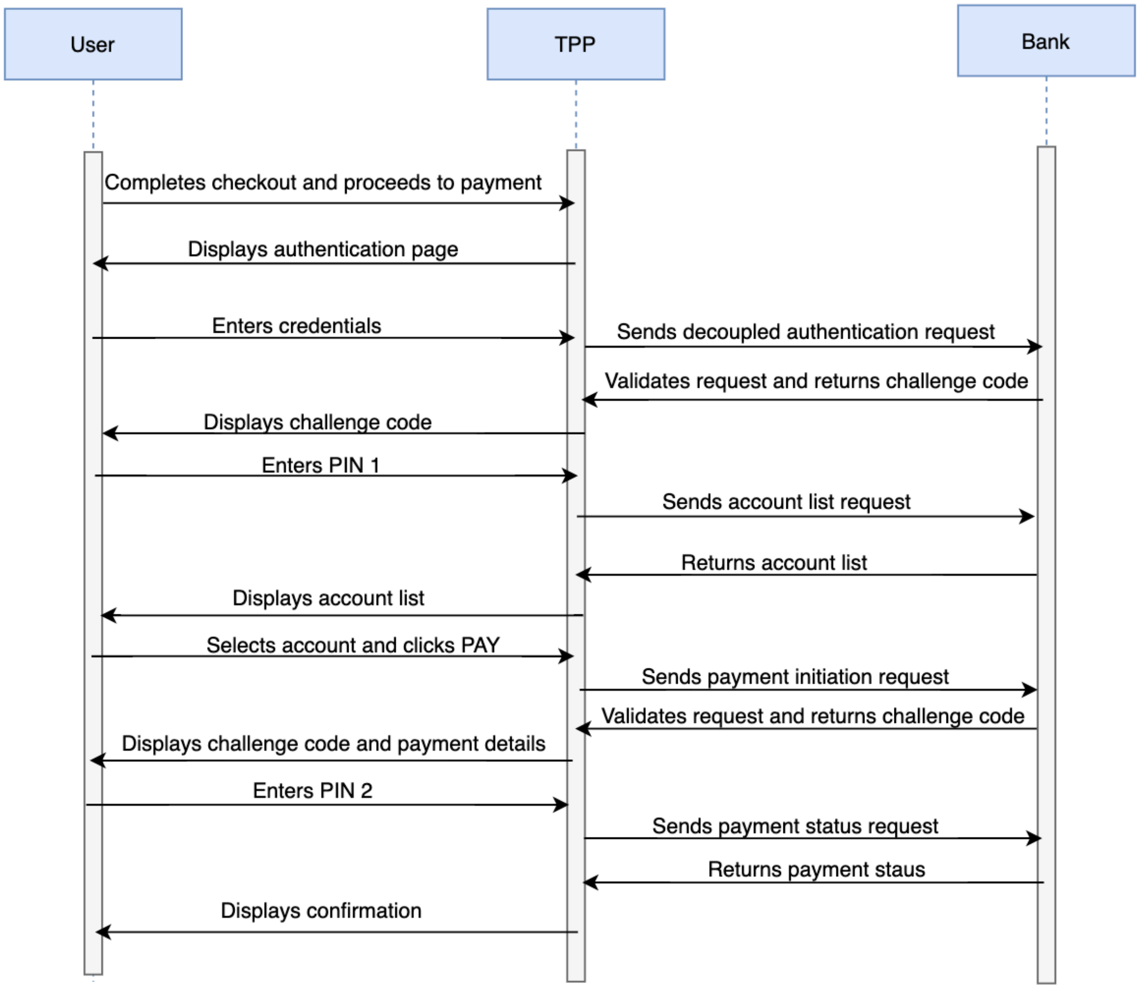

User
TPP
Bank
Completes checkout and proceeds to payment
Displays authentication page
Enters credentials
Sends decoupled authentication request
Validates request and returns challenge code
Displays challenge code
Enters PIN 1
Sends account list request
Returns account list
Displays account list
Selects account and clicks PAY
Sends payment initiation request
Validates request and returns challenge code
Displays challenge code and payment details
Enters PIN 2
Sends payment status request
Returns payment staus
Displays confirmation

Figure 5: The sequence diagram of payment flow in decoupled approach. Compiled by author.

From the Figure 5 which captures the new decoupled approach, it is visible that users do not have to interact with the bank to complete a payment. It seems PSD2 aimed to improve customer experience and convenience by preventing redirection to bank for authentication and payment confirmation. In the Appendix B the sample user interface for decoupled payment flow can be seen.

In this flow, customers can enter their internet bank login credentials into TPP's page. Also, TPPs can show payment details and ask customers to confirm the payment with their Strong Customer Authentication device (e.g., Smart-ID or Mobile-ID in Estonia). The payment flow starts with customers inputting their login credentials into the TPP's page. It means, now, TPPs can see and even store customers' login credentials before sending a request to the bank. But what TPPs can do with the login credentials is limited. By themselves, customers' login credentials cannot be used, because Strong Customer Authentication is mandated by PSD2. Therefore, even if the user's login credentials are stolen by TPP or some other party, it cannot be used without the user authenticate himself with PIN1.

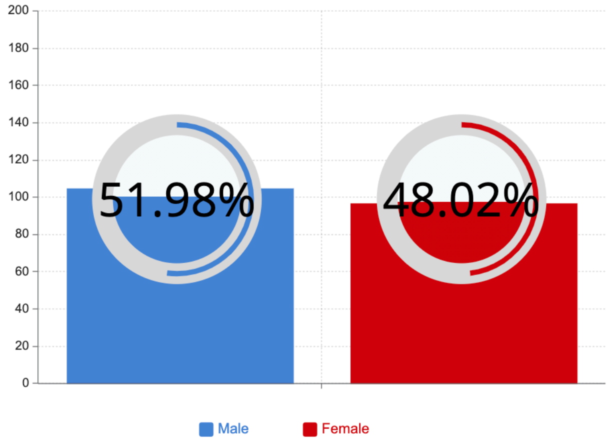
After successful authentication, in the next step of the payment flow, TPP can access users' account list without balances and transactions. Once they get the account list, they present it to the user for selection. Once user selects and clicks pay, TPP can send payment initiation request to the bank. During this process, the request might be changed by unwanted parties and even if user sees a different amount and receiver in the user interface, these can be different in the request.

4.2. The Analysis of Online Questionnaire

In this part of the thesis, the author visually presents findings from the questionnaire with graphs and numbers. The author presents the collected data as demographic, general, and specific, as previously mentioned.

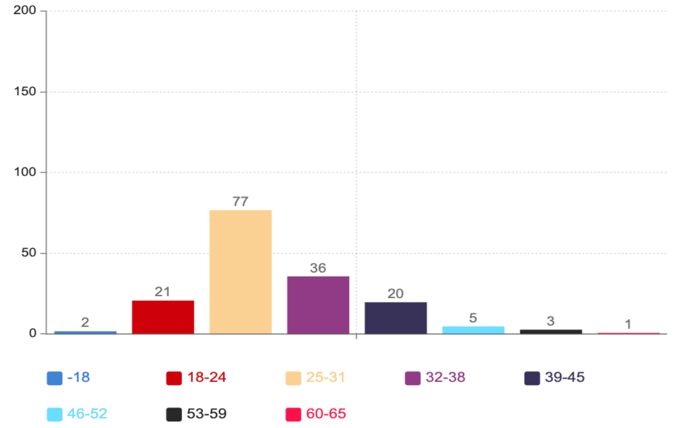
4.2.1. Demographic Questions

From the 202 valid respondents, 97 of them were female and 105 of them were male. The following graph shows the numbers visually.



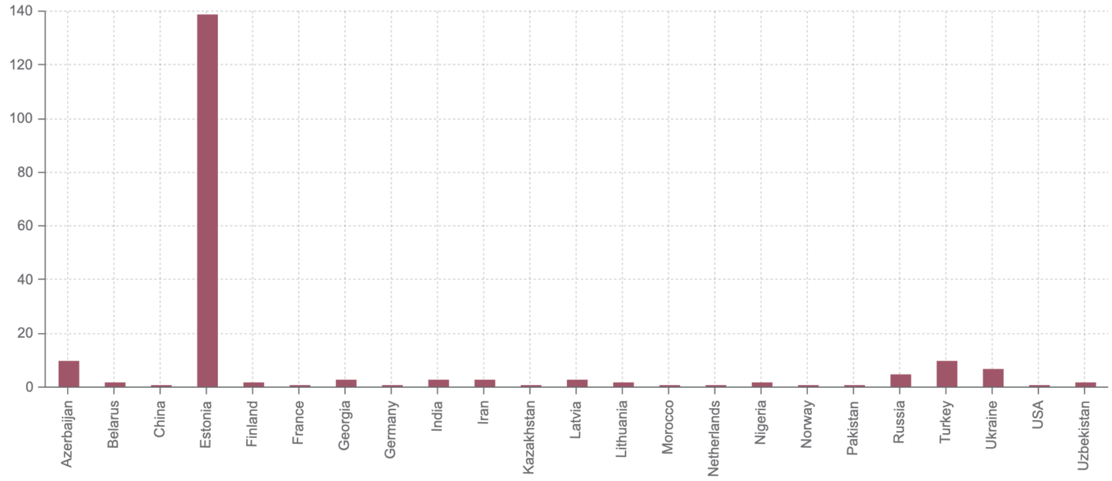
Graph 1: Distribution by Gender (Author)

After their gender, people were asked to specify their age group. In total 9 different options were presented to people for selection. The last age group, 66+, was not selected by any of the respondents. The number of respondents who are in the 25-31 age group was the highest with 77. This age group was followed by the 32-38 age group with 36 respondents. The number of respondents who are in 18-24 and 39- 45 age groups are quite close with 21 and 20 respectively. In the 46-52 age group, there were only 5 respondents. 53-59, <18, and 60-65 age groups have less respondents with the numbers 3, 2, and 1 respectively. In the following graph, the numbers can be seen visually.



