MYKOLAS ROMERIS UNIVERSITY-MIDDLESEX UNIVERSITY

BUSINESS AND MEDIA SCHOOL

PAULIUS LAPĖNAS

Electronic Business Management

DEVELOPMENT OF BIOMETRICS BASED PAYMENT CONFIRMATION MODEL IN CONSUMER TO BUSINESS MOBILE PAYMENTS IN LITHUANIA

Master thesis

Supervisor: Prof. dr. Mindaugas Kiškis

Vilnius, 2016

TABLE OF CONTENT

LIST OF FIGURES

LIST OF TABLES

INTRODUCTION

Novelty and relevance. Subject of biometrics-based mobile payment confirmation has already been explored in terms of global technology and digital payments. Naturally technological development of every country influenced the adoption of security, user authentication, and payment confirmation options. Therefore, they differ from country to country depending on each country's technological development. In Lithuania payment confirmation options are mainly based on either password or electronic signature. Statistical data clearly indicates that mobile payments are very low compared to other payment methods available in Lithuania. Moreover, data reflects that in 2016 mobile payments made up only 0.01% of total digital payments performed that year. Analysis of Lithuanian market showed that market players offering payment solutions had attempts to introduce mobile payment option to Lithuanian consumers. Currently, biometrics in Lithuania are used mainly by governmental organizations rather than by companies operating in payment industry. European market research illustrates that legal entities and consumers are willing to adopt and use biometrics as security and payment confirmation measure. However, insufficient security measures tend to make consumers abandon last payment phase in money transfer procedures as they start feeling insecure. Biometrics-based payment confirmation option is not offered to consumers in Lithuania. Creating a model adopted to Lithuanian consumer and current environment in Lithuania would be a new option, which could lead to increased reliability and usage of mobile payments.

Subject related researches. Subject of biometrics and its usage in technologies are discussed by a number of scientists. Requirements and main features of biometrics, in different time period, were analyzed by R. Bolle (2006), A. Jain (2008), U. Uludag (2004) and others. W. Yang (2013) and B. Schouten (2009) identified main stages of when and how biometrics could be used in person authentication. R. Bolle (2006) ranked all main biometrics according to its usage and reliability in terms of technologies. Biometrics usage from security perspective was studied by R. Garg (2015). S Agrawal (2014) identified main security issues in mobile payments and consequences that might occur if these issues are not addressed properly. Organizations such as European Payments Council and Visa conducted several studies on consumer behavior and preferences towards security and biometrics usage in payment processes. The same researches targeted financial sector companies which plan to use biometrics in their security processes.

Problem statement. Biometrics-based mobile payment authorization option has not yet been offered to Lithuanian consumers. Consequently, security measures have not been used to their full capacity and thus reliability and usage of mobile payments are very low.

Research purpose. This research aims at creating biometrics-based mobile payment confirmation process model which could be adopted in Lithuania.

Objectives:

1. To analyze biometrics and determine most suitable biometrical feature to be used in person authentication;
2. To review environment for mobile payments in Lithuania;
3. To identify biometrics-based payment confirmation model, which could be used as an example in creating process model for Lithuania.

Research object. The object of this research is biometrics and biometrics-based payment confirmation model, which could be implemented in Lithuania according to existing legal and mobile payment environment. Research on the object is supported by scientific articles, legal documents, and analysis of statistical data.

The following research methods were applied:

- Review and analysis of scientific literature and researches;
- Review and analysis of legal documents;
- Statistical data analysis;
- Case study.

Structure. This master thesis consists of five parts. The first part is dedicated to reviewing essentials of biometrics. The second part describes usage of biometrics in technologies and how it is implemented in security of technologies. The third part provides insight into both legal and payment environment in Lithuania. The forth part is dedicated to describing methodology which the research is based upon. The fifth and final part includes comparative analysis of countries and also a case study on payment confirmation model of Estonian company “AS Pocopay”.

1. MAIN CHARACTERISTICS OF BIOMETRICS

Each person has unique behavioral, physical or chemical attributes which form identity of an individual person. Authors describe biometrics as science which explores unique attributes of a person and helps establish identity (Jain, 2008).[1] Uludag at al. (2004)[2] introduces biometrics as a "technique" of recognizing a person based solely on their biological features. Different authors argue that biometric is physiological or behavioral features of a person. In a broader sense biometrics could be understood as a method identifying a person based on one unique biological features. Those features could be divided into two main categories:

1. Physiological – hand geometry, fingerprints, points of face structure;
2. Behavioral – signature, voice.

As there are many biological features of a person which could be qualified as eligible to be called biometrics, it is important to distinguish the main aspects which should be followed. According to (Bolle, 2006)[3] the main requirements are:

1. Universality – characteristic could be found in each and every person;
2. Uniqueness – no more than one person has certain characteristics;
3. Permanence – characteristic that remains unchanged over time;
4. Collectability – characteristic could be measured and saved.

When the four mentioned requirements are put in practice, there are several additional important things which should be considered[3]:

- Performance – states that identification accuracy of certain feature should be acceptable;
- Acceptability – determines to what extent people are willing to accept biometrical features;
- Circumvention – determines if a particular feature is suitable and how easily can it be influenced by a fraudulent activity.

Gathering biological data of a person is just one step in using biometrics for identification purposes. If characteristic does not meet all four above listed requirements – it could not serve for identification purposes. Two main stages have to be covered in order to consider a specific characteristic as eligible for identification:

[1] Jain, A. K., Flynn, P., Ross, A. (2008). *Handbook of biometrics* 978-0-387-71041-9
[2] Uludag, U., Pankanti, S., Jain, A.K., Prabhakar, S. (2004) *Biometric cryptosystems: issues and challenges* IEEE, vol. 92, no. 6
[3] Bolle, R., Jain, A., Pankanti, S. (2006). *Personal Identification in Network Society* 978-0387-28539-9

1. Verification[4] or enrollment[5] stage – capturing and storing a feature of a person;
2. Recognition stage – finding the feature in database and matching it with a current feature.

If the first phase of eligibility is passed but certain feature does not meet permanence or collectability requirement – the second phase of using biometric in identification process could not be employed. For example, if certain biological feature does not remain the same throughout time (permanence requirement), it could not be recognized, for example voice of a child and grown up person. The same applies to collectability requirement – if the feature could not be saved and used for comparison in the future, in such case recognition stage could not be employed. The same pattern applies to other requirements as well.

In order to understand how each stage works, it is necessary to break it down into smaller processes or steps. The following steps are usually applied to enrollment phase (Raina, 2011)[6]:

1. Person enters his ID which is already recognized by the system (it could be log in ID, national ID, number related with banking details);
2. Person is requested to present his biometrical data – for example put finger on fingerprint scanner, say certain words to voice recognizer;
3. System might ask to repeat step number two in order to compare data;
4. Data is captured in the system following the existing standards;
5. Biometrical data is stored in database along with existing customer identification number (described in point number one).

When enrollment phase is completed, next time the person decides to use certain system he/she is already automatically moved to recognition stage in which different steps are followed:

1. Person enters ID which is already stored and recognized in the system;
2. The system matches person's ID and asks to provide biometrical data;
3. The system compares biometrical data with the data in the system;
4. According to the received results – system decides either to approve or deny person's request.

Each person has more than one biological feature which could be used in enrollment and/or recognition phases. There are a number of analysis conducted on different biometrical features, but

[4] Schouten, B., Jacobs, B., (2009), Biometrics and their use in e-passports, Image and Vision Computing, Volume 27, Issue 3
[5] Yang, W., Hu, J., Yang, J., Wang, S., Shu, L., (2013) 6th International Congress on Image and Signal Processing
[6] Raina, V. K., (2011) *Integration of Biometric authentication procedure in customer oriented payment system in trusted mobile devices*, International Journal of Information Technology Convergence and Service (IJITCS) Vol, 1, No. 6

majority of authors identify, that the main biometrical features which allow to identify person are the following:

- Human face – existing system captures and recognize certain points of human face. It could be done by scanning the face of a person or simply identifying it from a photo or video[7];
- Fingerprint – pattern of finger ridges is captured and stored. There are no two people who share same fingerprint pattern, so this makes fingerprint one of the most suitable biometrical feature for identification purposes;
- Voice – is biological feature of humans which is easy to capture by existing systems and record in order to store in databases. Voice is not considered as most reliable feature in person identification as voice have tendency to change throughout time, voice recording might be influenced by surroundings and etc.[8];
- Iris – colored part of an eye as well as an eye retinal are used for same purpose;
- Signature – even signature is something that does not come with biological features of person, but how person signs, demonstrate certain biological features. How hard and at which steps do people push when signing? Or is there a gap, or signature is written without lifting the hand up from the paper. These features indicate certain biological tendencies which allow to identify the person.

In addition, biological features such as ear, body temperature, DNA could be used for identification, but they are not that widely used due to costs and difficulty in application. All biometrical features have to meet certain characteristics/features, but levels of their suitability vary. Table 1 demonstrates differences between commonly used biometrical features. The ranking is based on how well a certain biometric meets certain requirements, where low means that biometric meets certain features only with minimum requirements and high indicates that biometric feature meets requirement at maximum level.

Table 1. Ranking of biometrics

	Face	**Fingerprint**	**Voice**	**Iris**	**Signature**	**Temperature**	**DNA**
Universality	High	Medium	Medium	High	Low	High	High
Uniqueness	Low	High	Low	High	Low	High	High
Permanence	Medium	High	Low	High	Low	Low	High
Collectability	High	Medium	Medium	Medium	High	High	Low
Performance	Low	High	Low	High	Low	Medium	High

[7] Li, Y., Xu, X., (2009) *Revolutionary information System Application in Biometrcis,* IEEE International Conference on Networking and Digital Society

[8] Jain, A., Ross, A., Prabhakar, S., (2004) *An introduction to biometric Recognition,* IEEE Transactions on Circuits and Systems for Video Technology, Vol. 14, No. 1

Acceptability	High	Medium	High	Low	High	High	Low
Circumvention	Low	High	Low	High	Low	High	High

Source: Bolle et al. (2006)

From information displayed in Table 1 it could be seen that DNA as biometric could be considered as most unique and secure but just because it is low accepted and hard to be collected, it is not considered as most appropriate for daily use in identification process. Voice on the contrary has high level of acceptability and medium level of being collected, but all other requirements are met only at minimum level. Finalizing findings from Table 1, it is seen that fingerprint meets all the criteria at acceptable level. And as it is not changing throughout the time, is acceptable and hard to be faked, it could be considered as one of the most suitable biometric for identification purposes.

Biometrics are physiological or behavioral features. In order to state that certain biometric could be used for identification purposes, it has to meet seven requirements. As existing biometrics meet listed requirements at different levels, it is important to determine what purpose biometric will serve. Literature analysis shows that fingerprint could be considered as the most suitable biometric looking from different perspectives. When biometric feature serves for identification purpose, it is important to determine two main phases – enrollment and recognition as these two phases, one after another, allow to utilize biometric for a complete identification of an individual.

2. BIOMETRICS IN TECHNOLOGIES

Growth and improvement of technologies are rapid nowadays. Usage of technologies in daily life is no longer a question. Currently, more important question is what is next, what companies will deliver to the market? Technologies currently covering fields from toys to space industry and somewhere in between there are technologies which are utilized for making payments.

As described in the first section, different authors agree that fingerprint, due to its certain features is one of the most suitable biometric to use in identification process. When looking from implementing fingerprint as a way of identification in technologies, authors also support this opinion. Garg (2015) states that fingerprint will provide customers with convenient, safe and seamless experience in using technologies[9]. Yang (2013) analyses biometrics in technologies and payments in general, but focuses on usage of fingerprint as the most suitable option[10]. Alimi (2013) focuses on mobile technologies and sees fingerprint as the most suitable biometric due to the structure and features of smartphones[11].

Alongside with scientists and authors of articles, companies developed technologies which allow to utilize biometrics for identifying a person. Apple and Samsung developed smartphones which read fingerprint or iris. Financial companies such as PayPal allows their users to perform financial transaction using biometric authentication. ATM and POS (point of sale) terminal machines are now featured with recognition devices which read certain biometrical feature (Kou, 2003). Research shows that around 30% of companies by the end of 2016 will use biometric authentication for mobile devices and the same research indicates that biometrics technology market grows by 21% annually[9].

There are several reasons why fingerprint is considered the most suitable biometrical feature among companies and scientists:

- More and more technology related features could be managed via smartphone, which is controlled by hand;

[9] Garg, R., Garg, N., (2015) *Developing a Secured Biometric Payments Model Using Tokenization*, Whitepaper
[10] Yang, W., Hu, J., Yang, J., Wang, S., Shu, L., (2013) *Biometrics for Securing Mobile Payments: Benefits, Challenges and Solutions* 6th International Congress on Image and Signal Processing
[11] Alimi, V., Rosenberger, C., Vernois, S., (2013), *A mobile contactless point of sale enhanced by the NFC and biometric technologies* Inl. J. Internet Technology and Secured Transactions, Vol. 5, No, 1

- It is forecasted that in 2016 there will be 2.1 billion smartphone users (The Statistics Portal, 2016)[12];
- Average person have ten fingerprints which all could serve as identification or password when accessing systems;
- Biological features of fingerprint meet main security requirements – it does not change over time period, it is unique (there are no two people with same fingerprint), it is readable and data could be stored.

Biometrics, and especially fingerprint, is becoming part of not only identification of person when accessing certain systems, but also when dealing with payments (Buchmann, 2014). As log ins and payment confirmations are related with sensitive information such as password or payment card details, security becomes very important in all end to end process.

2.1. Biometrics-related security in technologies

When it comes to security in accessing systems, authorizing payments, traditional method is user ID and password or PIN code. Even though it is widely spread, it is not the most secure method. PIN codes, user IDs are generated using certain algorithm which could be hacked, information could be leaked or a person could share his or her sensitive data. In 2015 around 1.5 million cybercrime attacks took place (CBS 2015)[13] which influenced both individuals and companies. Only in the United States of America annual loss from cybercrime is 525 million USD (The Statistics Portal, 2016)[14]. The mentioned numbers just stress importance of security on the internet environment and shows that currently used security measures are not always preventing from possible loses.

The importance of security is also reflected in reports and strategies introduced by financial institutions. Four main pillars or groups of initiatives in security subject could be identified while reviewing overviews by financial institutions:

1. **Internet payment security** – financial institutions are creating guidelines and requirements which have to be met when dealing with internet payments. Main focus area – customer authentication;

[12] The Statistics Portal (2016) *Number of Smartphone users worldwide from 2014 to 2020*. Retrieved from https://www.statista.com/statistics/330695/number-of-smartphone-users-worldwide/
[13] Cybercrime statistic portal. (2015). *Cybercrime statistics.* Retrieved from http://www.cbs.com/shows/csi-cyber/news/1003888/these-cybercrime-statistics-will-make-you-think-twice-about-your-password-where-s-the-csi-cyber-team-when-you-need-them-/
[14] The Statistics Portal. (2016). *Statistics and Market Data on Cybercrime* https://www.statista.com/markets/424/topic/1065/cyber-crime/

2. **Mobile payment security** – this measure is directed to mobile service providers and especially in Europe. As mobile payments are identified as one of the most valuable drivers in the future, these security measures to mobile services providers are delivered with cautious in order not to stop progress of developing new technologies;
3. **Data privacy and protection (including cybersecurity)** – this initiative covers requirements which are delivered to financial institutions which stores customer data. It requires to inform customer and media in case of major security breach within 30 days (Personal Data Notification and Protection Act, 2015) [15].;
4. **Electronic identification and trusted services** – initiative dedicated to Europe and seeks to introduce unified and secure electronic interaction between business, authorities and citizens. This should improve online service and especially e-commerce (World Payment Report, 2015)[16].

In two out of four pillars, customer authentication and mobile payments are the focus area. Different sources indicate that when it comes to security in mobile payments, both parties, consumer and service provider, are involved and could become victims of security breach. Around nine main possible threats could be indicated in mobile payments (Mobile Payments: Risk, Security and Assurance Issues, 2011)[17]. As one the most important risk is named interception of traffic which leads to identity theft. Even though there are countermeasure in place, such as data encryption, security protocols and similar, but still security breaches take place. Figure 1 illustrates different security issues related with mobile payment platforms. Three different systems of mobile platform might be affected by cyber-attack. These attacks cause two main consequences:

1. Repetitive attacks – this means if system is hacked once and no extra counter measures are taken, there is high chance that system will be attacked once again. Frequency of attacks might depend on the system and potential value which could be gained by criminals during the attack. Firstly, an attempt of an attack is made, it is hard to be detected by the system as it is one-time event. If the attempt is successful – criminals might flood the system with massive attacks.
2. Impersonation – an act when the attacker imitates to be a legitimate customer. This could happen either when identity (user ID and password) is stolen or the data base of the service provider is compromised. In originally introduced mobile payments (when transaction is

[15] Personal Data Notification and Protection Act of 2015, U.S., Mar. 26, 2015, H.R.1704
[16] World Payments Report 2015 (2015), Royal Bank of Scotland
[17] Mobile Payments: Risk, Security and Assurance Issues, (2011), *An ISACA Emerging Technology White Paper*. Retrieved from http://www.isaca.org/Groups/Professional-English/pci-compliance/GroupDocuments/MobilePaymentsWP.pdf

submitted from and to mobile account linked to mobile operator), impersonation is related to cloning sim card of the customer. When smartphone was introduced, mobile payment area became broader, as now mobile payment is also considered when the person uses smartphone to log in to his or her bank account and makes a payment. So in this sense, cloning SIM card is no longer valid as in order to imitate a genuine customer – it is necessary to know the log in credentials, password for payment authentication and in more advanced systems, even to be connected via legitimate customer's device

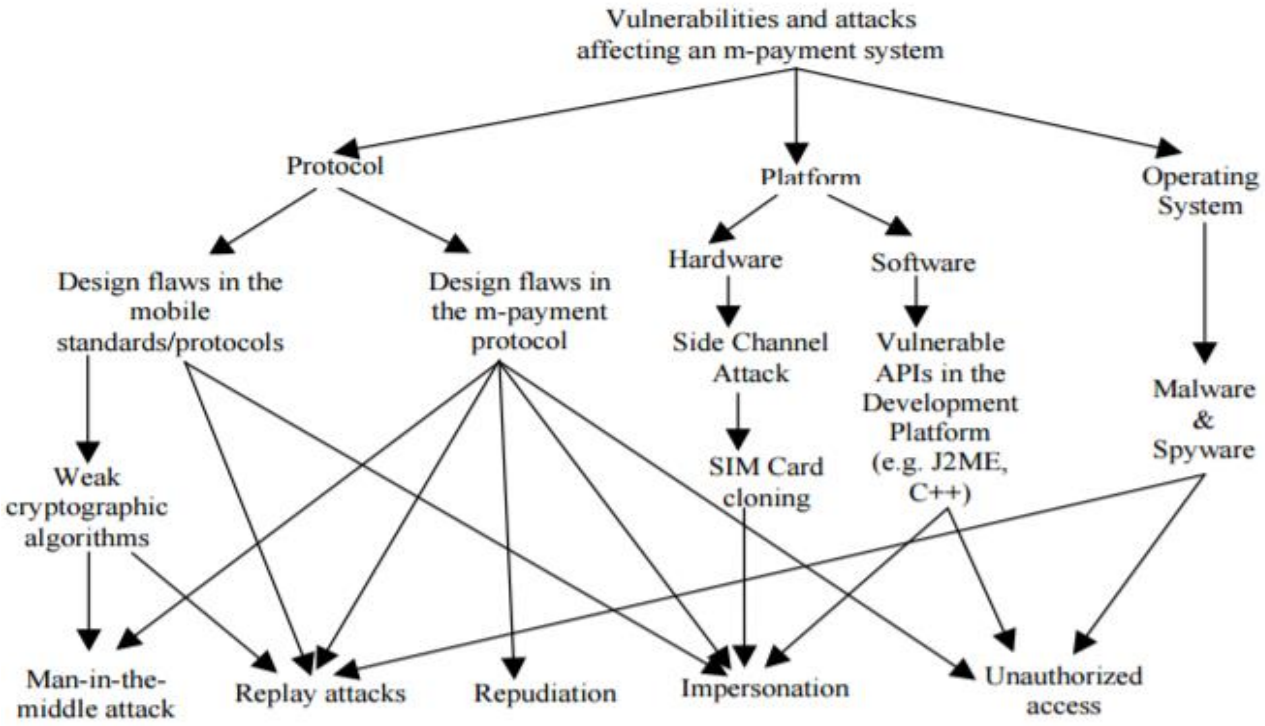

Figure 1. Vulnerabilities affecting mobile payment systems. Source (Agrawal et al. 2011)[18]

Countermeasures against system attacks and identity thefts are put in place by developers and companies which care about their reputation and customers. Because SIM card based mobile payments are put aside due to expansion of smartphone and mobile internet, companies have to introduce new ways how to identify and allow customers to authorize payments. One of the solutions is implementing biometrics into mobile payments authorization process. Currently different solutions exist. According to (Raina, 2011)[19] integrating multimodal biometric payment model into biometric multi-server authentication model could be a solution. A combination of these two models give a user friendly payment options to customers and also ability to connect to several different servers while

[18]Agarwal, S., Khapra, M., Menezes, B., Uchat, N., (2014) *Security issues in mobile payment systems* Department of Computer Science and Engineering, IIT

[19]Raina, V. K., (2011) *Integration of Biometric authentication procedure in customer oriented payment system in trusted mobile devices*, International Journal of Information Technology Convergence and Service (IJITCS) Vol, 1, No. 6

maintaining a high level of security. This model combination supports and addresses the risk mentioned in the article of security issues in mobile payments (Agrawal et al. 2011). According to authors this module will allow to resist:

- Guessing attack – when fake customer tries to guess credential of log in;
- Replay attacks – when a successful attempt leads to massive attacks;
- Stolen credential attacks – as it would be hard to steel biometrical data of a person;
- Insider attack – password and ID, even if it is encrypted, could be decrypted and compromised by internal employee, while fingerprint or other biometrical feature is hard to replicate as in authentication process it has to be delivered physically;
- Server spoofing attacks;
- Registration spoofing attacks;
- Impersonation attacks – as biometrical metric is hard to fake and present it physically during authentication or payment authorization process.

Biometrics in terms of security brings lots of value and allows to avoid potential risks which could not be addressed by pin based or password based security systems. There are several reasons as to why companies have not implemented biometrics in its security or authorization processes. Even if biometrics brings benefits such as cost reduction, improved security and customer satisfaction, companies who already have PIN based systems are not willing to invest additional money because existing systems work and security and customer expectations are met. The mentioned factors convincingly are not materialized when comparing these two systems (Breebart, at al., 2011)[20]. There are opinions that even with this amount of benefits biometrics are not always the most suitable measure. Biometrics are safe and secure only to the level how secure are mechanisms in which data is stored (Schneier, 2009)[21]. Different opinion from authors is demonstrated by financial institutions, which state that majority of banks and other financial institutions indicates that biometrics services are in top priority list. Figure 2 demonstrates that 65% of respondents of financial institutions plan to have biometrics in their systems. Moreover, for more than half of them, fingerprint is priority. Second most popular biometric security measure, according to respondents is voice recognition. Referring to the previously listed strengths and weaknesses of fingerprint and voice, financial institutions select more reliable and better data stored feature – fingerprint. Majority of financial institutions (70%) indicate that in their process, most important thing is proper identification of customer and authorization of payment. Financial institutions are strictly regulated by government authorities, so

[20]Breebaart, J., Buhan, I., Groot, K., Kelkboom, E. (2011), *Evaluation of a template protection approach to integrate fingerprint biometrics in a PIN-based payment infrastructure*
[21]Schneier, B., (2009). *Biometrics*. Retrieved from https://www.schneier.com/blog/archives/2009/01/biometrics.html

search of more secured solutions is reasonable and is in line with meeting requirements set by governments.

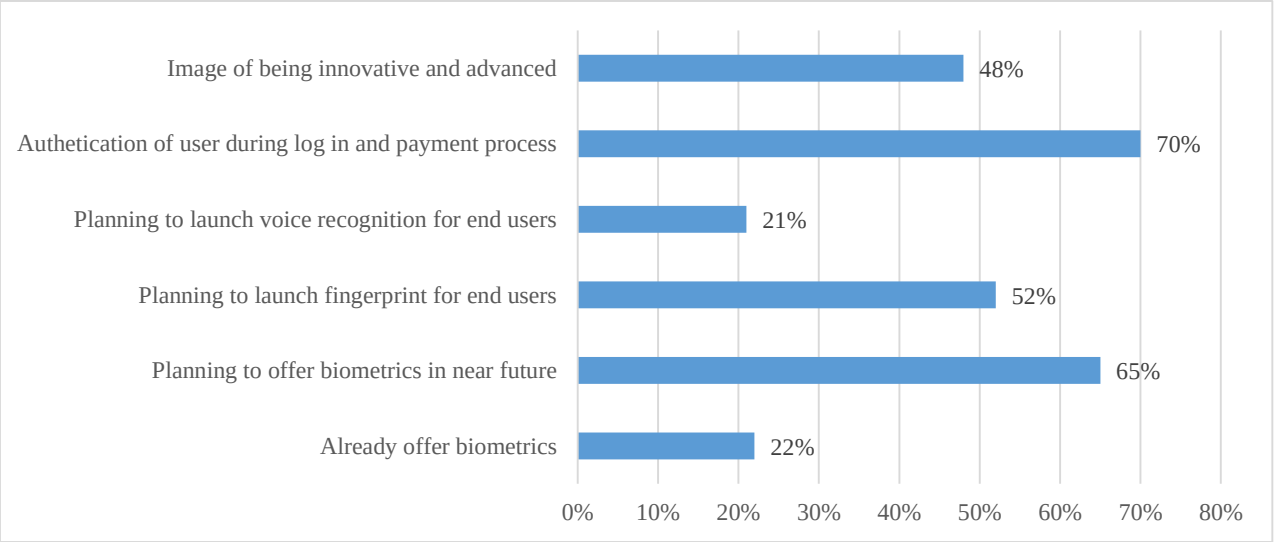

Figure 2. Priorities in financial sector. Adapted according to (Nordlund, 2016)

Beside secured identification of customer and proper payment authorization almost half of financial institutions stated that providing service to the customer in convenient way is also very important. The same respondents aim at being seen as innovative and advanced banks (Nordlund, 2016)[22].

End to end process of financial transaction, includes financial institution on one end, and customers on the other. Banks and other financial institutions, according to the data, are willing to move to biometrics in their systems and processes. Study made by Visa demonstrates that customers are also in favor of using biometrics and even have preferences on which type to use. 14 000 European consumers were interviewed in 2016. Figure 3 shows, that consumers similarly to banks prefer fingerprint option as the main feature of biometrics. Consumers would also like to have iris (retinal scanning) as option, which was not named and focus area by the banks. One third of respondents indicated that they would like biometric authentication not to stand alone and be combined with currently used PIN based systems. Voice or face recognition is not on the top of the list of consumers in Europe and this just supports theoretical background which indicates that these two features have drawbacks looking from several different perspectives. Majority of respondents indicated that biometric, as way of approving payments, would be most useful in online shopping.

[22]Nordlund, S. (2016), *Mobile biometrics has finally come of age*, European Payments Council Newsletter Issue 30

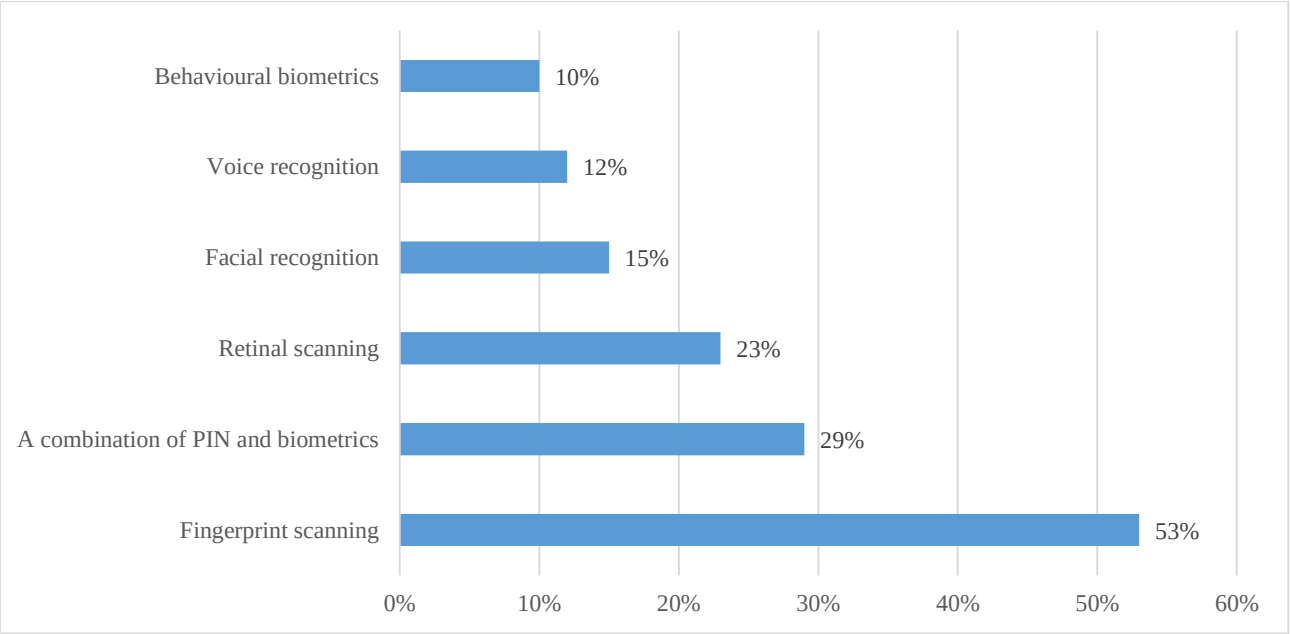

Figure 3. Consumer preferences for using biometric authentication for payments in the future. Source (Visa report, 2016)

Consumers indicated that, when looking solely at the perceived security provided by biometric technologies, around 81% selected fingerprint as the most secure option (Visa report, 20016)[23]. On the other hand, around 70% of respondents in the mentioned study, provided information that they are equally comfortable to use either current PIN based security system or fingerprint based system. Visa report showed that consumers would also like to use biometrical authentication not only in online environment. When consumers were asked about places where they would like to use this option, following results were mentioned:

- Payments on public transport;
- Payments at the bar/restaurant;
- Payments for good and services at retail;
- Payments when shopping online;
- Payments for content download.

Consumers indicate several different places and goods or services which are in favor to adopt biometrics in its payment systems. According to Visa report data around 30% of consumers usually abandons final payment phase just because feeling not fully secured in making this step and as study shows that confident in biometrics exists among consumers and financial institutions, this could be opportunity for both side to reduce this avoidance of payments due to feeling unsecure.

In order to understand why financial institutions and consumers are willing to implement and use biometrics in daily processes it is necessary to know how transactional flow looks in both PIN based and biometrics-based models.

[23] *European consumers ready to use biometrics for securing payments*, research by Visa, (2016)

Figure 4 illustrates simplified transaction, when payment is card funded. In this flow consumer enters his payment, credit or debit, card information which is verified in bank's database whether the data is valid and the payment card exists. There are more steps involved in this process, such as entering amount of transaction, checking if there is sufficient funds on the account and etc. Assuming that payment card is valid and the funds are sufficient the process is similar to the one indicated in Figure 4. Upon the completion of the verification, the consumer either gets the transaction processed, or is asked to enter the password; after successful entry – transaction is processed. In this flow there are several areas where security breach might occur. First, payment card information could be compromised and used not by a genuine customer. In the instances when password is not required this information is sufficient to submit fraudulent transaction.