Graph 2: Distribution by Age Groups (Author)

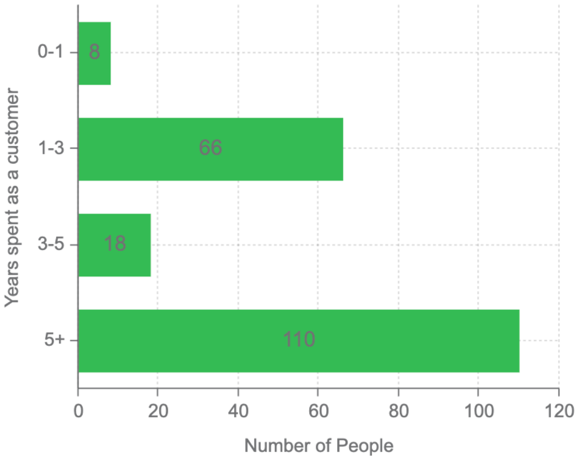
As a last demographic question, respondents were asked to specify their country of nationality. People from 23 different nationalities answered the survey. These countries alphabetically are Azerbaijan, Belarus, China, Estonia, Finland, France, Georgia, Germany, India, Iran, Kazakhstan, Latvia, Lithuania, Morocco, Netherlands, Nigeria, Norway, Pakistan, Russia, Turkey, Ukraine, USA, and Uzbekistan. As expected, Estonia was the highest number with 139. There was only one respondent from China, France, Germany, Kazakhstan, Morocco, Netherlands, Norway, Pakistan, and the USA. The countries with two respondents are Belarus, Finland, Lithuania, Nigeria, and Uzbekistan. Georgia, India, Iran, and Latvia have three respondents. Most representatives in this survey after Estonia are from Azerbaijan and Turkey with ten respondents per each country. These countries were followed by Ukraine and Russia with respectively 7 and 5 respondents. In the following graph, the distribution was presented.



Graph 3: Distribution by Country of Nationality (Author)

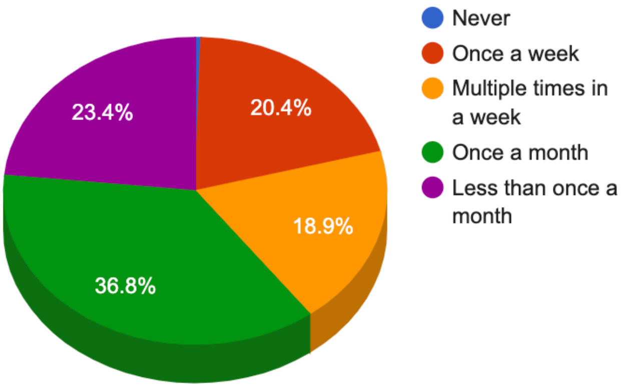
4.2.2. General Questions

As stated earlier, the general questions are asked to understand the position and behavior of Estonian bank accounts holders. First, respondents were asked to indicate how long they have been customers of their banks. 202 Estonian bank account holders responded to this question with the following numbers. 8 of them are less than one year, 66 of them between one and three years, 18 of them between three and five years and 110 of them have been customers of their banks for more than five years.



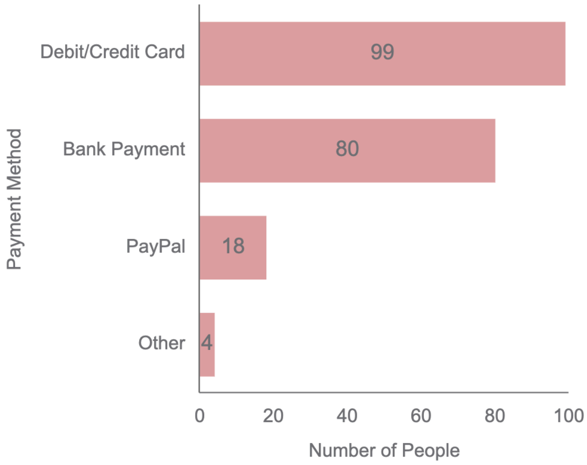
Graph 4: The number of years as a customer in banks (Author)

Secondly, respondents were asked if they shop online or not. Except one Estonian female, all of the Estonian bank account holders responded with yes to this question. As a third question, the question, "How often do you shop online?" was asked. 5 different option, "Multiple times in a week", "Once a week", "Once a month", "Less than once a month" and "Never" were presented for selection. Only one person answered with "Never". Most common answer was "Once a month" with the number of 74. While 41 people answered "Once a week", 38 people said "Multiple times in a week". The answer which shows the least frequency, "Less than once a month" was selected by 47 respondents.



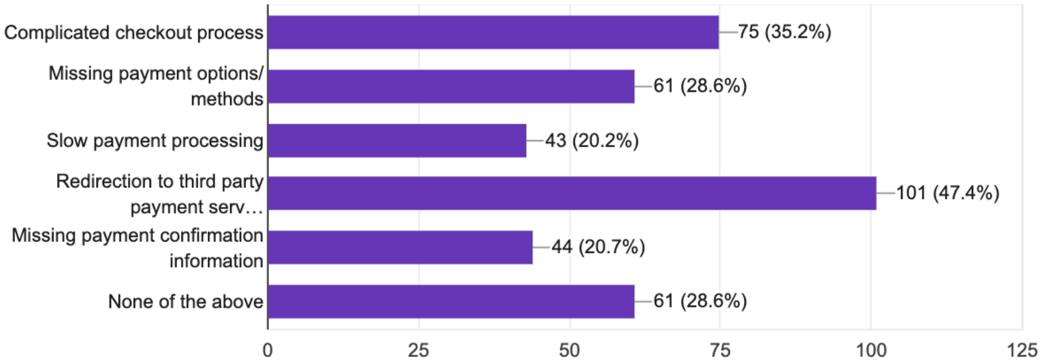
Graph 5: Online shopping frequency of respondents (Author)

After this question, respondents were asked to indicate the payment method that they used most frequently during the online shopping. For this question, the author presented four different options: Debit/Credit card, Bank payment, PayPal and other. The results for this question demonstrated that Debit/Credit card is the most frequently used payment method among respondents. While Bank payments were the second, the option of other came at the bottom of the list.



Graph 6: Most frequently used payment methods by respondents (Author)

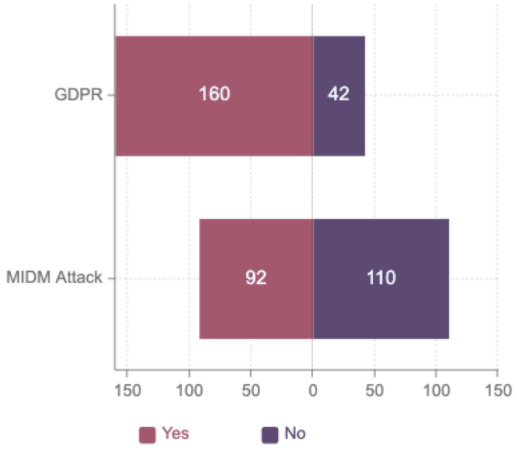
As a last general question, most common challenges that respondents encountered was posed. For this question, respondents were allowed to choose multiple options. The options were "Complicated checkout process", "Missing payment options", "Slow payment processing", "Redirection to third party payment service provider", "Missing payment confirmation information", and "None of the above". Based on the results, the most common challenge for respondents is "Redirection to third party payment service provider". This option was selected by 101 people. The results of the other options can be seen in the following graph.



Graph 7: Most common challenges during the online shopping (Author)

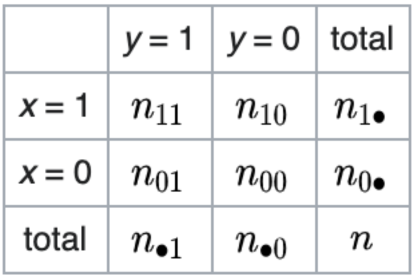
4.2.3. Specific Questions

There are three sub-objectives of gathering data with specific questions all of which served to respond to the second research question. The first one is to measure the familiarity of Estonian bank account holders regarding security and privacy concepts. To meet this objective two questions were asked. These questions are if they have heard about General Data Protection Regulation (GDPR) and the man-in-the-middle (MITM) attack. The motivation to ask such general question is to understand whether they are even aware of the concepts so that minimum unawareness can be measured for sure. 160 of 202 Estonian bank account holders responded said they have heard about GDPR. On the other hand, the familiarity with the MITM attack was lower compared to GDPR. More than half of the Estonian bank account holders, 110, said they did not hear about MITM attack before.



Graph 8: Familiarity with the terms GDPR and MITM Attack (Author)

To calculate the correlation coefficient between awareness in GDPR and MITM, phi coefficient formula is used because both variables are binary variables. The calculations are made based on the following table and formula (Aaron et al., 1998):



	$y = 1$	$y = 0$	total
$x = 1$	n_{11}	n_{10}	$n_{1\bullet}$
$x = 0$	n_{01}	n_{00}	$n_{0\bullet}$
total	$n_{\bullet 1}$	$n_{\bullet 0}$	n

$$\phi = \frac{n_{11}n_{00} - n_{10}n_{01}}{\sqrt{n_{1\bullet}n_{0\bullet}n_{\bullet 0}n_{\bullet 1}}}.$$

In the table and formula, x represents the answers for GDPR question and y represents the answers for MITM questions. So, n is the combined answers for two questions. After calculations phi coefficient is found as 0.40 (r=0.40, p<0.05). This shows that there is a significant and positive correlation between awareness in GDPR and MITM attack. So, if a person is aware of GDPR, he is more likely to be aware of MITM attack or vice versa.

The author also checked whether awareness for GDPR and MITM attack differs based on the gender. For that, the author benefited from hypothesis testing for two-sample proportions.

Here our hypothesizes are:

H0: p1=p2

H1: p1≠ p2

α = 5%

$$Z = \frac{(\hat{p}_1 - \hat{p}_2) - 0}{\sqrt{\hat{p}(1-\hat{p})\left(\frac{1}{n_1} + \frac{1}{n_2}\right)}}$$

$$\hat{p} = \frac{Y_1 + Y_2}{n_1 + n_2}$$

Male	Female

n1=105
Y1=93
p1=0.88
	n2=97
	Y2=67
	p2=0.69

GDPR awareness values for males and females (Author)

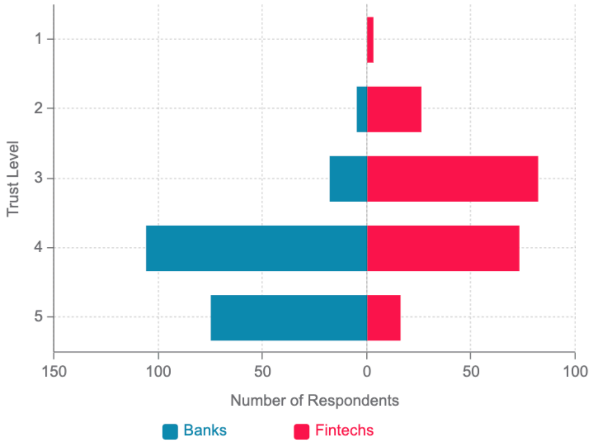
Male	Female

n1=105
Y1=72
p1=0.685
	n2=97
	Y2=20
	p2=0.206

MITM awareness values for males and females (Author)

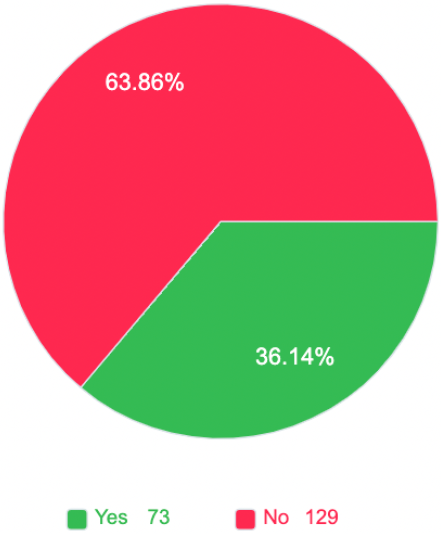
Here we calculate Z for GDPR as 3.33. Since P(Z) is 0.000868< α we reject the null hypothesis and we can conclude males are more aware than females in GDPR. For awareness in MITM attack, Z value is 6.84 and P(Z) is 0.00001< α we reject the null hypothesis. Again, we can conclude that males are more aware for MITM attack than females.

The second objective of specific questions is to understand Estonian bank account holders’ trust to banks and fintech firms. For that, they were asked to rate their trust level on a scale of 1 to 5. The results indicated that all of the respondents trust banks more than fintechs. None of the respondents rate their trust level with 1 for the banks. However, 5 respondents gave the score of 1 for their trust level to fintechs. On average, while average score level is 3.34 for fintechs, it was 4.25 for the banks.



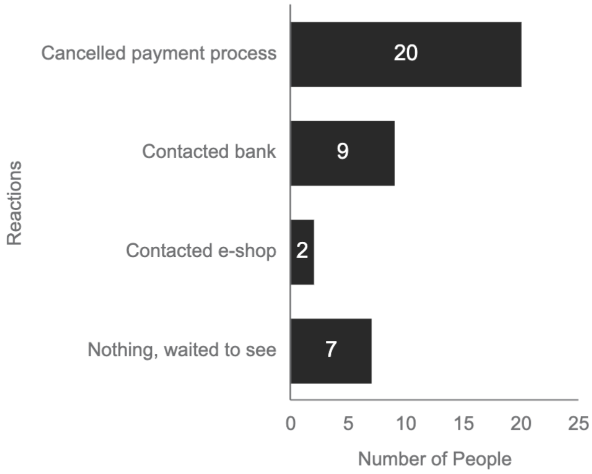
Graph 9: Trust level for banks and fintechs (Author)

The third and last purpose of the specific questions is to collect data about Estonian bank account holders' behavior during online shopping. This type of questions is quite crucial since they help to build a relationship with security risks in open banking. In the questionnaire, the author asked three questions to understand the behavior during online shopping. To comprehend if they used decoupled approach previously, the respondents are asked to specify if they entered their internet bank login credentials into another website. 73 people said yes to this question, while 129 people said no.



Graph 10: Whether respondents use their login credentials in some other webpage (Author)

On the other hand, the author asked if they ever encountered suspicious activity during online shopping. 38 people said yes to this question. After this question, they were asked how they reacted to that. For this question, the author presented four different options: “Cancelled the payment process”, “Contacted my bank”, “Contacted e-shop”, “Nothing, I waited to see what happens”. Interestingly, 7 of these 38 people answered with “Nothing, I waited to see what happens”. From these 38 people, it is clear that the most common reaction is cancelling the payment processing. And the least common reaction is contacting e-shop with two answers.



Graph 11: Reactions in case of suspicious activity during online shopping (Author)

5. Discussion of Findings

In this section, the author discussed the security risks of open banking integrations based on open banking APIs. He would further discuss the awareness level of Estonian bank account holders. From the findings it can be observed that Estonian bank account holders who are aware of GDPR are more likely to be also aware of MITM attack.

5.1. Data Privacy and Security in Open Banking

Unlike payment initiation service, there are not similar applications of Account Information Service (AIS) before PSD2. Since AIS is a new and broad concept as discussed by Wolters and Jacobs (2019) it raises some concerns. These concerns mainly stem from permitting TPPs to access customers’ data. With the chance of accessing customer data, there is no doubt that TPPs create new applications to ease users’ life. It is expected that these applications would allow customers to see their accounts and transaction histories in different banks in one application. So, for the customers who have accounts only in one bank, there is no benefit of using such applications since the functionality would be the same as their mobile or internet bank application. For the customers who have accounts in different banks, these applications might be convenient. However, there is a trade-off at this point. Customers who want to have a more convenient way to see their balances and transaction histories in different banks should be careful at who they are giving access to. They should keep in mind that, after giving consent to TPP, TPP can access all of their account numbers, account balances, and transaction histories. As explained in the overview of the open banking APIs section, refresh tokens are valid for 90 days. Therefore, once the consent is granted, TPP can access all this information for 90 days without asking to the user. Even though there is no need to store any of this data in the database since whenever requested banks provide this information, TPP can store this information into their database. If we think skeptical, we can even say that TPPs can sell this information to some other firms to make more money. Even if we exclude this option, TPPs can be attacked by some other parties and in case of security leakages all stored data can be stolen by attackers. So, all the confidential information such as balances, money transfers and purchases can be seen by unwanted parties. At this juncture, we can say that one of the risks of open banking integrations is personal data security and privacy as a response to first research question. This confirms the worries of Romānova (2018), regarding the data security and privacy.