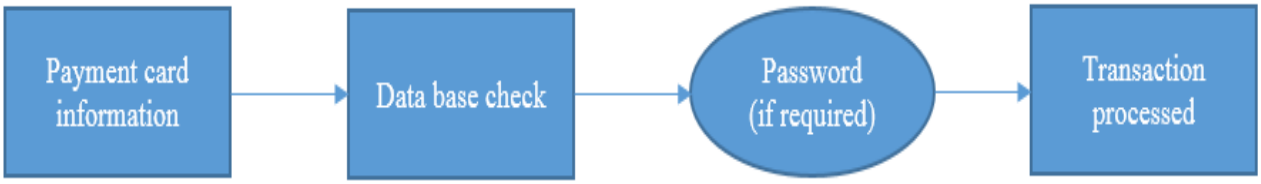

Figure 4. Simplified traditional card funded transaction flow. Adopted according to (Breebaart et al. 2011)

Figure 5 illustrates the same card funded transaction but just placed on biometrics-based process. In this flow, when consumer enters his or her payment card information, he or she has to validate identity by biometric data. It could be fingerprint, voice, iris or any other data depending on the system. While consumer gets biometrical data verified, bank data base simultaneously checks if payment card information is valid. Thus in this flow two verification processes are carried out at the same time. In systems where password is required, consumer has to enter a password. This would represent dual approach model, when two security measures (biometric and password authorization take place). The final stage before processing with transaction is to check whether the information matches – if the person who entered payment card details is the same person who registered the biometrics linked to this payment card. When payment card information matches biometrical information and vise a versa – transaction could be processed.

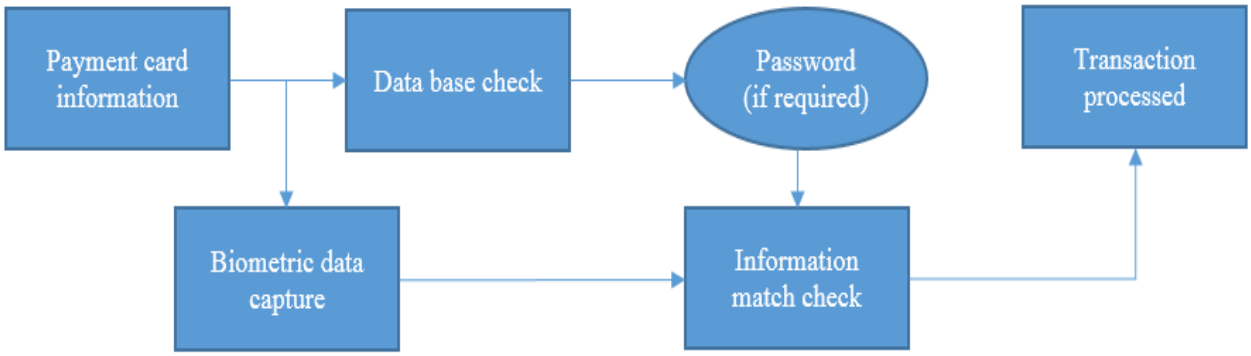

Figure 5. Simplified biometric based card funded transaction flow. Adopted according to (Breebaart et al. 2011)

Comparing flows, demonstrated in Figures 4 and 5, it is visible that in biometrical based flow additional security measures are implemented. In case payment card information is compromised and data base check process is done, transaction will not be processed as payment card and biometrical data match will not be performed as fraudster does not have access to customer's biometrical data. In this case money transfer would be declined. Even if biometrical based process looks more complex, this does not cause any inconveniences to the customer as both data checks are performed simultaneously.

One more important difference between biometrical based and password/PIN based authentication processes is the measurement of how to indicate if authentication was successful or not. In PIN based system it is done simply – entered PIN/password is either correct or incorrect. Biometrics are not binary measurement, it is based on probability of match (Visa report, 2016)[24] in this, case authentication process is based on false positive result. In biometrical authentication model, knowing that it is based on probability of match, technology which is used in the process plays an important role. Technology such as swipe fingerprint sensors are considered as cheaper to implement but level of accuracy is low compared with static fingerprint sensors (360 Biometrics, 2016)[25]. Other technologies such as eye scanners are considered as the most accurate (Nordlund, 2016)[26] but as it requires bigger investments it is not well spread as technological solution.

Topic of security, in terms of technology and payments, is well studied and addressed by both scientists and companies (Goode, 2014), who are inventing new technologies or are willing to invest into it for company's and its costumer's needs. Financial institution is not an exception. Initiatives show that banks, which are major players in payments, focuse on customer authentication and secure payment flows. Two major security problems are identified by several different authors. These

[24] *European consumers ready to use biometrics for securing payments*, research by Visa, (2016)
[25] 360 Biometrics. (2016). *Frequently asked questions*. Retrieved from http://360biometrics.com/faq/biometrics.php
[26] Nordlund, S. (2016), *Mobile biometrics has finally come of age*, European Payments Council Newsletter Issue 30

problems are related to system issues which cause repetitive security breaches and impersonation, when fraudulent activity is performed in order to pretend to be a genuine customer. Several countermeasures to prevent from named problems exist and biometrics is recognized as a solution which minimizes possibilities of security breaches. Popularity of biometrics is represented in studies and surveys performed by market players such as Visa or institutions such as European Payments Council. Studies showed that around 65% of banks and other financial institution are ready to implement biometric in near future as a tool to improve security. On the other hand, 22% of these institutions already offers biometrical solution for the customers. Willingness of financial institutions are also supported by consumers. Around 80% of them are willing to use biometrics and think that security is the main attribute when deciding on authorizing a payment. Both financial institutions and consumers agree that fingerprint as biometrical option is the most suitable. When comparing traditional (PIN/password based) and biometrical process flow in payment authorization, it is seen that by implementing just one additional step of biometric authorization, increases level of security in payment process. Key difference is that in biometric process flow, payment card information is compared and matched with biometrical one, and only then payment could be processed. In case of fraudulent activity, when payment card information is compromised, it is not enough to process the payment. Success of biometrical authentication is based on false positive response, instead of correct or incorrect password, this fact stresses the importance of what technology is used in the process. Taking into consideration costs, reliability, easiness of use – fingerprint solutions demonstrates solid performance and are in favor amongst financial institutions and consumers.

3. ENVIRONMENT FOR MOBILE PAYMENTS AND BIOMETRICS IN LITHUANIA

Studies analyzed in section 2, demonstrates that consumers and businesses are ready and willing to adopt biometrics in payment processes. Researches demonstrates a picture of Europe as the whole, but not divided into individual countries. Looking from global world perspective it makes sense, especially when digital payments are internet based and world wide web eliminates boundaries between countries. Despite united Europe and global world, companies and consumers tend to behave differently in different countries and Lithuania is not an exception.

Lithuania has been six years in a row in a leading position in terms of fiber-optic internet network penetration (Invest Lithuania, 2015)[27] in Europe, but mobile payments and biometrics are not as developed and widely used as in other countries. In 2013 one of commercial banks in Lithuania, Danske Bank, was first to introduce mobile payment option to its customers. It was PIN based payment where each user could set their own transactional limits (Finextra, 2013)[28]. In that year 50% of new phones bought in Lithuania were smartphones, director of Danske Bank Corporate Development, expressed regret that the potential of smartphone is still not utilized.

Data and forecasts for Lithuania in mobile payments area look optimistic. Figure 6 illustrates how value sent in mobile payments will have an upward tendency in Lithuania until 2020. Even if the current situation in 2016 demonstrates value of 5 million USD sent per year, in 4-year perspective this value will grow approximately 12 times. Even with this kind of increase Lithuania is far behind the United States of America, where in 2016 value of mobile payments was 29 billion USD (Statista, 2016)[29].

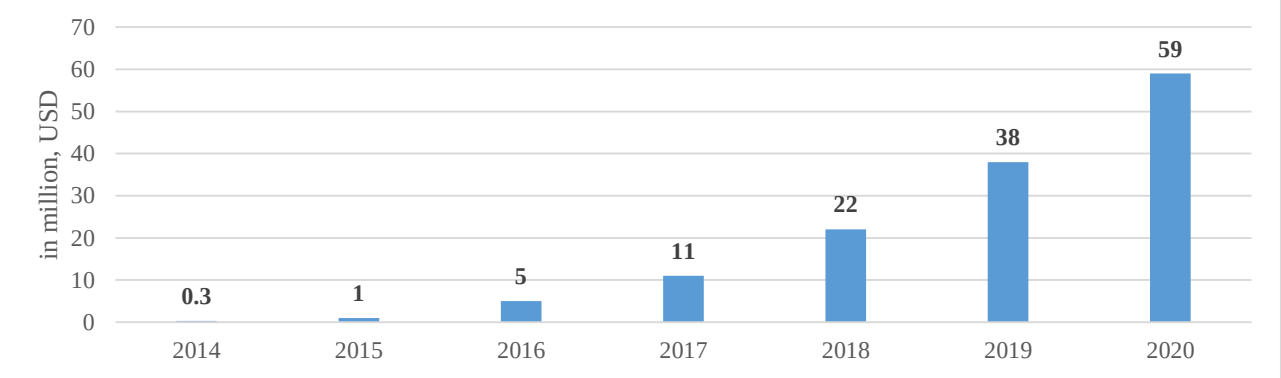

Figure 6. Transaction value in mobile payments segment in Lithuania. Source (Statista, 2016)

[27]Invest Lithuania. (2015). *Lithuania Europe's No. 1 in fiber-optic internet penetration*. Retrieved from http://www.investlithuania.com/news/lithuania-europes-no-1-in-fibre-optic-internet-penetration/
[28] Finextra. (2013). *Danske Bank brings mobile payments to Lithuania*. Retrieved from https://www.finextra.com/news/announcement.aspx?pressreleaseid=52428
[29]Statista. (2016). *Mobile Payments*. Retrieved from https://www.statista.com/outlook/331/143/mobile-payments/lithuania#

Growth ratio of mobile payments value in Lithuania in upcoming years demonstrates potential for companies to invest in this field. Figure 7 shows that growth ratio for mobile payments value in 2017 will be around 130% compared to the year 2016. Even seeing that growth ratio is decreasing, it will still bring 55% growth in 2020. Value growth will be driven by increased value per transaction, because growth of new user in mobile payments in period of 2016-2020 is forecasted to fluctuate from 3% to 6% per year and reach around 200 thousand users in 2020 (Statista, 2016)[30].

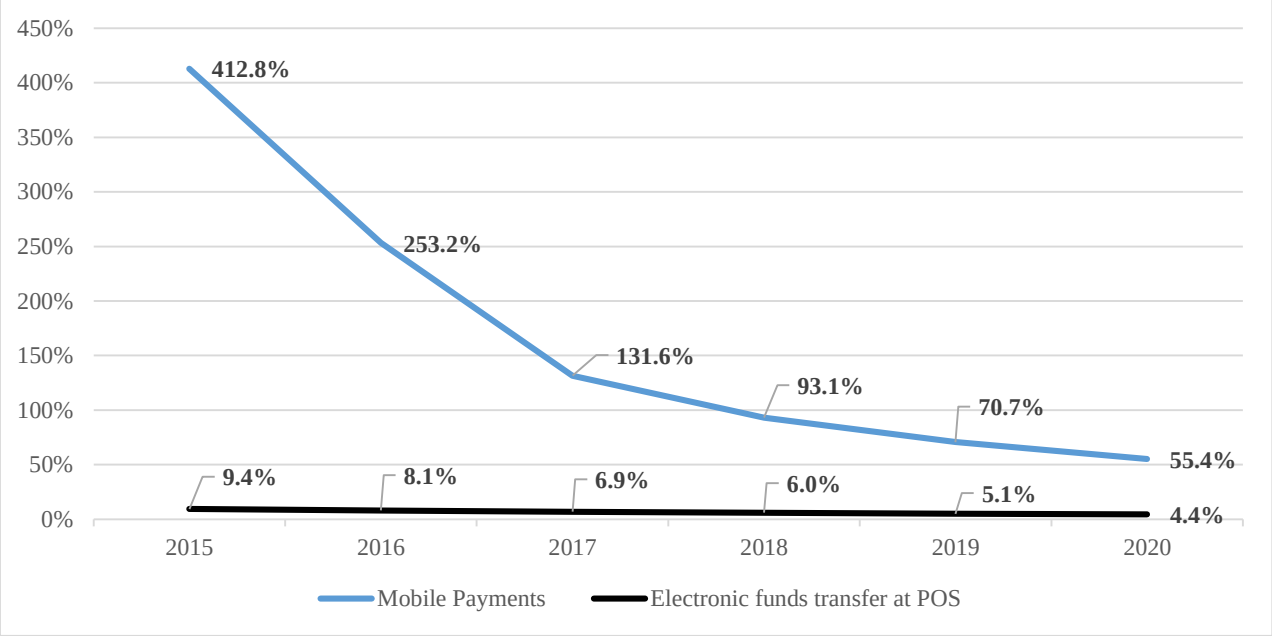

Figure 7. Mobile payments transaction value growth in Lithuania. Source (Statista, 2016)

Mobile payments value growth compared with traditional electronic funds transfer value at point of sales demonstrates double digit increase on a yearly basis, but as demonstrated in Figure 8, value expressed in currency, will still represent low part among all digital payments in Lithuania. Only in 2020, mobile payments will represent more than 1% from total electronic funds transfer value. This is mostly driven by the fact, that value of one mobile payment transaction is going to be 3-6 times lower compared with other digital commerce transactions in Lithuania (Statista, 2016)[31].

[30] Statista. (2016). *Mobile Payments*. Retrieved from https://www.statista.com/outlook/331/143/mobile-payments/lithuania#
[31] Statista. (2016). *Digital Payments*. Retrieved from https://www.statista.com/outlook/296/143/digital-payments/lithuania#

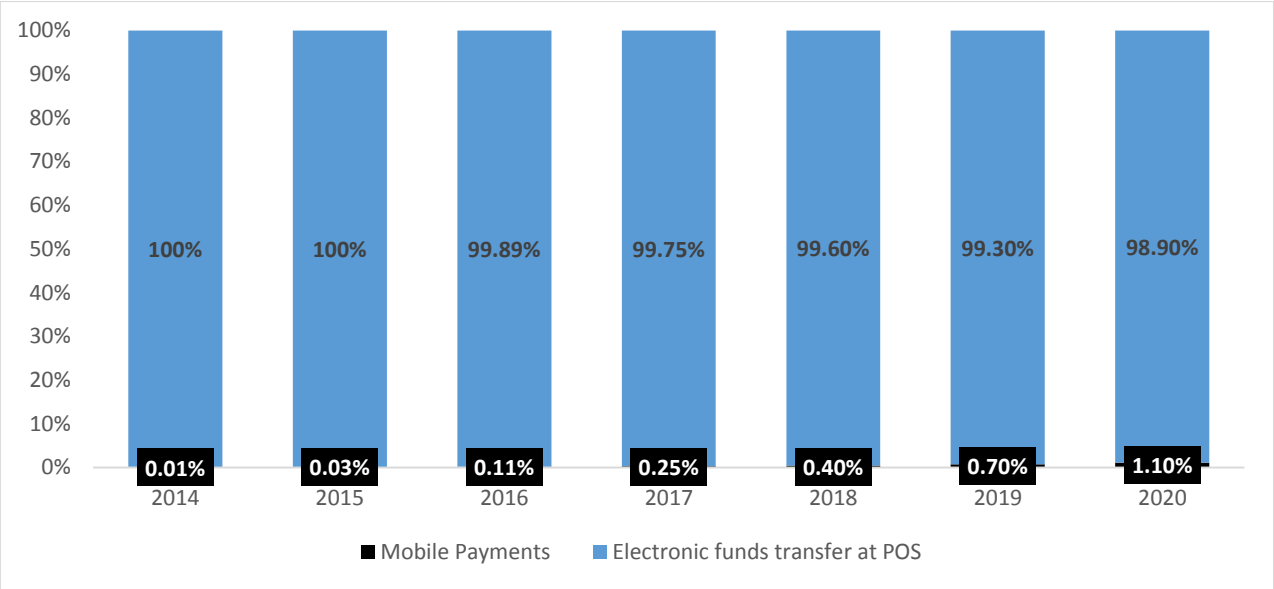

Figure 8. Benchmark of transaction value in Lithuania. Source (Statista, 2016)

Mobile payments, according to the numbers, demonstrate growth potential in upcoming years. Market share compared to all digital payments is, and forecasted to be, low but yearly value of 59 million USD indicates potential for companies to expand in this market. Studies made by Visa in Europe indicated, that one of the most important factors in payment area is security and solution for increasing it was biometrics, with the biggest focus put on fingerprint. Current mobile and digital solutions in Lithuania do not provide an option to authorize payment or identify consumers using biometrical data such as fingerprint, voice recognition, iris, etc. Current solutions are based on code generators, code cards, e. signature but not simple solution of verifying payment with the touch of a finger. Based on statistics, there are around 116 companies which operate in the field of biometrics, but none of them works in financial sector (Sourcesecurity, 2016)[32]. Most of these companies provide solutions for physical security, access control and similar security related features. Even if it is not payment related field, a number of companies in Lithuania illustrate, that if biometrical data was to be implemented in payment field, there already exist expertise in the market, which could be used. The fact that there are experts in applying biometrics in technologies and person identification using biometrics is demonstrated by the government. Back in August, 2006 first Lithuanian biometrical passport was issued. After two years, in 2008 new model civil servant certificates with integrated chip containing biometrical data was issued (Personalization Center, 2009)[33]. Ten years has passed since the first biometrical passport was issued in Lithuania and the government is still investing in improving biometrics-based systems. In 2015, Lithuanian authorities and company "Morpho" signed an agreement, according to which the company will provide 145 fingerprint readers which will be

[32]Sourcesecurity. (2016). *Biometric companies in Lithuania*. Retrieved from http://www.sourcesecurity.com/companies/search-results/company-search/pa.biometrics,c.lithuania.html?page=1
[33]Personalization center. (2008). *Biometrics in eID cards*. Retrieved from https://www.dokumentai.lt/viewpage.php?page_id=79

used to process all requests for visa documents (Mayhew, 2015)[34]. Examples from Lithuanian government show that technologies which use biometrics for person identification, biometrical information capturing, data storing and matching existing data bases in real time situations, are already in place and widely used. It could be considered that there is only one step left in adoption of existing practices to payment industry, and Lithuania is ready to use a more secured way for payment authorization.