When it comes to awareness of Estonian bank account holders, the awareness in regard of GDPR is around 79.2%. So, it is expected these people to be more careful while allowing TPPs to reach their data. The more preferable option is not to use TPPs AIS application.

The study also found a difference in awareness based on the gender. Based on the statistical test, the results showed that males are more aware than females in GDPR. This may be associated with the fact that males are more interested in the information technology (IT) related concepts and IT sector is more preferrable for men.

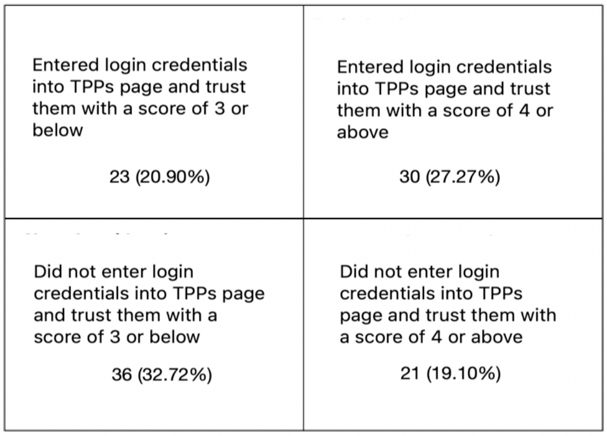
5.2. Man-in-the-middle Attack and Risk of Unauthorized Payments in Open Banking

Although there are some Payment Initiation Service applications before PSD2, PSD2 introduces new features. In the previous applications, customers who want to make a payment from their bank account have to be redirected to their bank's page for authentication and payment confirmation. However, now, PSD2 allows TPPs to create a different payment flow. In this flow, customers can enter their internet bank login credentials into TPP's page. Also, TPPs can show payment details and ask customers to confirm the payment with their Strong Customer Authentication device (e.g., Smart-ID or Mobile-ID in Estonia). Basically, for customers, there is no need to interact with their banks to complete payment. From the user experience point of view, it is so convenient. However, there is a security risk here. As stated above, in case of security issues man-in-the-middle can read or even change the data during the communication between two parties. So, the most crucial part is MITM can change the payment initiation request. This request includes information such as receiver IBAN and amount. If MITM capture this request and change it, the amount might be different and money can go to different bank account than the targeted receiver's account. During this process, the user has no chance to realize to who money is transferred. Because in user interface, everything is shown as expected but the data is changed in backend where user has no access.

In addition to MITM attack risk, there is also a risk of unauthorized transaction risk. However, this risk depends on the bank's position on whether to allow some transactions to be completed without strong customer authentication. For example, some banks allow payments that are lower than certain amounts to be completed without the user's confirmation. As explained previously, oAuth services are required to use PIS. So, once the user uses one TPPs service, his refresh token is valid for 90 days. With the refresh token, the first authentication step can be skipped if TPPs design their application in that way. If banks allow payment to be completed without confirmation, payment can be made without user involvement. But the good news is even if TPP or some unwanted party make such transactions, the liability is on the bank which allows unauthorized transactions (2018). Thus, the bank needs to make a refund to the user for such transactions.

So, answering the first research question, it is correct to say that there is a risk of MITM attack as stated by Mansfield-Devine (2016). However, Mansfield-Devine does not mention any detail where and how it can occur. On the other hand, this study says it can occur in the decoupled payment flow.

Regarding the awareness in MITM, more than half of the Estonian bank account holders have not heard about this concept previously. The results also showed that females are less aware of MITM attack than males. This is expected when the fact more males work in IT sector than females is taken into account. Within 110 people who are not aware of the MITM attack, 53 of them entered their internet bank login credentials into the TPPs page which is an indicator of usage of the decoupled payment flow. 30 of these 53 people trust TPPs with a rate of 4 or more. From these numbers, it can be interpreted that 14.85% of all Estonian bank account holders do not know about the MITM attack, use the decoupled payment flow and highly trust TPPs. This group of people can be a target victim for such attacks. This unawareness might be because of the low amount of such attack type in the past or the low level of information technology literacy.



Entered login credentials into TPPs page and trust them with a score of 3 or below 23 (20.90%)	Entered login credentials into TPPs page and trust them with a score of 4 or above 30 (27.27%)
Did not enter login credentials into TPPs page and trust them with a score of 3 or below 36 (32.72%)	Did not enter login credentials into TPPs page and trust them with a score of 4 or above 21 (19.10%)

Figure 6: The distribution of respondents who are not aware of MITM attack. Compiled by author.

6. Conclusion

The purpose of this study was to point out security risks of open banking integrations and show the awareness level of Estonian bank account holders regarding this matter.

With the analysis of open banking APIs, it was envisioned how TPPs can create applications by using the APIs. It turned out that, applications which can be built with AIS have a risk of revealing confidential information such as account balances and transaction history. For payment service provider applications which is possible to create with PIS APIs, the main risk comes with the new decoupled payment flow. Analysis showed that, in this payment flow, there is an invitation to man-in-the-middle. MITM attack can cause financial loss for the users of the decoupled payment flow.

As mentioned, the second purpose of the study was to show awareness level of Estonian bank account holders. In this regard, people were surveyed. Based on the results of the survey, it is understood that familiarity and awareness of GDPR which ensures data privacy is higher than MITM attack.

Overall, I hope this study brings awareness to the payment service users while using the financial services. The readers of this thesis will be more cautious during their online shopping process. Moreover, from the service provider's point of view, I believe this study will be helpful while building new applications if the highlighted risks are taken into account.

Even though this study showed the security risks of open banking integrations and awareness level of Estonian bank account holders, there were some limitations for better results. These limitations and recommendations for further studies are discussed in the following parts.

6.1. Limitations

For the online questionnaire, only 213 people shared their answers. With a longer period of availability of survey, the number could be higher and more representative results could be achieved to generalize the findings of all Estonian bank account holders.

Another limitation was the lack of previous AIS application since it is a new concept. If those would exist, respondents' behavior and awareness level for data security and privacy could be measured more accurately.

6.2. Recommendations

This study focused on the risks of open banking integrations and pointed out two major risks as data privacy/security and MITM attack. Since PSD2 and open banking are new concepts, they are not mature yet. Despite these risks, they provide new opportunities for TPPs and a better user experience for customers. For further studies, it is highly recommended to work on how TPPs can ensure security and mitigate these risks or what is the current position of the TPPs who build applications with open banking APIs.

For the users of open banking services, it is highly recommended not to share their data with TPPs which they don't know. Moreover, while making a payment, they should prefer the redirect approach which is more secure than decoupled approach.

Considering the existing risks in open banking, TPPs that want to earn customers' trust should build their system as secure as possible. For AIS application service providers, it is crucial not to store any customer data. To convince the customers to use their services, going through an auditing process and communicating this with customers might be helpful.

References

1. Aaron, B., Kromrey, J. D., & Ferron, J. M. (1998, November). Equating r-based and d-based effect-size indices: Problems with a commonly recommended formula.
2. Luvanda, A., Kimani, S., & Kimwele, M. (2014). Identifying Threats Associated With Man-In-The-Middle Attacks during Communication between a Mobile Device and the Back End Server in Mobile Banking Applications. *Journal of Computer Engineering*, 35–42.
3. Mallik, A. (2018). Man-in-the-middle-attack: Undestanding in simple words. *Jurnal Pendidikan Teknologi Informasi*, *2*(2), 109–134.
4. Bär, F., & Mortimer-Schutts, I. (2020). Innovation in open banking: Lessons from the recent wave of payment institutions that have been authorised to provide payment initiation and account information services. *Journal of Payments Strategy & Systems*, *14*(3), 268–285.
5. Basel Committee. (2019). *Report on open banking and application programming interfaces*.
6. McDowell, B. (2019, February). Three ways in which GDPR impacts authentication. *Computer Fraud & Security*.
7. Döderlein, D. (2018). What is the optimal mix between banks and FinTechs in the payments architecture? *Journal of Payments Strategy & Systems*, *12*(2), 122–129.
8. Llewellyn, D. (2018, October 30). *Financial Technology, Regulation, and the Transformation of Banking*. Financial Disintermediation and the Future of the Banking Sector, Madrid.
9. Dratva, R. (2020). Is open banking driving the financial industry towards a true electronic market? *Electronic Markets*, *30*(1), 65–67. Scopus. https://doi.org/10.1007/s12525-020-00403-w
10. European Parliament. Directorate General for Internal Policies of the Union. (2019). *Competition issues in the area of Financial Technology (FinTech): Study presentation: in depth analysis.* Publications Office. https://data.europa.eu/doi/10.2861/825391
11. Farrow, G. S. D. (2020). Open banking: The rise of the cloud platform. *Journal of Payments Strategy & Systems*, *14*(2), 128–146.
12. Gozman, D., Hedman, J., & Sylvest, K. (2018, November 28). *Open Banking: Emergent Roles, Risks & Opportunities*. https://aisel.aisnet.org/ecis2018_rp/183/

13. Haubrich, D. (2018). The development of regulatory requirements for payment services: The European Banking Authority and the revised Payments Services Directive. *Journal of Payments Strategy & Systems*, *12*, 130–139.
14. Hernández, E., Öztürk, M., Sittón, I., & Rodríguez, S. (2019). Data Protection on Fintech Platforms. In F. De La Prieta, A. González-Briones, P. Pawleski, D. Calvaresi, E. Del Val, F. Lopes, V. Julian, E. Osaba, & R. Sánchez-Iborra (Eds.), *Highlights of Practical Applications of Survivable Agents and Multi-Agent Systems. The PAAMS Collection* (Vol. 1047, pp. 223–233). Springer International Publishing. https://doi.org/10.1007/978-3-030-24299-2_19
15. Imerman, M. B., & Fabozzi, F. J. (2020). Cashing in on innovation: A taxonomy of FinTech. *Journal of Asset Management*, *21*(3), 167–177. https://doi.org/10.1057/s41260-020-00163-4
16. Institute of International Finance. (2018). *Liability and Consumer Protection in Open Banking*.
17. Hsu, J. (2018). What you need to know about Europe’s data privacy rules. *IEEE Spectrum*.
18. Azorín, J. & Camero, R. (2010). The Application of Mixed Methods in Organisational Research: A Literature Review. *The Electronic Journal of Business Research Methods*, *8*(2), 99–105.
19. Kamiya, S., Kang, J.-K., Kim, J., Milidonis, A., & Stulz, R. (2018). *What is the Impact of Successful Cyberattacks on Target Firms?* (No. w24409; p. w24409). National Bureau of Economic Research. https://doi.org/10.3386/w24409
20. Kapil M. Jain, Manoj V. Jain, & Jay L. Borade. (2016). A Survey on Man in the Middle Attack. *International Journal of Science Technology & Engineering*, *2*(09), 277–280.
21. Knewtson, H. S., & Rosenbaum, Z. A. (2020). Toward understanding FinTech and its industry. *Managerial Finance*, *46*(8), 1043–1060. Scopus. https://doi.org/10.1108/MF-01-2020-0024
22. Kumar, P. R., Raj, P. H., & Jelciana, P. (2018). Exploring Data Security Issues and Solutions in Cloud Computing. *Procedia Computer Science*, *125*, 691–697. https://doi.org/10.1016/j.procs.2017.12.089
23. Leong, K. (2018). FinTech (Financial Technology): What is It and How to Use Technologies to Create Business Value in Fintech Way? *International Journal of*

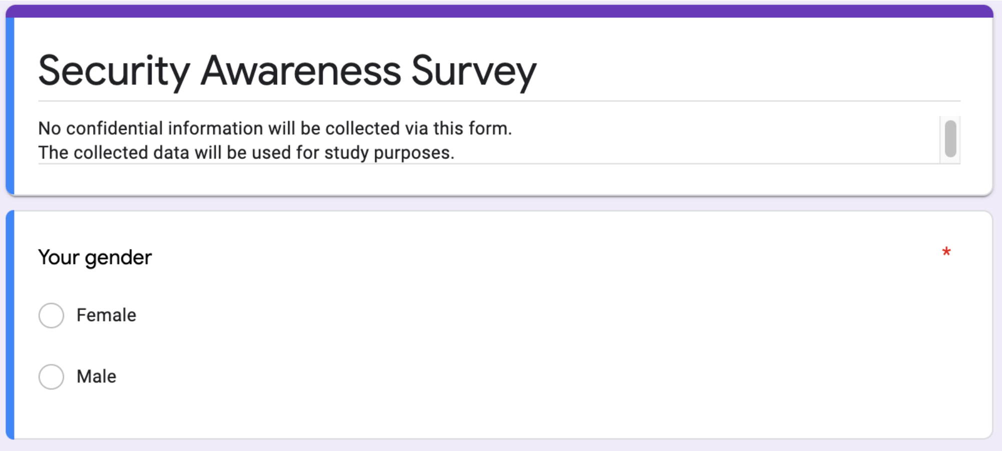
Innovation, Management and Technology, 74–78. https://doi.org/10.18178/ijimt.2018.9.2.791

24. Li, Y., & Saxunová, D. (2020). A perspective on categorizing Personal and Sensitive Data and the analysis of practical protection regulations. *Procedia Computer Science*, *170*, 1110–1115. https://doi.org/10.1016/j.procs.2020.03.060
25. Choy, L. (2014). The Strengths and Weaknesses of Research Methodology: Comparison and Complimentary between Qualitative and Quantitative Approaches. *IOSR Journal Of Humanities And Social Science*, *19*(4), 99–104.
26. Saunders, M., Lewis, P., & Thornhill, A. (2009). *Research Methods for Business Students* (Fifth edition). Prentice Hall.
27. Meng, M., Steinhardt, S., & Schubert, A. (2018). Application Programming Interface Documentation: What Do Software Developers Want? *Journal of Technical Writing and Communication*, *48*(3), 295–330. https://doi.org/10.1177/0047281617721853
28. Mukherjee, S. (2019). Overview of the Importance of Corporate Security in Business. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3415960
29. Kottayil, N. (2020). Consumer Security and Liability Model for Open Banking. *International Journal of Trend in Research and Development*, *7*(4), 230–232.
30. Ochieng Pamela Atieno. (2009). An Analysis of the Strenghts and Limitation of Qualitative and Quantitative Research Paradigms. In *Problems of Education in the 21st Century* (Vol. 13).
31. Omarini, A. E. (2018). Banks and Fintechs: How to Develop a Digital Open Banking Approach for the Bank's Future. *International Business Research*, *11*(9), 23. https://doi.org/10.5539/ibr.v11n9p23
32. Premchand, A., & Choudhry, A. (2019). *Open banking and APIs for transformation in banking*. 25–29. Scopus. https://doi.org/10.1109/IC3IoT.2018.8668107
33. Queirós, A., Faria, D., & Almeida, F. (2017). *Strengths And Limitations Of Qualitative And Quantitative Research Methods*. https://doi.org/10.5281/ZENODO.887089
34. Romanova, I., Grima, S., Spiteri, J., & Kudinska, M. (2018). The payment services Directive II and competitiveness: The perspective of European fintech companies. *European Research Studies Journal*, *21*(2), 3–22. Scopus. https://doi.org/10.35808/ersj/981

35. Ryu, H.-S., & Ko, K. S. (2020). Sustainable Development of Fintech: Focused on Uncertainty and Perceived Quality Issues. *Sustainability*, *12*(18), 7669. https://doi.org/10.3390/su12187669
36. Sagdeo, P. (2018). Application Programming Interfaces and the Standardization-Value Prioritization Problem. *Harvard Journal of Law & Technology*, *32*, 236–263.
37. Scheja, O., & Machielse, W. (2019). The nextgenPSD2 framework in a pan-european PSD2 account access context. *Journal of Payments Strategy and Systems*, *13*(1), 54–65. Scopus.
38. Skendzic, A., Kovacic, B., & Tijan, E. (2018). General data protection regulation—Protection of personal data in an organisation. *2018 41st International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO)*, 1370–1375. https://doi.org/10.23919/MIPRO.2018.8400247
39. Moffatt, S. (2015). Contextualizing Scientific Research Methodologies. *IOSR Journal of Research & Method in Education*, *5*(6), 52–57. https://doi.org/10.9790/7388-05615257
40. Mansfield-Devine, S. (2016). Open banking: Opportunity and danger. *Computer Fraud & Security*, 8–13.
41. Sukamolson, S. (2005). *Fundamentals of quantitative research*.
42. Tait, F., & Davis, R. H. (1989). The Development and Future of Home Banking. *International Journal of Bank Marketing*, *7*(2), 3–9. https://doi.org/10.1108/EUM0000000001452
43. Wolters, P. T. J., & Jacobs, B. P. F. (2019). The security of access to accounts under the PSD2. *Computer Law and Security Review*, *35*(1), 29–41. Scopus. https://doi.org/10.1016/j.clsr.2018.10.005
44. Yawe, U. B. L., & Mukisa, U. I. (2020). The impact of the Revised Payment Services Directive on the market for payment initiation services. *Journal of Payments Strategy & Systems*, *14*(1), 40–47.
45. Zachariadis, M., & Ozcan, P. (2017). *The API Economy and Digital Transformation in Financial Services: The case of Open Banking*. Swift Institute.
46. Zveryakov, M., Kovalenko, V., Sheludko, S., & Sharah, E. (2019). FinTech sector and banking business: Competition or symbiosis? *Economic Annals-XXI*, *175*(1–2), 53–57. Scopus. https://doi.org/10.21003/ea.V175-09