In order to get full picture about environment for establishing biometrics-based payment authorization it is necessary to understand legal environment in Lithuania, both from legal acts and the perspective of controlling government bodies.

3.1. Legal environment of payments related area in Lithuania

Several different laws regulating payments and governmental institutions monitoring legal procedures in the area of payment exists in Lithuania. Also as Lithuania is part of European Union (EU), part of requirements, recommendations and regulations are aligned with EU. The main payment related document in Lithuania is Payments Law of the Republic of Lithuania.

Payments Law (Payments Law) describes payment service provider's services and responsibilities, rights and duties of regulatory institutions, conditions for payment services, for both, consumers and business sides, also authorization and security of payments (Republic of Lithuania Payments Law, 2016)[35]. Payments Law is applicable to payment service institution such as banks, central bank, post, e. currency institutions and other entities which deals with payments. 3rd article of Payments Law describes what services should be considered as payment services, but also sets out 16 exceptions of services which are outside the scope of Payments Law. Putting this law into framework of mobile payments in consumer to business model (C2B) which have biometrics as terms of security, Payments Law states the exception, that this law is not applicable to services, which are provided by technical service providers, which are responsible for smooth payment process but never participates in receiving funds of payment. The 3rd article also states that Payments Law is not applicable, if service provider is responsible for security measures, identity authentication, data base maintenance or providing connection services. In these terms, company or C2B model, which would provide biometric security services in mobile payments and would act only as intermediator without receiving payment amount, would not be considered as payment institution. Section 2, 5th article of

[34]Mayhew, S. (2015). *Lithuania to deploy MorphoTOP fingerprint scanners for visa requests*. Retrieved from http://www.biometricupdate.com/201503/lithuania-to-deploy-morphotop-fingerprint-scanners-for-visa-requests
[35]Republic of Lithuania Payments Law (2016). Valstybės žinios, 1999-11-17, Nr. 97-2775. Retrieved from https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.89775/dimqMSiPWp

Payments Law describes what should be considered as payment service or payment operation. Excluding traditional cash payment operations, Payments Law sets out that payment operation is the operation when payer provides agreement to make a payment via digital or telecommunication devices and using services of connection provider. According to this condition, mobile payment is considered as subject of Payments Law in Lithuania. Together with providing explanations on what is considered payment service provider and payment service itself, Payments Law also describes authentication and security measures. Article 24 of the Payments Law indicates what is considered as an agreement for authorizing a payment operation. Payment operation is considered to be authorized only when the payer provides an agreement to authorize the payment. In which form authorization is provided – is an agreement between the payer and the service provider. Going back to C2B model in mobile payments which use biometrics as security option, according to the Payments Law, if agreement of authorization form between service provider and payer is made, Payments Law does not limit the form of agreement, so in this case payment could be authorized or, agreement to make a payment could be made based on biometrics options; for example, approving payment with fingerprint. Usage of biometrics in authorizing payments, could be a solution in situations when fraudulent consumers tends to gain value from bank or service provider and denies approving a payment. In 29th article of Payments Law, situations regarding proof of authorizing payment are described. In case of occurrence of fraudulent activity by consumer, when consumer claims that he did not authorized a payment, and issues a claim for a refund, payment service provider or financial institution, such as bank, has to prove that everything was done proper in payment process, and consumer himself/herself authorized payment as otherwise service provider has to refund the amount claimed by the consumer. If biometrics was used in payment process for authorizing payments, it would be difficult for fraudulent activity to take place. In section two, process flow of payment with biometrics as one of security measures is described and it showed that when using this option additional match between payment information and biometrical information is performed. In cases where consumer claims that he/she did not authorized the payment, this additional match would allow to clarify the dispute who indeed authorized the payment. Current situation, when authorization of the payment is questionable, influences not only service providers, but also genuine consumers. Article 31st of Payments Law sets out that consumer might be eligible to cover expenses from 50 to 150 EUR if unauthorized payment confirmation took place. In these type of situations implementing biometrics would be a win-win situation for both, consumers and payment service providers.

Together with legal documents available in Lithuania, some government institutions are also actively participating in improving payment service environment. Central Bank of Lithuania is one of the most active participants in this field. In June, 2016 Central Bank of Lithuania introduced

National Payment Strategy the aim of which is to achieve that in 2020 for citizens of Lithuania new electronical payment methods, such as near field communication based payments, would be available and all these new business models could be easily integrated into the existing ones. Central Bank of Lithuania strives to achieve, that new payment methods would be widely spread and well used by consumers in Lithuania (National Payment Strategy, 2016)[36]. Alongside with National Payment Strategy, Central Bank of Lithuania introduced best practice principals for payment initiation service providers. Central Bank of Lithuania listed seven principles which cover, security, data protection, clarity in providing services and information, agreements between service provider and consumer, requirements for technical infrastructure (Best Practice Principles, 2016)[37]. Looking into National Payment Strategy, introduced by Central Bank of Lithuania, three main strategical directions are discussed in the paper:

1. Develop infrastructure between point of sales and payment service providers, which will create environment for NFC and instant payment mass usage, and will ensure economy of scale for creating and producing payment options;
2. Increase involvement of consumers in decision making, regarding development of payment services and future trends;
3. Increase trust of consumers in payment service providers and payment options which will form new consumer behaviors in using payment methods.

National Payment Strategy includes several initiatives related to new payment methods, such as using social network as payment option, but lacks of initiatives related to using new security measures such as biometrics in payment processes.

Legal environment in Lithuania and the initiatives coming from regulatory institutions indicate that overall environment in Lithuania for mobile payments which use biometrics as way of security measurement is properly regulated and open for service providers to be active in the market. Previously analyzed data illustrates that value of mobile payments in Lithuania is significantly low compared with rest of digital payments. Looking into Lithuanian market there were several companies which tried to offer mobile payment options. In 2011 "MokiPay Europe" introduced NFC stickers but after a short time kept focus only on payments in schools and universities, "EVP International" introduced trademark "Paysera", "WoraPay" allows mobile payments and payments in

[36]Central Bank of Lithuania (2016). *National Payment Strategy*. Retrieved from https://www.lb.lt/n27462/konsultacija_del_strategijos.pdf
[37]Central Bank of Lithuania (2016). *Best Practice Principles*. Retrieved from https://www.lb.lt/gerosios_praktikos_principai

distance, but all these market players represent less than 1% of all market. There are two main reasons for that (Verslo Žinios, 2015)[38]:

1. There is no possibility to directly connect your banking credentials (bank account) to other payment method – consumer in order to use other payment method has to transfer funds to other account and only then use payment method;
2. Existing infrastructure is too outdated to support new technologies and new payment methods.

Environment in Lithuania for mobile payments in upcoming four years indicates big potential. Value sent via mobile payments per year will increase almost 12 times until 2020. Growth rate in value sent via mobile payments demonstrates double digit growth perspective. Of course, compared with such countries as the United States of America, values in Lithuania, even in 2020 looks very small, but for country where projection is to have 200 thousand mobile payment users in 2020, 60 million dollars sent per year in 2020 using mobile payments is a valuable result. Lithuania is a conservative country and it is clearly seen in the numbers which represents that even with such growth rates mobile payments in 2020 will only represent 1.1% of total market share of digital payments. With number indicating this potential Lithuania lacks companies which could introduce biometrics into payments area. Even if there are more than 100 companies operating in the field of biometrics, none of them focus on financial area. On the other hand, government institutions demonstrate better adoption of biometrics in their services. Already in 2006 first passport with biometrical data was introduced and new technologies were implemented in other government controlled areas. In 2015 Lithuanian government bought more than 100 new, high quality fingerprint readers which support all services related with providing visa documents. Legal environment in Lithuania both laws and regulatory institutions create positive surroundings for mobile payment growth. Republic of Lithuania Payments Law does not require becoming a payment institution, if a company decides to introduce biometrics-based payment authorization or customer identification model, as long as the amount paid is not sent to this service provider's account. This fact gives ground to establish an intermediary between consumer and service provider. Initiatives introduced by Central bank of Lithuania support new payment methods and security in it. Considering all the facts Lithuania has created a decent environment from growth potential and legal points of view to introduce new payment methods. As security is one of the priorities in Europe and Lithuania, biometrics based solutions also could be implemented. Only roadblocks are old infrastructure and no possibility to directly connect consumer

[38] Verslo Žinios (2015). Mobilieji atsiskaitymai: permainos neišvengiamos. Retrieved from http://vz.lt/sektoriai/informacines-technologijos-telekomunikacijos/2015/12/20/mobilieji-atsiskaitymai-permainos-neisvengiamos

bank account to payment method which is not supported by bank. This concern is already addressed and going to be solved by EU new Payment service directive.

The data provided by studies made by Visa and European Payments Council, also environment analysis in Lithuania, raise question as to how to implement best existing practice and what best example to choose in order to create biometrics-based payment confirmation model in Lithuania, which would fit C2B mobile payments.

4. METHODOLOGY FOR RESEARCH ON MODEL CREATION IN LITHUANIA

Creating mobile payment confirmation model, comparative analysis of other countries is required in order to identify, if the country specifics in digital payments matter, when deciding if new payment confirmation model should be introduced. After comparative analysis of countries, case study on existing model and its adoption has to be conducted.

Research purpose. To create biometrics based mobile payment confirmation process model, which could be adopted in Lithuanian.

Objectives:

1. Analyze biometrics and determine most suitable biometrical feature to be used in person authentication;
2. Review environment for mobile payments in Lithuania;
3. Identify biometrics-based payment confirmation model, which could be used as an example in creating process model to Lithuania.

Research object. Biometrics and biometrics based payment confirmation model, which could be implemented in Lithuania according to existing legal and mobile payments environment. Research on object is supported by scientific articles, legal documents, statistical data analysis.

Following research methods were used:

- Review and analysis of scientific literature and researches;
- Review and analysis of legal documents;
- Statistical data analysis;
- Case study.

4.1. Literature overview supporting selected research method

Literature overview suggests several different ways of how to conduct a research in social or business science. Each method is supported by advantages and disadvantages, which allows to distinguish between methods and find the best suitable for conducting a research. Depending on the field of research, hypothesis, historical data, behavioral data, survey data, is subject of research one-time occasion or pattern of occasions and other aspects, influence selection of research type. Research methods could be, but not limited to, following (Yin, 2009)[39]:

[39]Yin, K., (2009) Case Study Research design and Methods, 4th edition, Applied Social Research Methods Series, Volume 5 ISBN 978-1-4129-6099-1

- Experiment;
- Survey;
- Case study;
- Economic research;
- Epidemiologic research.

In order to determine which type of research could be the most suitable to conduct and what model could be applied in Lithuanian case, it is important to understand specifics of each model. When considering different models, three conditions have to be kept in mind, first one considered as the most important (Yin, 2009)[39]:

a) What was the research question?
b) What control does the researcher have over actual behavioral events?
c) Degree of focus on contemporary to historical events

Table 2 represents importance of each of the above mentioned condition when deciding which research method should be used. Column called "Form of question" covers question or hypothesis of research, if question or hypothesis is formulated in form to answer questions how and why, research method should be selected, from experiment, historical analysis or case study, because questions themselves are explanatory.

Table 2. Different research methods comparison

Method	**Form of question**	**Control over actual behavioral events**	**Focus on contemporary events**
Experiment	How? Why?	yes	yes
Survey	Who, what, where, how many, how much?	no	yes
Archival analysis	Who, what, where, how many, how much?	no	Yes/no
Historical analysis	How? Why?	no	no
Case study	How? Why?	no	yes

Source: Yin, 2009

Based on the question raised at the end of theoretical analysis part, three possible options could be suitable in selecting research form. As biometrics and its usage in mobile payments is relatively recent, historical analysis method is not suitable in establishing basis for creating a model, which could be introduced in Lithuania. Experiment and case study, both methods focus on contemporary data, except that experiment has influence on actual behavioral events. Actual behavioral events were not in scope of research and subject of research is more contemporary data driven. Case study research method accommodates necessary requirements to answer research question.

The word "case" means "an instance of something", this gives a definition of case study as research or an investigation of "the one", or to be more specific an "instance of" something, that comprise cases in the study (Rose at al. 2015)[40]. Other authors also agree that case study method, allows to closely examine data within specific context (Zainal, 2007)[41]. In this term, case could be something more specific like organization, group of people or individual, or something more abstract, like an event, some kind of program. According to scientists, other features which are related to case study are:

- *In-depth study of a small number of cases, often longitudinally (prospectively or retrospectively).*
- *Data are collected and analyzed about a large number of features of each case.*
- *Cases are studied in their real-life context; understanding how the case influences and is influenced by its context is often of central interest to case researchers.*
- *Cases are naturally occurring in the sense that they are not manipulated as in an experiment.*
- *The use of multiple sources of data including interviews, observation, archival documents and even physical artefacts to allow triangulation of findings* (Rose at al. 2015).

Listed features of case study allow to include both quantitative and qualitative data, by this, case study includes explanation on both process and result of instance (Tellis, 1997)[42]. Fields where case study as research method applies vary and different authors have different opinions where this research method should be applied. Sociology, law, medicine, education – are subjects listed in several scientific articles (Zainal, 2007). Other opinions link case study to subjects such as information systems, strategy, innovation, organizational changes and similar (Rose at al., 2015). Case study allows deep analysis with involving multiple sources of information and when detailed descriptive researches is needed. It allows to focus on some specific or unique case. In terms of uniqueness, it means that only very small number or instances are examined in very detailed manner. Case studies also might be used when question of research is related to process and its improvement, this is because case study supports multiple data sources and gives ability to focus not only on contemporary, but also on retrospective events. When selecting case study as a research option, two main things have to be considered – what cases and how many cases should be explored in research. The biggest concern related to case study, according to authors (Rose at al., 2015), is if a single case is sufficient to conduct a proper research. Single case study raises concern such as:

[40]Rose, S., Spinks, N., Canhato, A., (2015) *Management Research: Applying the Principles*. Retrieved from http://documents.routledge-interactive.s3.amazonaws.com/9780415628129/Chapter%206%20-%20Case%20study%20research%20design%20final_edited.pdf

[41]Zainal, Z., (2007) *Case study as a research method.* Retrieved from http://psyking.net/htmlobj-3837/case_study_as_a_research_method.pdf

[42]Tellis, W. (1997) *Introduction to case study*. Retrieved from http://www.nova.edu/ssss/QR/QR3-2/tellis1.html

- Is selected case representative enough?
- Could general findings be results from one case?
- Confirmed statements, hypothesis is vulnerable;
- Will enough data be collected?
- Hard to perform comparative analysis.

However, some scientists suggest that there are five reasons which support single case studies (Yin, 2009):

1. Single case is critical to research specific item;
2. Research item is either unique and there is no other similar case, or very typical and there is no reason to explore two more identical cases;
3. Case was never revealed before and was not in scope of any research;
4. Involves repetitive observations or examination;
5. Comparing same one item at different time spams.

Researchers can use single case or multiple case research depending on question, hypothesis which is raised in research. Selection depends on individual researcher, but in case, event or item is limited to single occurrence, single case should be applied. On the other hand, researches are not limited to use one or another research method, there is always a possibility to triangulate methods (Zainal, 2007).

After addressing concerns and deciding between single or multiple case research should be made, another important aspect i.e. category of case study is to be determined. Three categories are determined by authors (Yin, 2009):

1. Exploratory – cases study in this category is determine to explore phenomenon in the data set, which is selected by researcher as a foundation for his researcher. Exploratory case studies are started with general questions which lead to open further examination on the phenomenon identified in data. In this type of case studies small scale data collection could be performed prior to proposing a question or hypothesis for research. Together with data collection phase, a pilot phase could be done in order to set plan for further investigation
2. Descriptive – name of the category itself explains the purpose, which is to describe natural phenomena which occur in the data related with raised question or hypothesis. General question usually starts with “what?” question word and leads to the aim of describing data. Narrative (story telling) form could be used in this category, such as journalistic description of event or subject of research. Descriptive case studies face challenge that it begins with describing theory to support the phenomenon or event which is in center of research. In case describing theoretical part is not successful, it might happen that case study itself will lack of preciseness which will cause not conducting full and correct research.

3. Explanatory – the main purposes of this category is to make both deep and surface data analysis in order to explain phenomena in the data. Question in this category is formulated as why question and allows researcher to form a theory which has to be tested later on according to available data. This category of case study also is used in situations where pattern matching is required, it allows to analyze phenomena in complex and multi-approach cases. Complex cases can be explained by selecting knowledge driven, problem solving or social interaction theories. Knowledge driven theory is based on assumption, that research product is result of ideas and findings from basic research. In problem solving theory - product of research is result of external source and not from basic research. Social interaction theory is based on fact that communication and knowledge sharing results in product of certain research.

Based on literature analysis and necessity to perform comparison analysis of other countries with Lithuania, case study suits to determine if new model creation and adoption could be based on existing models. Several different categories of case study were identified by authors, as to use only one category or theory limits possibility of research, combination of exploratory and explanatory case studies with knowledge driven theory, allows to perform research in acceptable form.

5. BIOMETRICS BASED PAYMENT CONFIRMATION MODEL IN CONSUMER TO BUSINESS MOBILE PAYMENTS IN LITHUANIA

The purpose of this research is to create biometrics-based mobile payment confirmation process model which could be adopted in Lithuania. In order to serve this purpose, it is necessary to break down initial purpose into two parts. Firstly, to perform comparative analysis of the countries in order to determine whether the specifics in digital payments matter when deciding if new payment confirmation model should be introduced. Secondly, to select and analyze the existing biometrics based payment confirmation model in one of the compared countries with the aim to determine if best practice could be adopted in creating a new model.

The context of comparative analysis performed on Lithuania and other countries leads to compare Lithuania with the other two Baltic countries. There are several reasons behind comparing Latvia, Estonia and Lithuania. In historical perspective the mentioned countries share very similar pattern, starting form the end of Soviet occupation and finishing with joining the European Union. The main economic indicators also demonstrate similarities among the countries. In order to better understand and compare the selected countries in terms of mobile payments along with the main economic metrics a comparison of behavior in information technology environment is essential. Figure 9 illustrates part of activities of citizens in Lithuania, Latvia, and Estonia utilizing information technology infrastructure. It is visible from Figure 9, that in part of the cases the three Baltic countries have very similar consumer behavior, with only Estonia demonstrating higher numbers in specific field. Percentage of individuals who used internet connectivity to finalize a purchase is very similar in all the countries and stand in the range from 10% to 13%. This indicates similar consumer behavior in terms of what part of citizens are willing to buy something online. Estonia is leading in terms of the number of consumers who used mobile device (or smart phone) to access internet. Lithuania and Latvia have similar figures in this graph, while Estonia has around 17% higher figure of the individuals who used a mobile device to access the internet. This is mostly driven by one main reason – according to Eurostat data[43], mobile penetration in Estonia is two times higher compared with Lithuania and Latvia. The fact that the individuals use internet not only for buying something online indicates that almost the same percentage of individuals in all three countries used internet connection to make a phone call. All three Baltic countries demonstrate solid results in the number of individuals using internet. In fact, last year not less than 70% of citizens of the mentioned countries used internet. This segment is also dominated by Estonia with almost 9 out of 10 people using internet last year. Analyzed numbers shows that individuals in all the countries are actively using internet for different

[43] Eurostat database. *Mobile broadband - subscriptions and penetration*. Retrieved from http://appsso.eurostat.ec.europa.eu/nui/show.do?dataset=isoc_tc_mbsupe&lang=en

purposes and some part of analyzed cases use it at the same level within all three Baltic countries. Similarly to individual citizens, legal entities use internet in Lithuania, Latvia, and Estonia to attract consumers. Companies which receive at least 1% of its turnover from online selling, in all countries represent not less than 10% of enterprises.

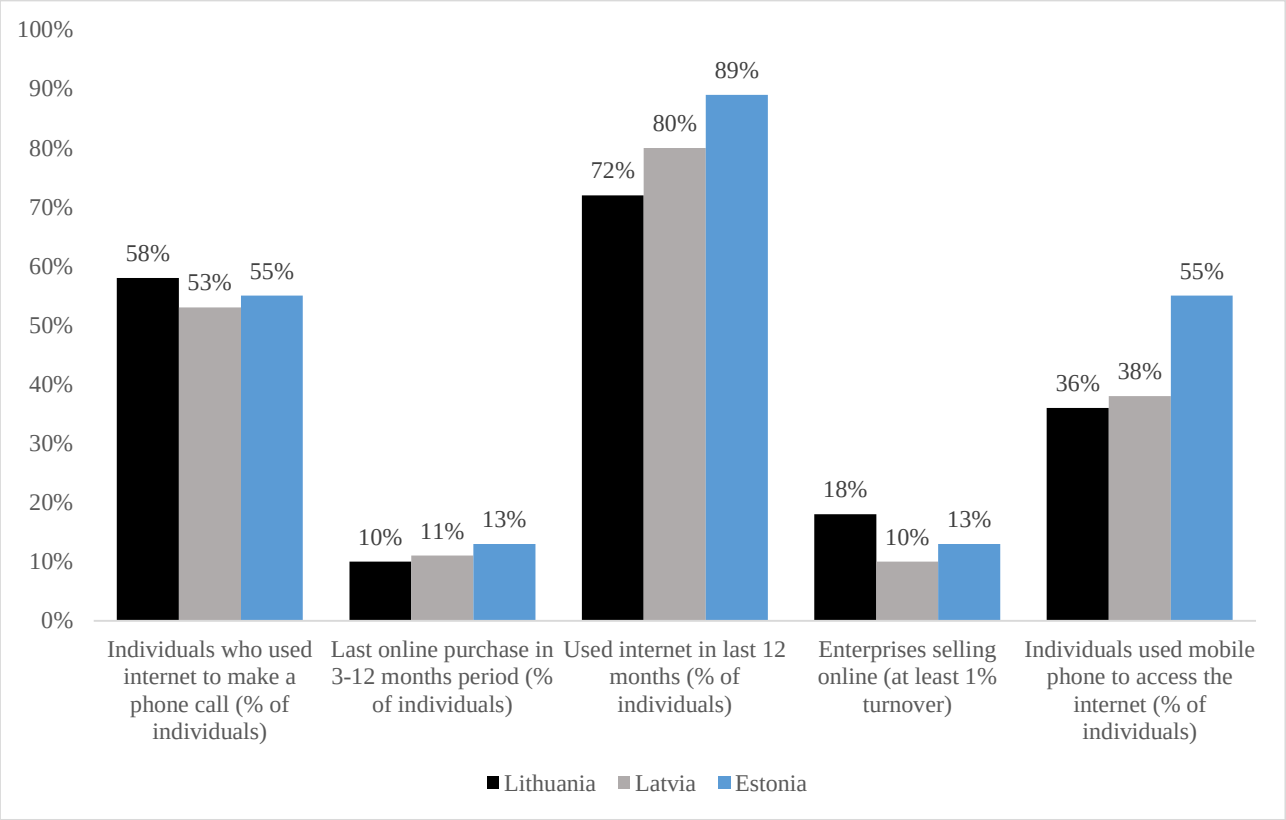

Figure 9. Consumer behavior in information technology environment. Source (Eurostat 2015)

Data analysis showed that individuals in three Baltic countries have similar habits in online purchase and making phone calls over the internet. Meanwhile Estonia stands outs in the number of individuals who use mobile phone as a mean of accessing internet. This metric, compared with Lithuania and Latvia, leads to hypothesis, that higher percentage of individuals, who use mobile device to access internet tend to results in higher usage of mobile payments as a payment option.

The data from Eurostat databases, indicates that Estonian consumers use mobile devices more frequent to access internet. Further data analysis is dedicated to indicate if higher percentage of individuals using mobile phone to access internet results in better usage of mobile payments. This will be analyzed from three perspectives – mobile payment value in the country, growth of value of mobile payments and benchmark of mobile payment in total digital payments.

Mobile payment value indicates that higher usage of mobile devices to access internet influences higher mobile payments value in country. Linking data in Figure 9 with data in Figure 10, it is noticeable that Lithuania and Latvia share almost the same percentage of individuals who use mobile devices to access internet (36% and 38%) and in four years' perspective, till 2020, it indicates

same value of mobile payments. In 2020 both countries make up 59 million USD value each. Different figure is demonstrated by Estonia. Figure 10 indicates, that 17% higher number of users using mobile device to access internet will bring 210 million USD mobile payment value to Estonia in 2020. Forecast shows around 3.5 times higher value of mobile payments on a yearly basis compared to Lithuania and Latvia. The numbers indicate, that there is correlation between habits to use mobile device to access internet and mobile payment value. The higher the percentage, the higher the value is generated in mobile payments. Looking from mobile payments value perspective, Estonia should be considered as an example to be followed in order to improve situation in value generated by mobile payments.

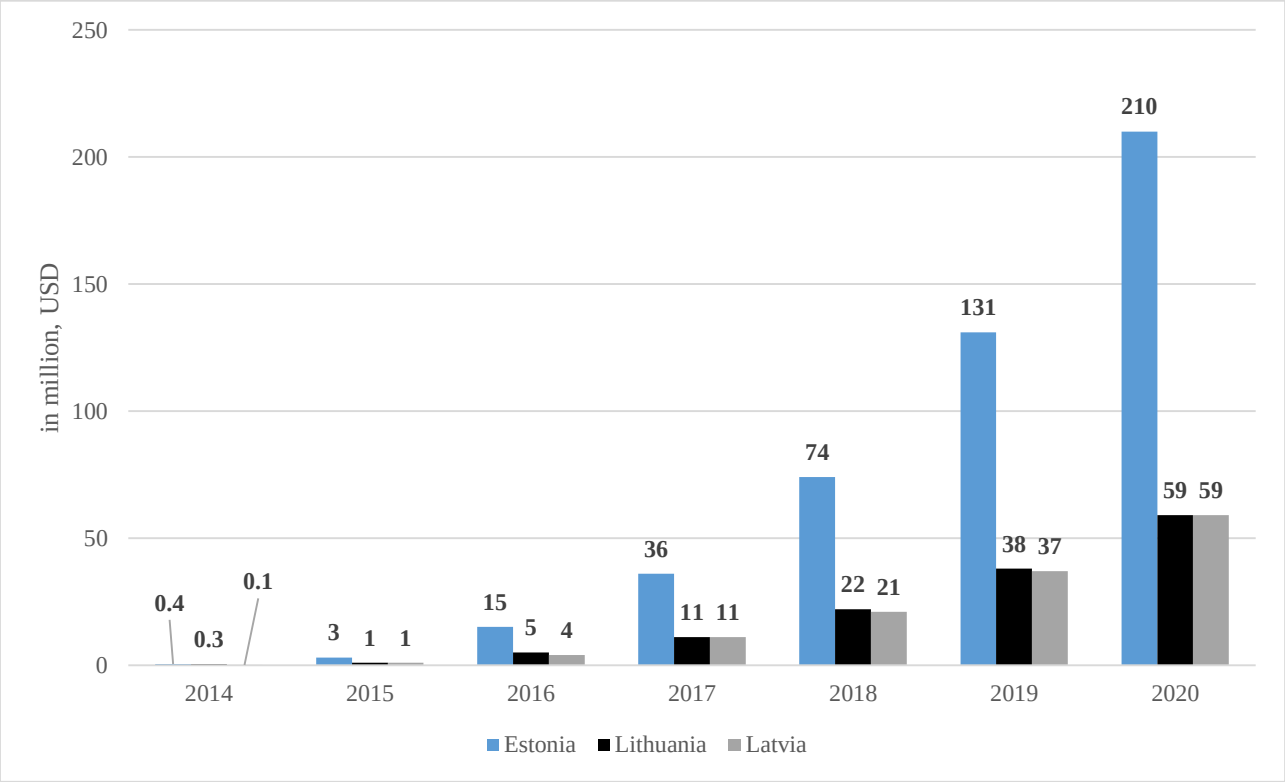

Figure 10. Transaction value in mobile payments segment in Baltic countries. Source (Statista, 2016)

Second aspect to be considered is mobile payments value growth ratio. Differences of mobile payment value in currency might be caused by several main aspects. First, the number of mobile payments users. Second, value of one mobile payment transaction. Possible scenario is that in one country consumers tend to use mobile payments to make low value transactions while in the other country, habits are to send high value transactions. Table 2 provides real reason behind higher mobile payments values in Estonia. Consumers in Estonia tend to send about 4 times higher amounts using mobile payments than Lithuanians and 2.5 times higher than Latvians. Second aspect is mobile payment users, Table 2 shows that, it is projected that in 2020 Lithuania will have the biggest number of mobile payment users, but calculations of mobile payments users per 1000 inhabitants show that Estonia will lead among the three Baltic countries.

Table 3. Metrics of mobile payments, Baltic countries 2020

	Lithuania	Estonia	Latvia
Average value of mobile payment, in USD	72	281	112
Mobile payments users	200 000	100 000	100 000
Mobile payments users for 1000 inhabitants	71	77	53

Source. Statista (2016)

Following the second point in the comparison of the countries, Figure 11 illustrates growth rate of mobile payment value in the Baltic countries in the perspective of upcoming 4 years. Looking from the value perspective in Figure 10, Estonia will have the highest value in 2020. Different situation is visible in Figure 11, which demonstrates growth rate of mobile payment value. From this aspect Estonia and Latvia demonstrate the same growth ratio for the period of year 2015-2017. It is forecasted that starting from 2018 all Baltic countries will demonstrate the same growth rate in mobile payment value. Throughout all 4-year period growth rate of mobile payments value in all Baltic countries will not be lower than 50%, which shows potential in business growth for companies operating in this field. On the other hand, the value from which growth is started to calculate was low. All Baltic countries in 2014 did not reach value of mobile payments higher than 0.5 million USD.