Appendices

Appendix A- Questionnaire



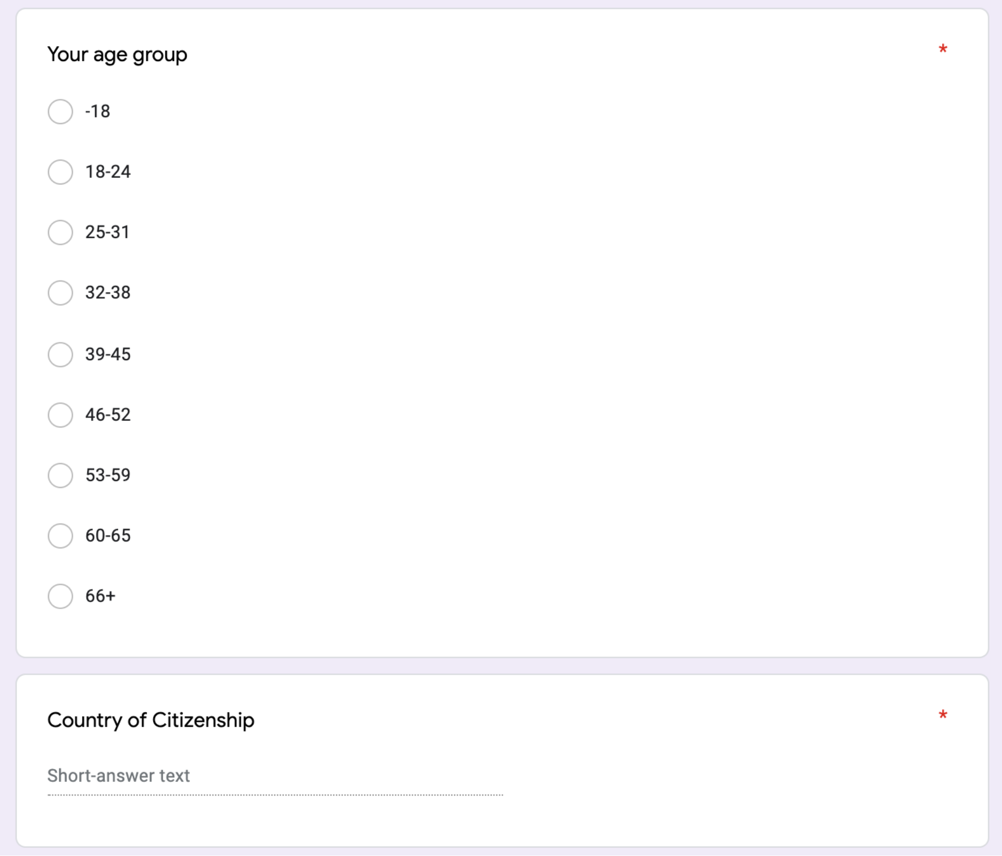
Security Awareness Survey

No confidential information will be collected via this form.
The collected data will be used for study purposes.

Your gender *

○ Female

○ Male



Your age group *

○ -18

○ 18-24

○ 25-31

○ 32-38

○ 39-45

○ 46-52

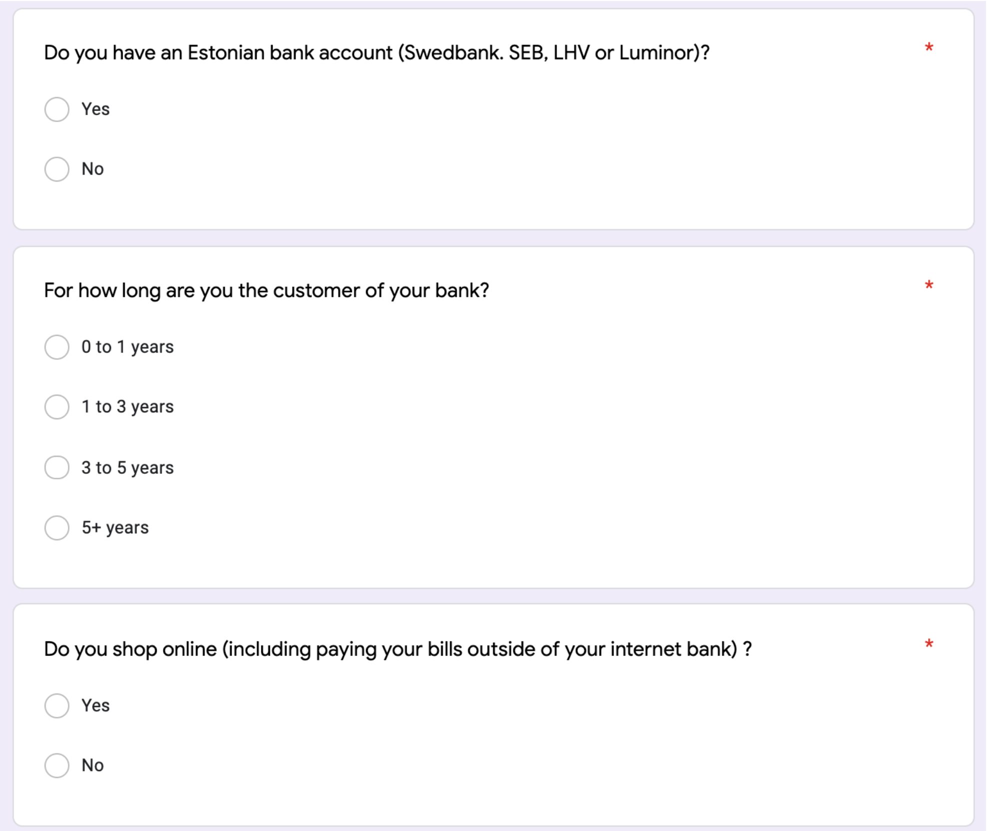
○ 53-59

○ 60-65

○ 66+

Country of Citizenship *

Short-answer text



Do you have an Estonian bank account (Swedbank. SEB, LHV or Luminor)? *

○ Yes

○ No

For how long are you the customer of your bank? *

○ 0 to 1 years

○ 1 to 3 years

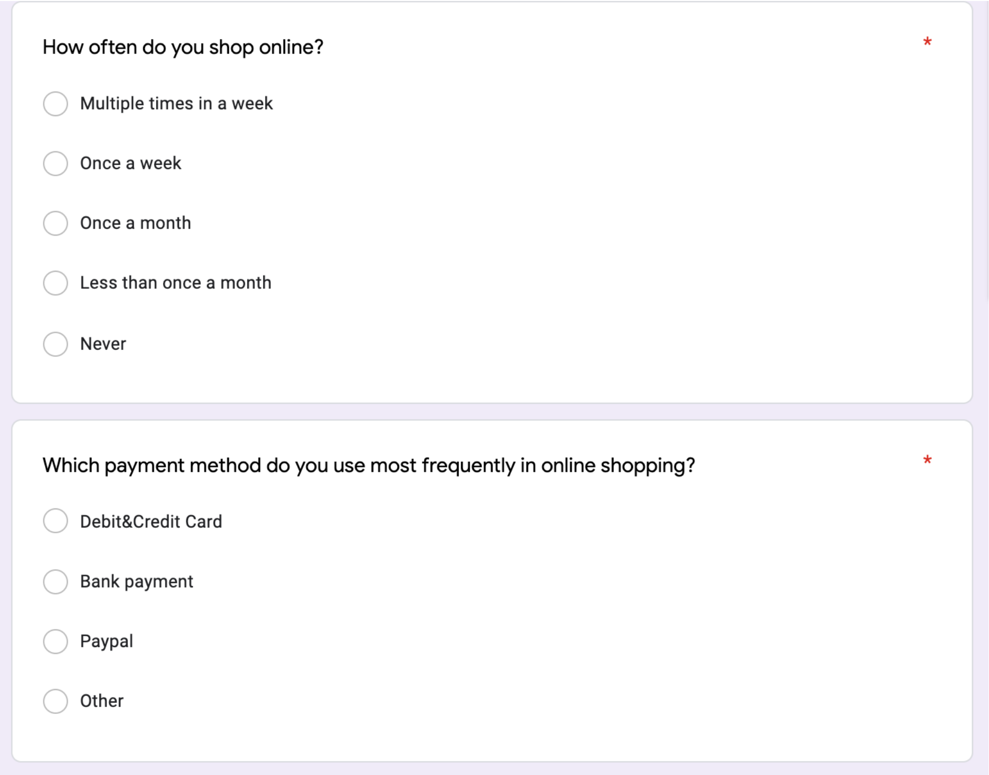
○ 3 to 5 years

○ 5+ years

Do you shop online (including paying your bills outside of your internet bank) ? *