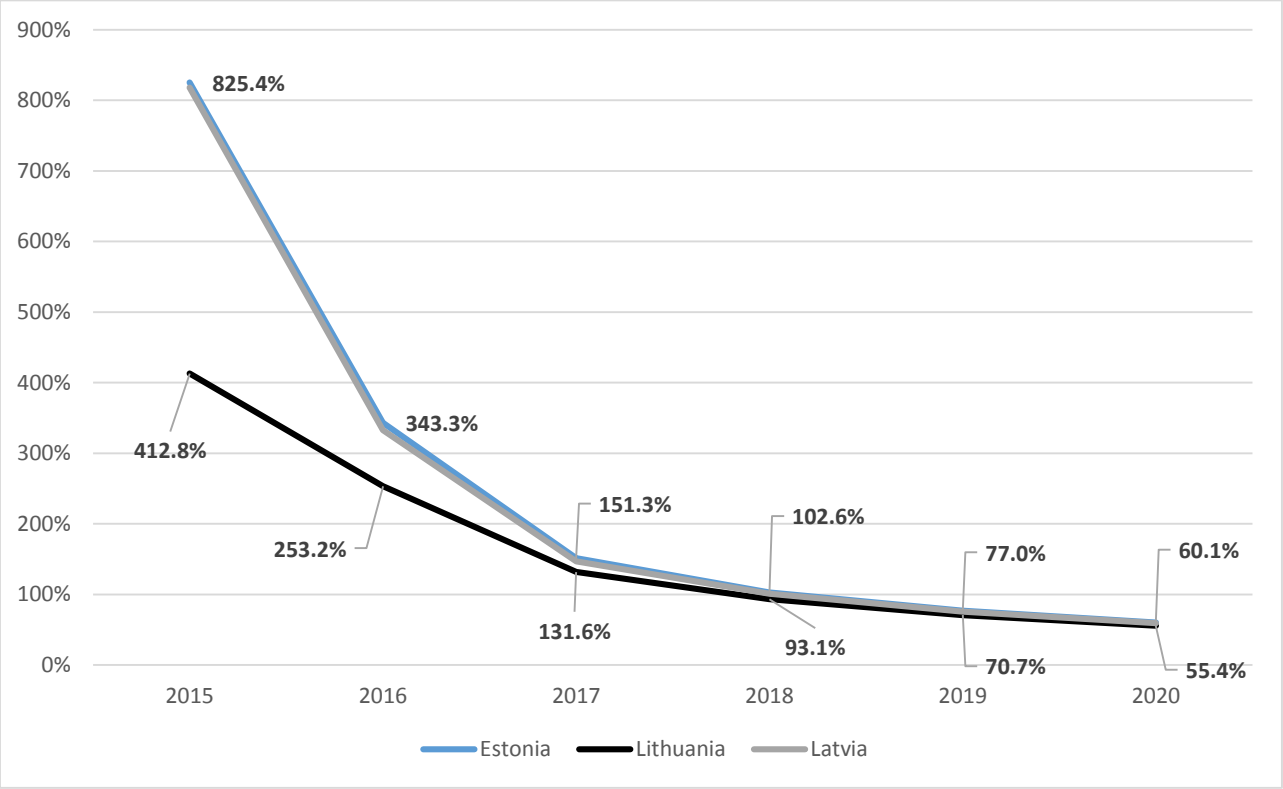

Figure 11. Mobile payments value growth in Baltic countries. Source (Statista, 2016)

Growth rate analysis showed that starting from 2017 all three countries are forecasted to demonstrate very similar growth rate in upcoming future. It is difficult to determine which country

will have a better potential in mobile payments in 2020, because difference in growth rate is low and in last forecasted year will not be higher than 5%. Third aspect of the comparison of the countries is benchmark of mobile payments in context of all digitals payments. Figure 12 indicates that in Estonia, in 2020, more than 2% of digital payments will be mobile. Compared with Lithuania and Latvia the number is two times higher. Numbers from Figure 12 could be interpreted also as cannibalization ratio within digital payments – this indicates that consumers in Estonia, will be willing to change traditional digital payments into mobile payments more often than in Lithuania and Latvia. This condition also explains why value of mobile payments in Estonia is forecasted to be highest among all three Baltic countries – consumers will change their behavior and will move value which is usually sent via traditional digital channel to mobile payments more often. In benchmark of mobile payments ratio, Lithuania and Latvia demonstrate the same ratio for all forecasted period, which falls into tendency demonstrated by these two countries in all three metrics which were compared. In the mentioned context Estonia demonstrated higher value results, which could be considered as an example when trying to implement new mobile payment model in Lithuania.

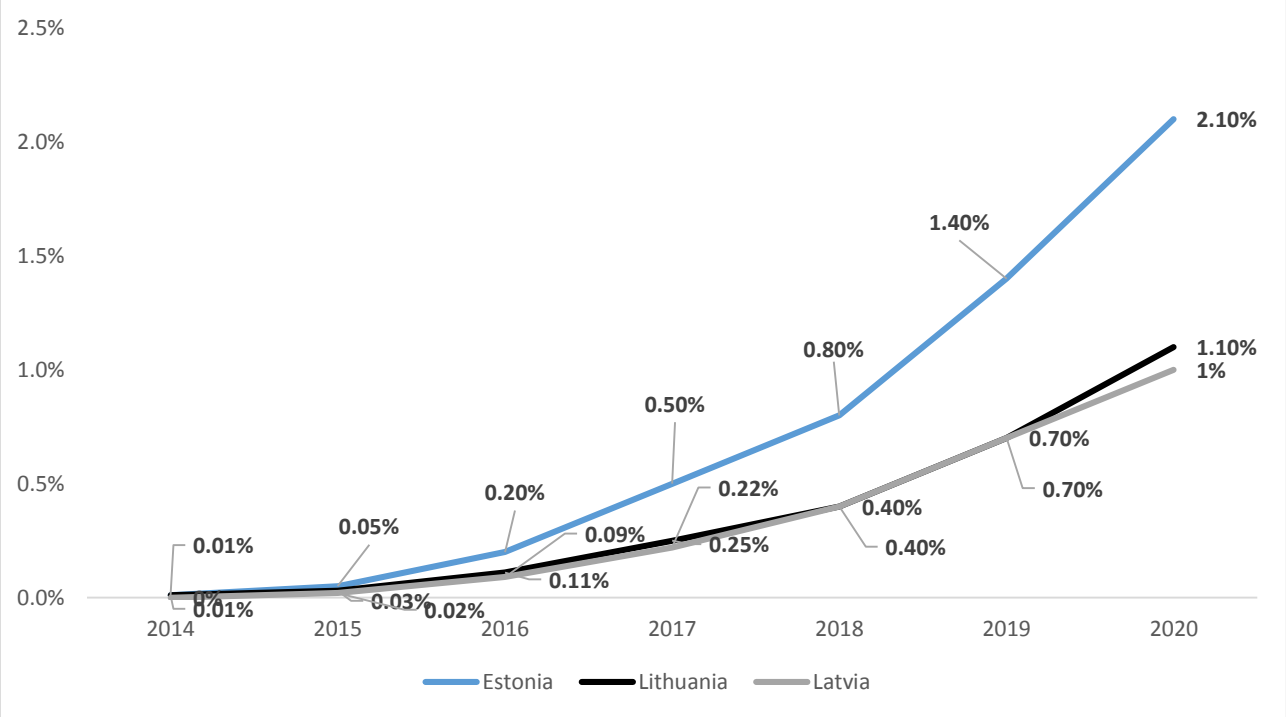

Figure 12. Benchmark of mobile payments in Baltic countries. Source (Statista, 2016)

Performed country comparison demonstrated the following results:

- Consumers in all three Baltic countries, demonstrate same tendency of making purchase and making phone calls using internet;
- Consumers in Estonia tend to use mobile device more frequently to access internet compared to the other two countries. This correlates with higher mobile payment value and mobile payment benchmark in context of digital payments;

- Mobile payment value growth ratio from 2017 is very similar in the compared countries, demonstrating less than 5% difference in the perspective of the year 2020;
- Lithuania and Latvia share more common tendencies in the analyzed digital payment related numbers, which in fact is more linked to the first part of research question. Nevertheless, Estonia could be considered as an exemplary country for implementing similar environment and models, due to:
    - Potential to increase mobile payments value in Lithuania up to level of Estonia;
    - Shape consumer behavior to use mobile devices more often to access internet which is directly linked with higher usage of mobile payments;
    - Create better diversity in all digital payments segment.

Second part of research question leads to necessity to identify existing biometrics-based mobile payment confirmation companies and models, in the selected countries in comparative analysis. In order to identify such companies, keyword research on the internet search engine was performed. Combinations of following keywords were used in search engine:

- Mobile payments;
- Payment confirmation;
- Biometrics;
- Country name.

Research on keywords for Latvia did not returned any results related to the company which provides biometrics-based payment confirmation services. Related findings were linked with government institutions which are responsible for biometrics implementation and usage in identity document field.

Keyword research for Estonia when using combination of “biometric payments Estonia”, returned the name of the company which introduced biometrics based payment confirmation to its customers. Also, same as in research for Latvia, keywords research showed that in all Baltic countries biometric features are mainly used by governmental institutions, such as police, border control, identity document regulators and issuers. Findings after keywords research identified that in Estonia the company “AS Pocopay” was the first, and currently the only one, which introduced biometrics based payment confirmation in Estonia.

Comparative analysis showed, that Latvia is a better match in terms of similarities in features related to mobile payments. Despite this, Latvia does not have model which could be explored and analyzed as an example. There is biometrics-based payment confirmation in Estonia however statistics indicate, that Estonia demonstrates better results in metrics, which allow Estonia to be

considered as an example. Furthermore, "AS Pocopay" company provides the same services in Spain, Finland and Netherlands. Table 4 demonstrates, that in 2020, none of the countries, where "AS Pocopay" provides similar service share the same values of main, mobile payments metrics. Numbers in Table 4, deny research question, if statistical specifics in digital payments matter, when deciding if new payment confirmation model should be introduced in a particular country. Following the mentioned statement the country's specifics in digital payments are not that relevant, when selecting biometrics based payment confirmation model as an example for analysis. Furthermore, under the service license of "AS Pocopay", company is eligible to execute payment transactions, including transfers of funds on a payment account with the user payment service provider or with another payment service provider in Lithuania. In such case Estonian company "AS Pocopay" is suitable to be selected as an object for case study, leaving country specifics of Estonia aside, as a role model for future growth of Lithuania.

Table 4. Main mobile payments statistic in 2020

	Value of mobile payments, in million, USD	**Mobile payments value growth, %**	**Benchmark of mobile payments, %**	**Number of mobile payments users**	**Average value of mobile payment, in USD**
Estonia	210	60%	2.10%	100 000	1500
Spain	1,929	44%	1.20%	2 900 000	154
Finland	1,774	52%	2.80%	800 000	500
Netherlands	5,082	48%	3.60%	3 200 000	387

Source. Statista, (2016)

5.1. Case study on "AS Pocopay"

Analysis of terms and conditions provided by "AS Pocopay" identifies that company is registered with the Commercial Registry of the Republic of Estonia and has its headquarter in Estonia, Tallinn[44]. "AS Pocopay" is a payment institution. Company's license is accessible on the Estonian Financial Supervision Authority's (EFSA) website. *Under the activities license, "AS Pocopay" may provide payment services in all Member States of the European Union and the European Economic Area pursuant to separate notifications to the competent authorities in the relevant Member States* ("AS Pocopay")[44].

AS Pocopay's main services allowed under the activity license are the following:

[44] "AS Pocopay" terms and conditions (2016). Retrieved from https://pocopay.com/en/terms-and-conditions/

- Execution of payment transactions – this service includes transfers of funds to a payment account with the customer's payment service provider or with another payment service provider;
- Issuing and/or acquiring payment instruments – "AS Pocopay" introduced its "MasterCard" debit card to customers;
- Assuring of services which allows cash withdrawals from a payment account as well as all the payment account operating procedures.

Company provides its services not only inside Estonia, but also cross border services. Services under the same service license are provided in Spain, Netherlands, Finland, and Belgium[45]. Table 5, provides information about countries where services of "AS Pocopay" are provided, with certain limitations, and customers can use services if they travel or are located in one of listed countries.

Table 5. Country list where "AS Pocopay" services are provided

Name of service	Service provided in country
Services enabling cash withdrawals from a payment account as well as all the operations required for operating a payment account	Czech Republic, Slovakia, Latvia, Lithuania, United Kingdom, Sweden, Germany, Romania, Malta, Cyprus, France, Greece, Italy, Ireland, Portugal, Slovenia, Denmark, Hungary, Croatia, Bulgaria, Austria and Poland
Execution of payment transactions, including transfers of funds on a payment account with the user's payment service provider or with another payment service provider	Czech Republic, Slovakia, Latvia, Lithuania, United Kingdom, Sweden, Germany, Romania, Malta, Cyprus, France, Greece, Italy, Ireland, Portugal, Slovenia, Denmark, Hungary, Croatia, Bulgaria, Austria and Poland
Issuing and/or acquiring of payment instruments	Czech Republic, Slovakia, Latvia, Lithuania, United Kingdom, Sweden, Germany, Romania, Malta, Cyprus, France, Greece, Italy, Ireland, Portugal, Slovenia, Denmark, Hungary, Croatia, Bulgaria, Austria and Poland

Source. FINANTSINSPEKTSIOON (2016)

In order to better understand biometrics based payment confirmation model which is applied in "AS Pocopay" analysis of customer identification requirements is needed. Terms and conditions

[45] FINANTSINSPEKTSIOON (2016). Supervised Entities. Retrieved from http://www.fi.ee/index.php?id=13581&action=showentity&eid=96373

between company and the customer, lists several following conditions which have to be met in order to conduct business with “AS Pocopay”:

- In order to start using services of “AS Pocopay”, company must identify customer properly. Company provides several different methods of identification to its customers. Variation of methods depends on requirements coming from legal regulation documents of country where customer wants to conduct business with ”AS Pocopay”. Different methods include, but not limited to online identification, face-to-face identification and similar.
- “AS Pocopay” have the right to request for any data and documents from its customer or representative of customer, required for identification process.
- During identification process, if “AS Pocopay” identifies that data or documents provided by the customer missing part of required information or might be related with fraudulent activity, then company may ask customer to specify provided data and documents, or even ask to apply for identification process from the beginning.
- Terms and conditions mentions that after customer agrees with conditions mentioned in the document, customer allows “AS Pocopay” to request any document or information and in any form, which is related to customer’s identification and verification. Required information and documents could be provided by customer itself, or “AS Company” could ask for this information to be provided by any other credit institution or financial institution, which in the past enrolled customer into its verification process, or had business relation with customer. Credit and financial institutions from where “AS Pocopay” might request information about customer are limited to those institutions, which use same identification method ad “AS Pocopay”. Liability to prove identity is one of the main conditions which have to be followed by the customer. Customer, on request of “AS Pocopay” is committed to provide required information and documentation to “AS Pocopay”.
- During the time while customer is conducting business with “AS Pocopay”, company may ask for additional identification in order to verify identity of customer for security and other reasons. It is customer’s duty to provide required additional documentation or information to the company.
- For the use of the Electronic Channels and/or Payment Instrument, “AS Pocopay” verifies the Client based on the Client Credentials given by the Client (e.g. username and password; card PIN code).

Analysis of terms and conditions, which bound company and customer, shows that “AS Pocopay” applies different methods of customer identification and have full control in decision making, if additional proof of identity is needed. Identification in digital channels are based on

username and password. This condition was updated with usage of biometrics – fingerprint on 6th of October, 2016.

"AS Pocopay" – first financial institution in Estonia which introduced biometric method in payment confirmation process. All "AS Pocopay" customers can access their bank accounts and confirm transactions with fingerprints. Based on publicly available information, main factors, which led company to introducing new method of payment confirmation were:

- Biometric solutions are in trend among worldwide financial institutions in order to be innovative and offer as many solutions as possible to its target audience, company selected biometrics;
- Security and convenience to the customer is priority in modern banking sector, as company is always looking for new opportunities, biometrics was one of it;
- Fingerprint confirmation is much more convenient and safer alternative to consumer as they no longer have to memorize all different codes and passwords.

"AS Pocopay" created a process where all payments have to be submitted using smart phone and application of the company. Fingerprint confirmation is activated via mobile application and its settings, for this reason customers have to make sure that the latest version of application is available in used device. There are five things to be mentioned when talking about "AS Pocopay" payment confirmation process:

1. There is an option allowing to choose between Poco code and Fingerprint confirmation for accessing account and confirming money transfers;
2. Poco code is a 4-digit number which is created by the customer at the first registration and account opening. This code also serves as payment confirmation option in original payment confirmation model;
3. In fingerprint confirmation option important thing is that, fingerprint stored in a smart phone is used to confirm the payment, so in cases several fingerprints are registered on the phone, payment could be confirmed by any of it;
4. Fingerprint authorization have the same value as Poco code authorization – this aspect puts liability on customer to make sure, that only his fingerprints are stored in a smart phone;
5. "AS Pocopay" does not store customer fingerprint data in any mean.

Figure 13 demonstrates process flow for customers of "AS Pocopay" company. Process itself starts only after customer downloads mobile application, in other case customer will not be able to use services. Mobile application is supported only by Android and iOS operating systems. After a successful download of application, customer can start registration with submitting all required

information. In situations, when customer does not want to provide required information, process ends as according to terms and conditions, company must verify its customer properly. Provided information is checked by the systems and in case no additional information or documentation is required, customer receives unique 4-digits Poco code, which serves as a tool to authorize payments. After registration and identification steps are done, customer can start to transact and initiate mobile payment. After submitting all required information about the recipient in a new model consumer can choose to authorize payment by using fingerprint. At the same step, authorization using Poco code is also available. Fingerprint authorization only could be applied if there are fingerprint data stored in smartphone, so in situations when smartphone does not support this function, or customer did not store his fingerprint data in the smartphone the only option left is to authorize payment using Poco code. On the other hand, if fingerprint data is available and matches with currently used fingerprint – payment is authorized and done successfully. In model used by "AS Pocopay" biometrical data has to be stored in smartphone device as company does not collect such data as a proof of identity, but accepts it as such.

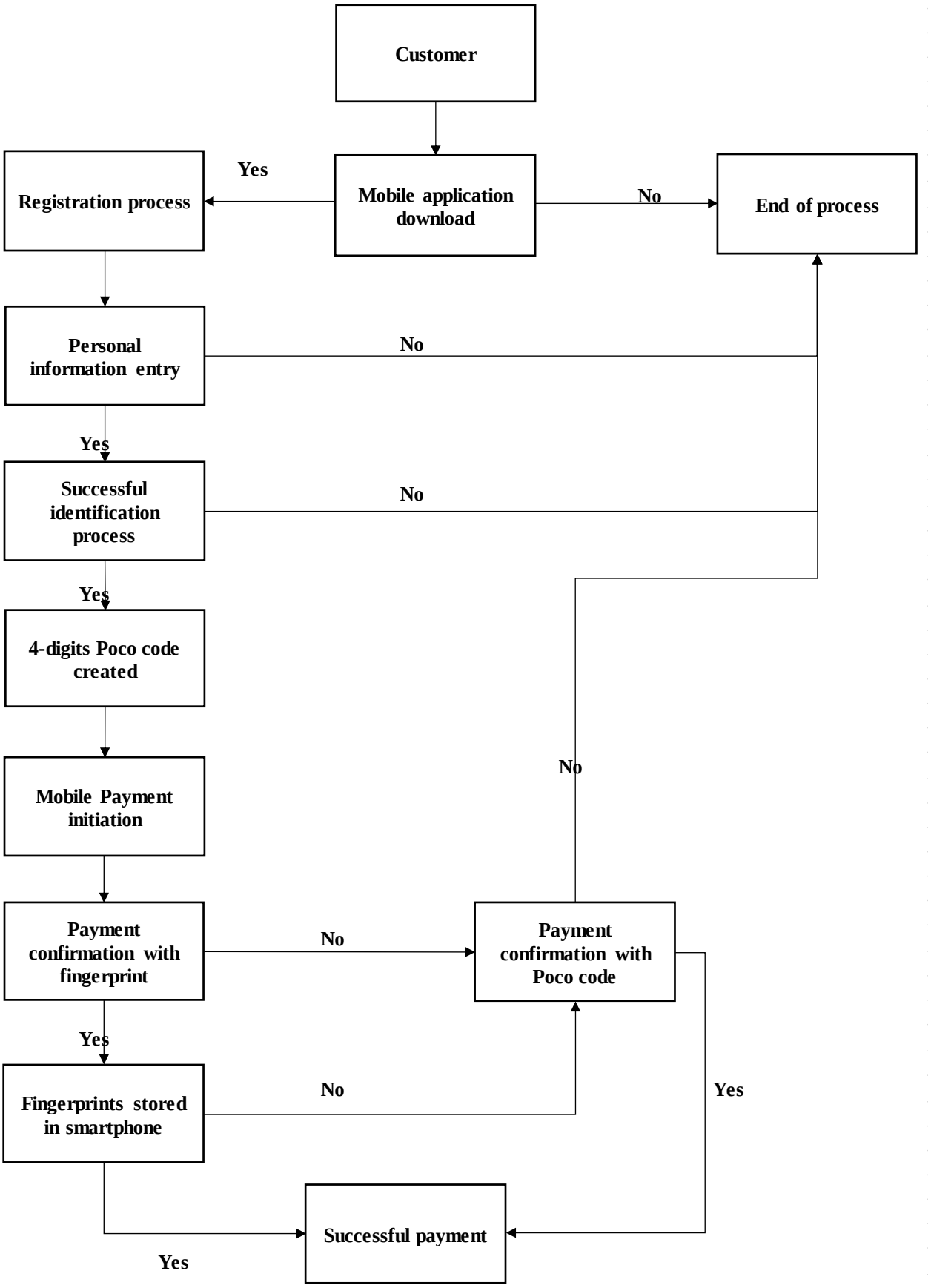

Figure 13. "AS Pocopay" payment confirmation flow

Figure 13 illustrated full process flow of mobile payment for "AS Pocopay" customer. To understand better how fingerprint authorizations happens, part of the process in Figure 13 should be broken down into sub processes, which indicates how authorization takes place. As full process flow was already described only steps of sub process now need to be explained. In situations when consumer decides to authorize payment with fingerprint, he/she receives notification to use finger to authorize the payment. When the action is performed, application checks with consumer's smartphone if current fingerprint is stored in smartphone database, as identifier of one or another user of smartphone. If match check is positive, then system message to "AS Pocopay" systems is sent with confirmation, that currently used fingerprint matched one of fingerprints stored in smartphone, and payment is authorized.

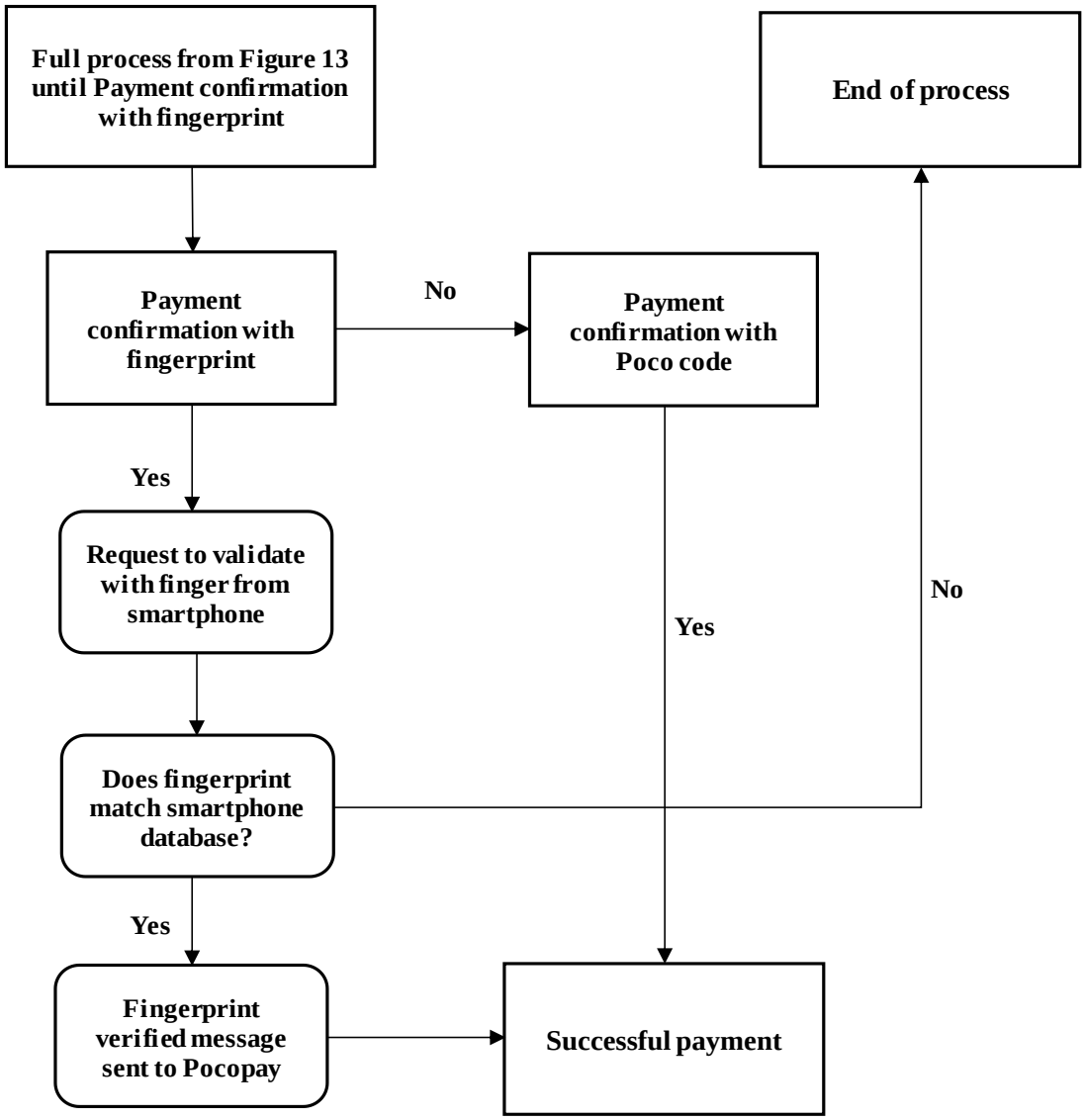

Figure 14. "AS Pocopay" fingerprint authorization sub process

Fingerprint authorization model by "AS Pocopay" involves one main risk, in case of occurrence of which certain consequences emerge. This risk is related to the fact that "AS Pocopay" does not store data of fingerprint, in process model, fingerprint data is stored in a smartphone and not in "AS Pocopay" mobile application. Identified risk may occur in following scenarios:

- Several different users have their fingerprint stored in one smartphone – this situation might cause fraudulent activity. Only one "AS Pocopay" account is linked to unique consumer, but device could be used and payment could be authorized by several users. In this case it might happen so that a genuine financial account holder, will not be aware of somebody else using his account;
- Security measures depend on the settings of a smartphone and not the settings of a service provider systems – smartphones settings have its own parameters, which indicates if the identification of fingerprint was successful or not, depending on the company, which produced smartphone, false positive ratio could be different – it could be so that one device requires currently used fingerprint to be exactly the same as first time used, while other might accept 80%, or any other, match. This false positive ratio does not depend on the payment service provider, in this case "AS Pocopay";
- A more complicated fraud management – if consumer did not initiate payment and was not aware of one taking place, he/she could apply for a refund. Company will perform investigation and will decide if there were all security measure taken by customer in order to prevent this from happening. In fingerprint based confirmation models, this issue should be solved, as fingerprint is unique metric and is very hard to be compromised, so if payment was approved by fingerprint, customer must be aware of the payment. But risk identified above, indicates that this is not always true. If one smartphone have several users who have their fingerprints registered on the smartphone, or false positive of smartphone device is set to accept low match results, fraudulent activity might happen without genuine customer knowing about it.

The purpose of research is to create biometrics-based payment confirmation model, which could be adopted to Lithuanian C2B mobile payments. Model used by "AS Pocopay" does not have any technical or implementation characteristics, which would not allow to replicate analyzed model in Lithuanian market. Identified risk shows that improvement of analyzed model is needed in order to have better security and customer experience.

Analysis of "AS Pocopay" model shows that the mentioned risks and consequences could be managed. Solution is to store fingerprint data at service provider database, and not trust fingerprints stored on a smartphone. This eliminates the mentioned risk:

- Even if smartphone device has several users with stored fingerprint data, if fingerprint data is stored at a service provider's database, each unique customer have his unique fingerprint linked to his financial account. In this scenario, even if device is used by different people, payment could be authorized only by the person who has the same fingerprint as it is stored in the database of service provider;
- Security measures will depend on the service provider – storing data in service provider database, dependency on false positive settings of smartphone is eliminated. In this scenario, service provide fully controls what false positive rate should be met in order for the payment to be authorized. This also gives beneficial advantages to service provider as company can control risk level – if high fraudulent activity is noticed, service provider could increase false positive to full match and vise a versa in low fraud periods.

To address the mentioned risks biometrics-based payment confirmation model, demonstrated in Figure 15, could be used in Lithuania. In the suggested model, framework of "AS Pocopay" model was used. Blue squares indicate improved process in payment confirmation model. As illustrated in Figure 15, customer's journey starts with mobile application download. After download a customer is transferred into registration process, which as in the previously analyzed model, requires to enter personal information. In case personal information is successfully verified at the back end of application, in Figure 15 model, the customer is requested for fingerprint data to be captured. After capturing necessary data, user profile (with required user name and password) is created. In case customer does not feel comfortable with providing biometrical data, he/she could always choose to participate in password based payment confirmation process flow. This type of possibility, to use dual type confirmation model, is beneficial for both consumer and company. Consumer does not have to provide data which he/she does not want to provide and the company can still provide services to consumer. In situation where customer registered his fingerprint, he initiates the payment and enters all required information about the receiver. Customer is referred to authorizing payment with fingerprint. In these newly added steps the system checks if currently used fingerprint is the fingerprint which is stored in the service provider's database and whether it links with the account from which payment is initiated. If all required conditions are met, payment is authorized successfully and is processed by the system. In other scenario, when fingerprint does not match requirements, money transfer is declined. Comparison of Figure 13 and Figure 15 shows that in a newly suggested model, fingerprint data takes place in two places instead of one as is in Figure 13. Firstly, fingerprint is captured in customer registration phase and after the fingerprint data is compared with the stored data linked to customer's profile to authorize the payment. This model allows to minimize risk listed after analysis of Figure 13 – "AS Pocopay" fingerprint based payment confirmation model.