○ Yes

○ No



How often do you shop online? *

○ Multiple times in a week

○ Once a week

○ Once a month

○ Less than once a month

○ Never

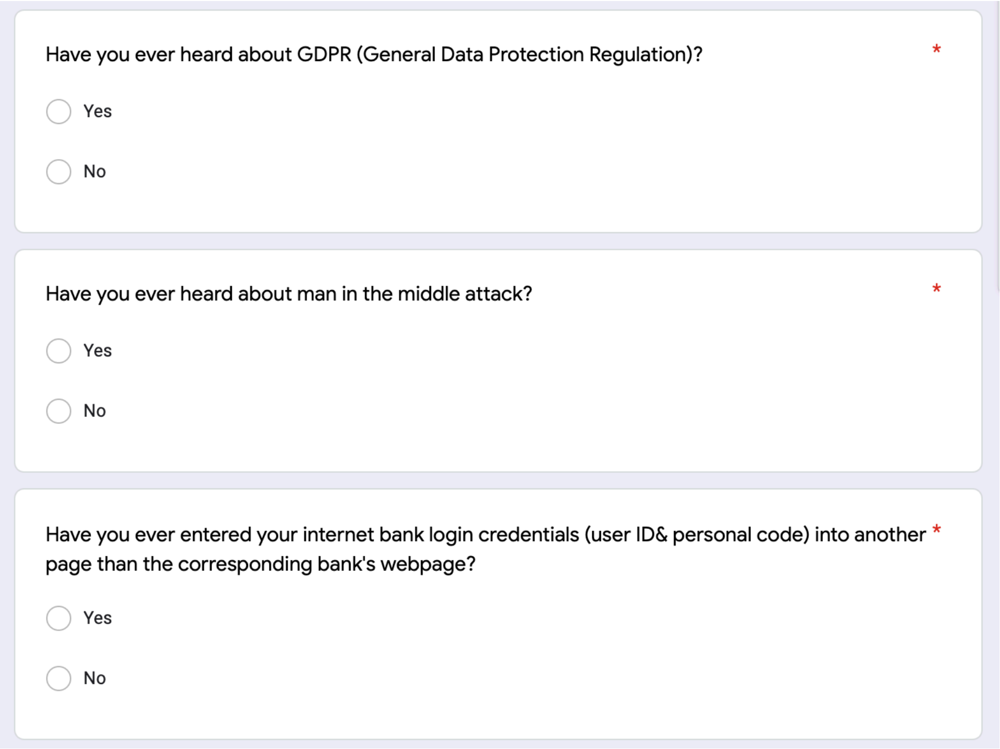
Which payment method do you use most frequently in online shopping? *

○ Debit&Credit Card

○ Bank payment

○ Paypal

○ Other



Have you ever heard about GDPR (General Data Protection Regulation)? *

○ Yes

○ No

Have you ever heard about man in the middle attack? *

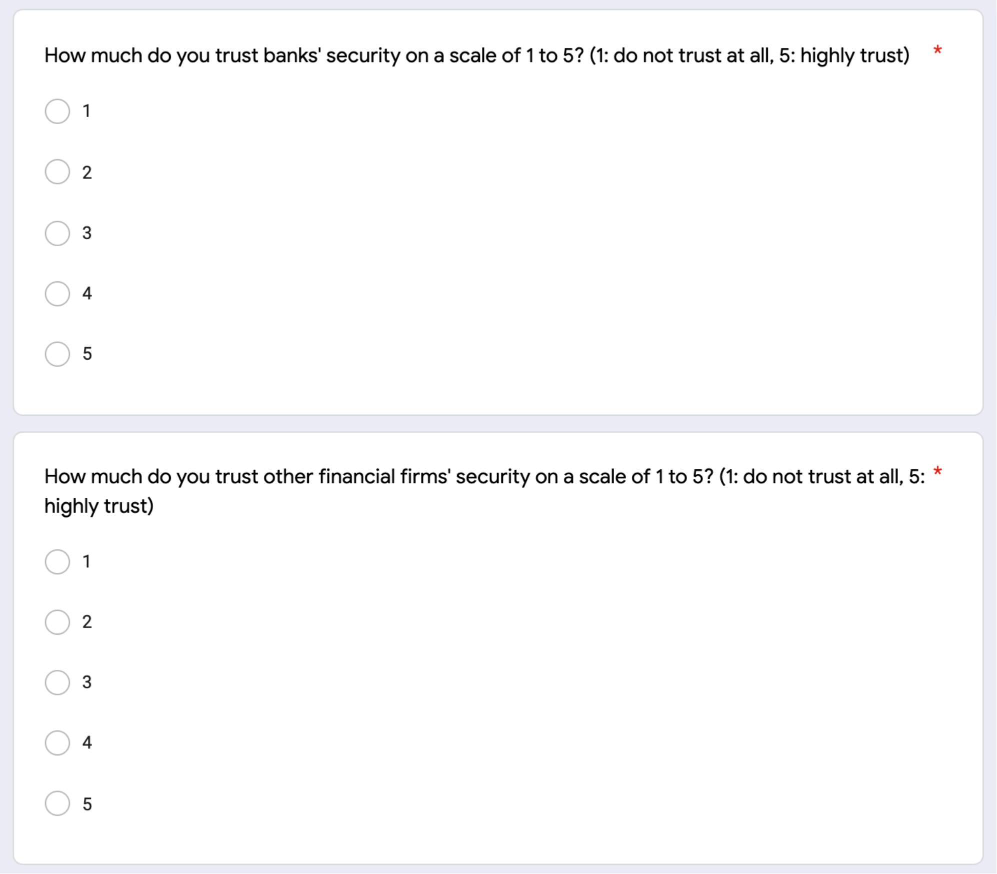
○ Yes

○ No

Have you ever entered your internet bank login credentials (user ID& personal code) into another page than the corresponding bank's webpage? *

○ Yes

○ No



How much do you trust banks' security on a scale of 1 to 5? (1: do not trust at all, 5: highly trust) *

○ 1

○ 2

○ 3

○ 4

○ 5

How much do you trust other financial firms' security on a scale of 1 to 5? (1: do not trust at all, 5: highly trust) *

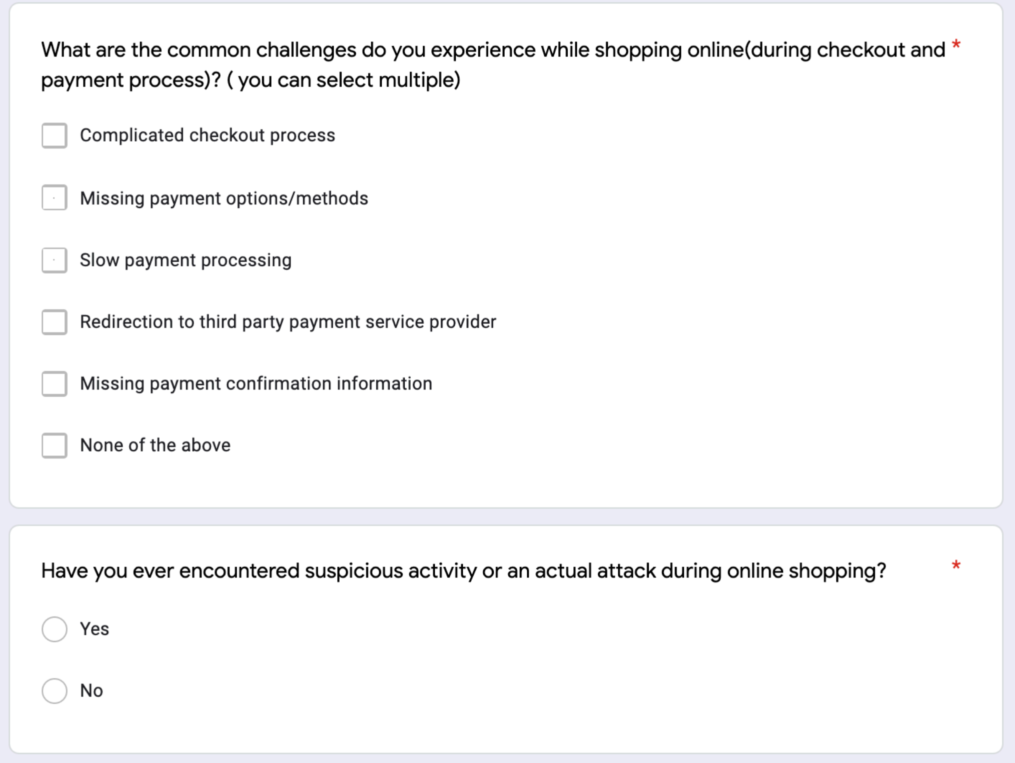
○ 1

○ 2

○ 3

○ 4

○ 5



What are the common challenges do you experience while shopping online(during checkout and payment process)? (you can select multiple) *

□ Complicated checkout process

□ Missing payment options/methods

□ Slow payment processing

□ Redirection to third party payment service provider

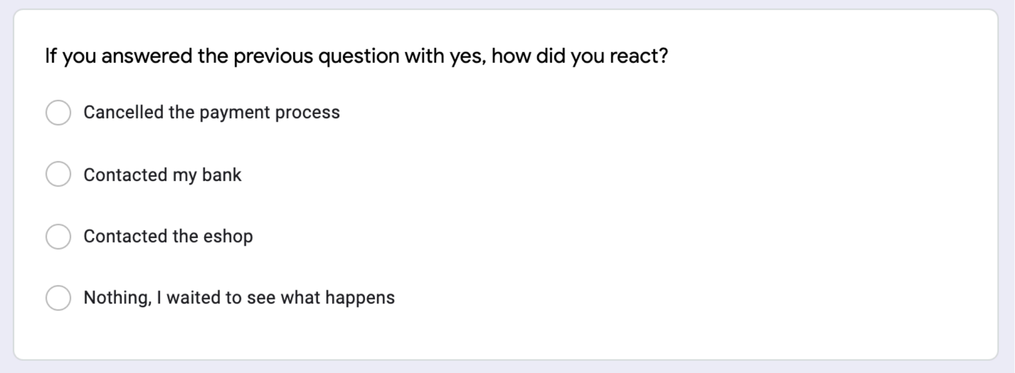
□ Missing payment confirmation information

□ None of the above

Have you ever encountered suspicious activity or an actual attack during online shopping? *

○ Yes

○ No



If you answered the previous question with yes, how did you react?

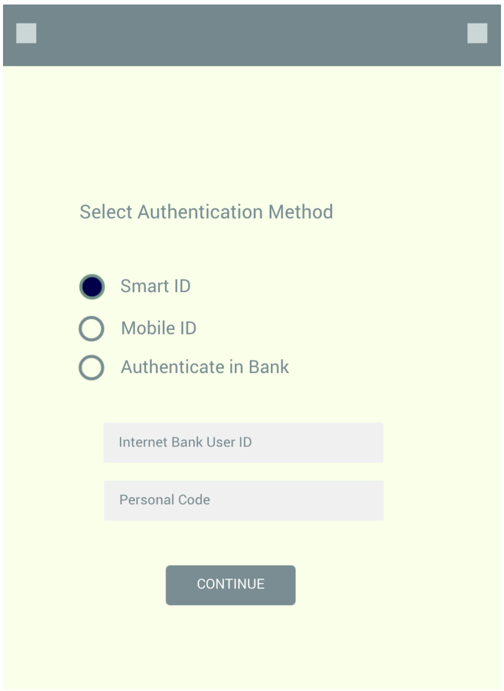
○ Cancelled the payment process

○ Contacted my bank

○ Contacted the eshop

○ Nothing, I waited to see what happens

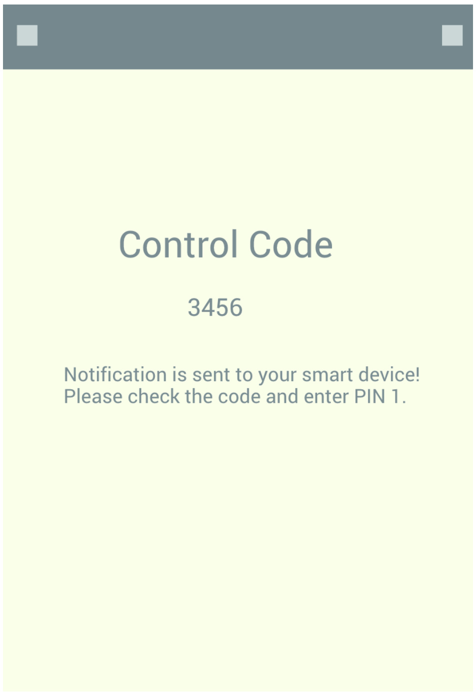
Appendix B- User Interface of Decoupled Payment Flow



Select Authentication Method

● Smart ID
○ Mobile ID
○ Authenticate in Bank

Step 1

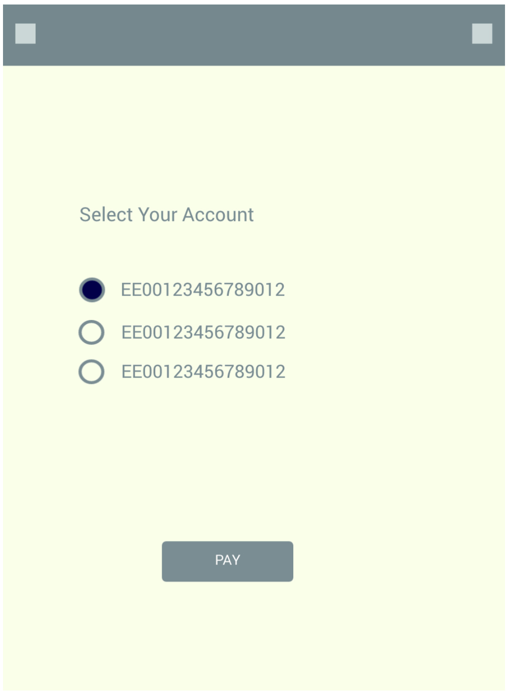


Control Code

3456

Notification is sent to your smart device!
Please check the code and enter PIN 1.

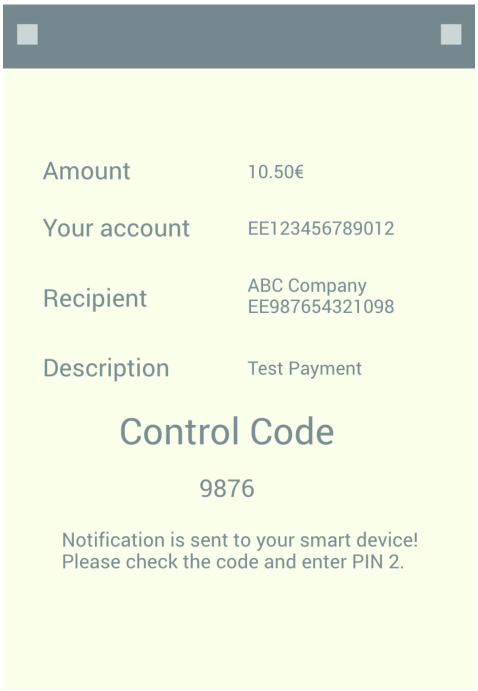
Step 2



Select Your Account

● EE00123456789012
○ EE00123456789012
○ EE00123456789012

Step 3



Amount	10.50€
Your account	EE123456789012
Recipient	ABC Company EE987654321098
Description	Test Payment

Control Code

9876

Notification is sent to your smart device!
Please check the code and enter PIN 2.

Step4

Resümee

AVATUD PANGANDUSE INTEGRATSIOONIDE TURVALISUSE ANALÜÜS JA EESTI PANGAKONTOT OMAVETE ISIKUTE TEADLIKKUS NENDEGA KAASNEVATEST RISKIDEST

Antud magistritöö eesmärgiks on identifitseerida avatud panganduse integratsioonide turvariskid ning Eesti pangakonto omavate inimeste teadlikkuse tasemega nendest riskidest. Selleks keskendub töö programmiliidese analüüsimisele ning kuidas kolmandate osapoolte pakkujad kasutavad neid programmiliideseid. Täpsemate tulemuste saamiseks kasutati töö teoreetilises pooles programmiliideste uurimiseks kvantitatiivset meetodeid. Kvantitatiivse meetodi andmete kogumiseks kasutati mugavusvalimi tehnikat, kus küsitleti 202 Eesti pangakontot omavat inimest. Konfidentsiaalsete andmete turva/privaatsuse ja inimese keskmises rünnakus olid kaks suuremat riski, mis magistritöö tuvastas. Kvantitatiivsest analüüsist tuli välja, et suurem osa Eesti pangakonto omavatest inimestest on teadlik isikuandmete kaitse üldmääruse mõistetest, kuid enam kui pooled ei teadnud, mis tähendab inimene keskmises rünnakus mõiste. Tulemused näitasid, et mehed on naistest teadlikumad GDPR ja vahendusrünnete (MITM) osas. Lisaks on positiivne korrelatsioon GDPR ja vahendusrünnete (MITM) teadlikkuse vahel. Edasine analüüs antud grupi kohta leidis, et just nemad võivad potentsiaalselt olla ohvrid inimene keskel rünnakule.

Non-exclusive licence to reproduce thesis and make thesis public

I, Abdullah Cem Açıkgöz,

1. herewith grant the University of Tartu a free permit (non-exclusive licence) to:

1.1. reproduce, for the purpose of preservation, including for adding to the DSpace digital archives until the expiry of the term of copyright, and

1.2. make available to the public via the web environment of the University of Tartu, including via the DSpace digital archives, under the Creative Commons licence CC BY NC ND 3.0, which allows, by giving appropriate credit to the author, to reproduce, distribute the work and communicate it to the public, and prohibits the creation of derivative works and any commercial use of the work from ***25/05/2021*** until the expiry of the term of copyright, SECURITY ANALYSIS OF OPEN BANKING INTEGRATIONS AND AWARENESS OF ESTONIAN BANK ACCOUNT HOLDERS, supervised by Isaac Nana Akuffo

2. I am aware of the fact that the author retains the rights specified in p. 1.

3. I certify that granting the non-exclusive licence does not infringe other persons' intellectual property rights or rights arising from the personal data protection legislation.

Abdullah Cem Açıkgöz

22/05/2021