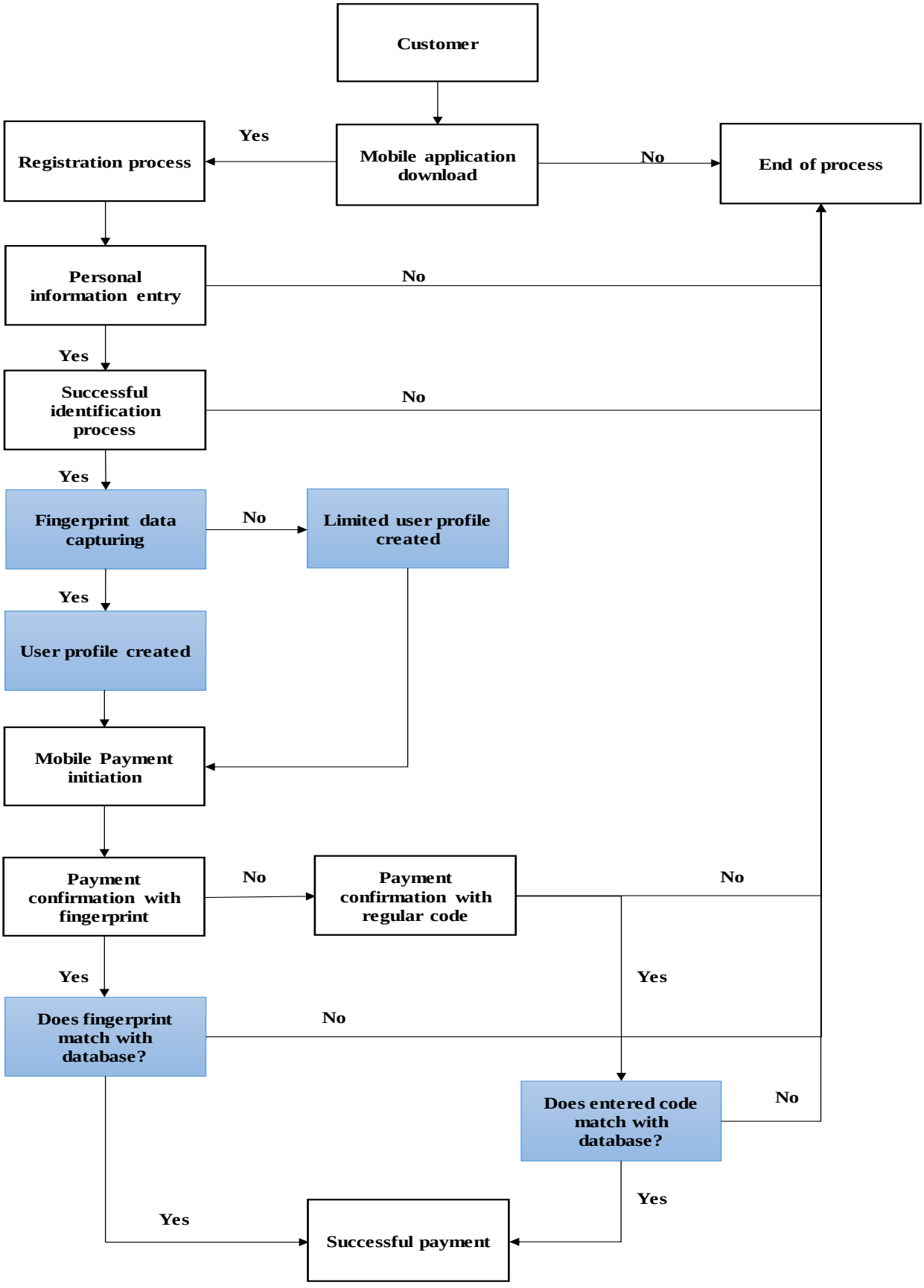

Figure 15. Biometrics based mobile payment confirmation model adopted to Lithuania

In order to better understand differences between the existing and updated models, fingerprint phases of Figure 15, should be divided into smaller sub processes. Figure 16 illustrates the breakdown of Figure 15 new processes. Firstly, when fingerprint data capturing takes place, a customer is requested to place his finger on a scanner in his/her smartphone. Fingerprint data is captured, translated into code which is acceptable to service provider database system and linked to customer's profile. This way unique fingerprint is linked to unique profile as additional security measure. Second time when fingerprint data is requested from the same customer – payment authorization phase. In this phase, the customer after placing all necessary receiver information, is asked to place his/her finger on a scanner to authorize the payment. While this is processed, currently captured fingerprint data is sent to service provider database and is compared with coded fingerprint data linked to customer's profile. If current data match the one in database – payment is authorized and successfully processed. In other scenario, payment is declined.

A newly adopted model addresses risks identified in the model used by "AS Pocopay", in model illustrated in Figure 15 and 16, risk of multiple users of smartphone is managed by shifting fingerprint data storage to the service provider's database. Table 6 addresses main advantages and two new additional steps which would be required in order to implement a newly proposed model.

Table 6. Advantages and disadvantages of new model

Advantages	**Disadvantages**
Eliminates risk of multiple smartphone users – even if smartphone is used by several users, payment only could be authorized by unique payment account owner	Additional investments required for service provider to create, manage and maintain additional database for fingerprint data storing
Ability to control security measures by service provider – false positive of fingerprint match is set by service provider and not by smartphone settings	Depending on the country, additional requirement for storing personal data might be addressed to service provider, due to storage of fingerprint data
In case of fraudulent activity better management of risk as fingerprint is associated with unique account and security measures controlled by service provider	
Leaves flexibility for customer to use traditional authorization methods	
Gives flexibility to service provider to control the risk by false positive settings	

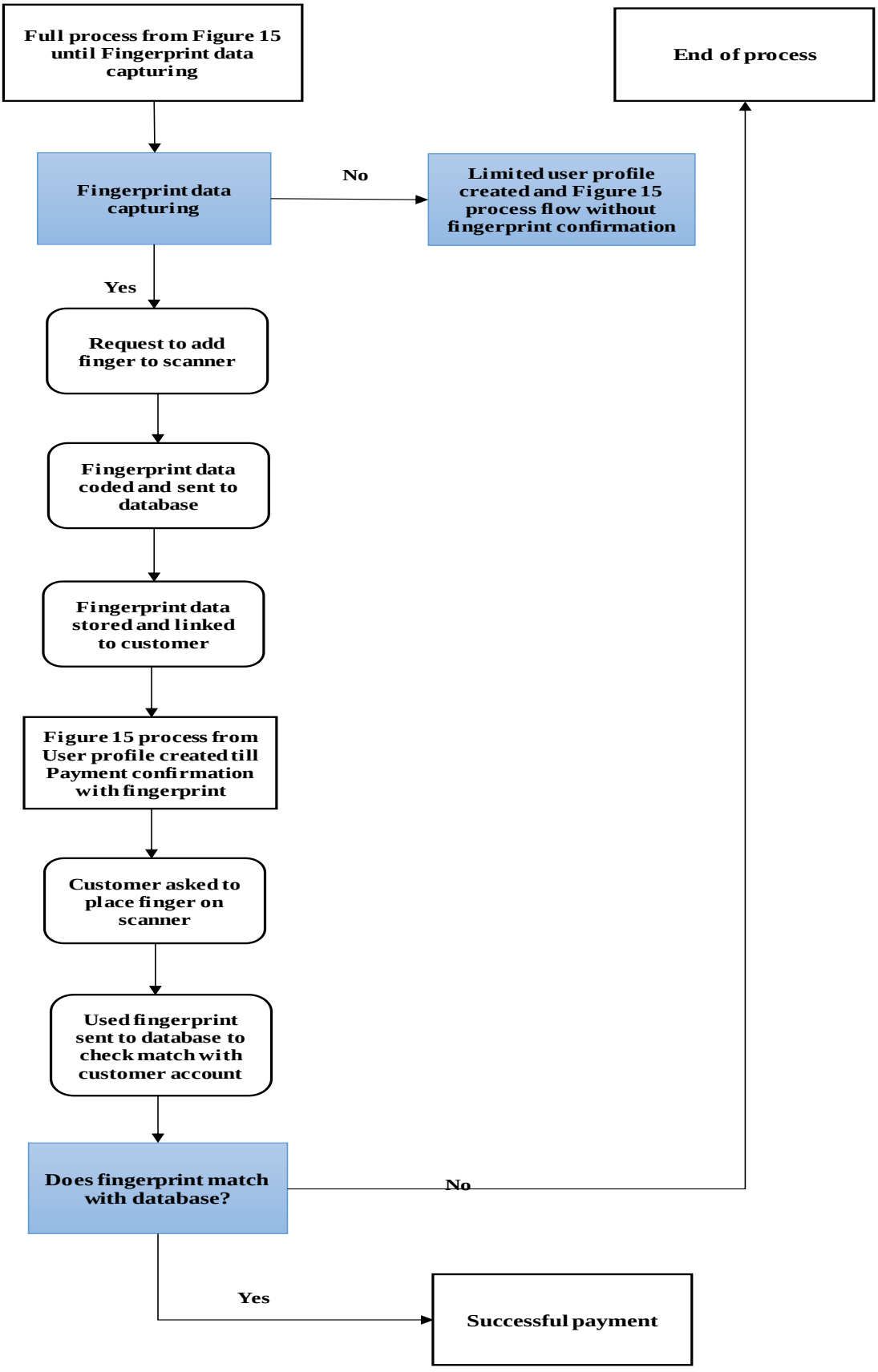

Figure 16. New model fingerprint authorization sub process

Biometrics based payment confirmation model, illustrated in Figure 16, covers risk identified after analysis of "AS Pocopay" model. A newly suggested model involves multiple layers of user authentication and different way of storing fingerprint data. Technical, process model implementation does not have unique requirements. Exploring practical implementation of fingerprint based payment confirmation model in Lithuania, solution to implement fingerprint data storage at service provider's side, creates additional requirement for the company which would implement this kind of solution. According to the Republic of Lithuania Law on Legal Protection of Personal Data (Personal Data law), fingerprint fits definition of personal data. Personal Data law, states that *personal data shall mean any information relating to a natural person (data subject) who is known or who can be identified directly or indirectly by reference to such data as a personal identification number or one or more factors specific to his physical, physiological, mental, economic, cultural or social identity.* Following explanation of Personal Data law, capturing and storing fingerprint data is action of processing personal data. For this purpose, in accordance to Personal Data law, legal entity, which will implement, created model in Lithuania, will be considered as data processor, which is described as "*legal or a natural person other than an employee of the data controller, processing personal data on behalf of the data controller. The data processor and/or the procedure of its/his nomination may be laid down in laws or other legal acts."* in Personal Data law. In order to serve a purpose of data processor, company should meet several different requirements, which are stated in law. One of the main requirement is to assure data protection of personal data, in this case – fingerprint data. General condition for data processor, listed in Personal Data law is that *data processor must implement appropriate organizational and technical measures intended for the protection of personal data against accidental or unlawful destruction, alteration and disclosure as well as against any other unlawful processing. These measures must ensure a level of security appropriate in respect of the nature of the personal data to be protected and the risks represented by the processing and must be defined in a written document (personal data processing regulations approved by the data controller, a contract concluded by the data controller and the data processor, etc.).* This condition, not only implies company to invest in technical and staff training measures, but also to document everything what is related with processing personal data. In case data processor is also data controller, it must be registered in the State Register of Personal Data Controllers which is administrated by the State Data Protection Inspectorate.

Comparative analysis of Baltic countries allowed to identify strengths of Estonia compared to Lithuania and Latvia. Numbers for Estonia showed that around 17% more people, compared with Lithuania and Latvia, use mobile or smart phone to access internet. Further analysis showed, that this number closely correlates with popularity of mobile payments. Forecasts and data analysis showed

that in 2020 Estonia will have the highest mobile payments value among the three Baltic countries. From 2017 percentage growth rate of mobile payments value, for all compared countries, demonstrates similar numbers. Estonians tend to send around 3 times higher mobile payment amounts and have most mobile payment users per 1000 inhabitants. These main characteristics allow Estonia to be a leader and great example for Lithuania and Latvia. All three Baltic countries only share similarities in online purchase percentage and making phone calls using internet.

Second part of the case study was supported by word analytics in search engine. Results showed that currently only in Estonia biometrics based payment confirmation model is implemented. In all three Baltic countries only "AS Pocopay" company exists as a model with biometrics based payment confirmation model. Primarily analysis of "AS Pocopay" company showed that the same services as in Estonia are provided in Netherlands, Finland, and Spain. This lead to comparative analysis of these three countries and Estonia in order to confirm or deny condition mentioned in the research question that statistical specifics in digital payments matter when deciding if new payment confirmation model should be introduced in a particular country. As there were no similarities in main metrics noticed, neither in comparing three Baltic countries nor comparing countries where "AS Pocopay" operates, research question was denied. Statistical specifics in digital payments do not play the main role when deciding to implement payment confirmation model in another country. Furthermore, under the service license of "AS Pocopay" is eligible to provide services in Lithuania, which leads to stating, that model existing in Estonia is suitable to be analyzed as an example. In such case Estonian company "AS Pocopay" is suitable to be selected as an object for case study, leaving country specifics of Estonia aside, as a role model for future growth of Lithuania.

For case study, "AS Pocopay" was chosen as an example. Model analysis identified few risks related with model which is place in Estonia. Main risk is associated with the fact that mobile payment authorization with fingerprint is based on fingerprint data stored in smartphone. Knowing that several different users could have stored their data in smartphone, this leads to situation when payment could be authorized by person who is not account holder. To implement model from "AS Pocopay" in Lithuania for C2B mobile payments, there are no roadblocks, as model is clear and simple. Just identified risks raised concerns about this model. Suggestion was to adopt the model, but make changes in process flow in order to address identified risks. To reach this result, new model was created, where fingerprint data is stored in service provider databases and is linked to unique customer. This allows to eliminate risk of payment being authorized not by account holder and also eliminates potential risks which follows after illegal authorization of payment. Also new model gives possibility for service provider to control security level by making its own settings of false positive for fingerprint matching.

Final step of case study, explored practical implementation of newly created model. Fingerprint is treated as personal data in Lithuania. New model creates possibility, for service provider, to store fingerprint data in it database. According to Personal Data Protection law in Lithuania, this action falls under data processor and controller roles, which creates additional requirements for company, which would implement suggested model. Additional technical and staff training measures required to be enrolled in order to implement suggested model. Even specific documentation and registration is necessary to be provided to Personal Data Inspectorate.

Overall, a newly suggested model is an improved form of the already existing model in Estonia. Suggested improvements bring less risk in mobile payment authorization when biometrics is utilized. Also this model creates additional requirements for company which will implement this option. Starting from additional database, for fingerprint storing, to additional technical measures for personal data protection and also becoming personal data controller which is regulated by Personal Data Inspectorate in Lithuania.

CONCLUSIONS

1. Literature analysis showed that fingerprint is identified as the most suitable biometric looking from identification and security perspective. When biometric feature serves identification purpose, it is important to determine two main phases – enrollment and recognition, as these two phases applied subsequently allow to utilize biometrics for full recognition.

   Topic of security in terms of technology and payments is well studied and addressed by both scientists and companies. Initiatives stemming from financial institutions, which are major players in payments, show focus on customer authentication and secure payment flows. Two major security problems are identified by several different authors. These problems are related to system issues triggering repetitive security breaches and impersonation, when fraudulent activity is performed in order to pretend to be a genuine customer. Biometrics is considered to be the main countermeasure ensuring that the mentions problems wouldn't occur.

   Popularity of biometrics is represented in studies and surveys performed by market players such as Visa or institutions such as European Payments Council. Studies have revealed that around 65% of banks and other financial institution are ready to implement biometrics in near future as a tool to improve security. On the other hand, 22% of these institutions already offer biometrical solution to the customers. Financial institutions are encouraged to apply biometrics by consumers as approximately 80% of them are in favor of using biometrics and think that security is the main attribute when deciding on authorizing a payment. While comparing traditional (PIN/password based) and biometrical process flows in payment authorization, it is seen that by implementing just one additional step of biometric authorization, the level of security in payment process increases. Success of biometrical authentication is based on false positive response, instead of having correct or incorrect password. This emphasizes the importance of what technology is used in the biometrical identification process.

   Taking into consideration costs, reliability, easiness to use – fingerprint solutions demonstrate solid performance and are liked amongst financial institutions and consumers.
2. Based on statistical data analysis, environment in Lithuania for mobile payments in upcoming four years indicates the potential of growth. Value sent via mobile payments per year will increase almost 12 times until 2020. Growth rate in value sent via mobile payment demonstrates double digit growth perspective. Despite such growth rates, mobile payments in 2020 will only account for 1.1% of total market share in digital payments. With the number indicating this potential, Lithuania lacks companies which could introduce biometrics into

mobile payment area. On the other hand, governmental institutions demonstrate better adoption of biometrics in their services. In 2006 the first passport with biometrical data was introduced and new technologies are implemented in other government controlled areas. Knowledge and practice of governmental institutions should be adopted by private companies so that new products and services with biometrical features could be created.

Legal environment in Lithuania, having in mind both legal framework and regulatory institutions, create positive and friendly environment for growth in mobile payments. Republic of Lithuania Payments Law does not require to become a payment institution, if a company decided to introduce biometrics-based payment authorization or customer identification mode. As long as the amount of payment is not sent to the service provider's account, there is no need to get a status of a financial institution. This fact creates favorable conditions to create a model as intermediary between consumer and service provider. Initiatives introduced by Central bank of Lithuania support new payment methods and security in them. Considering all facts, Lithuania have established a favorable environment from growth potential and legal points of view so that new payment methods could be introduced. As security is one of the priorities in Europe and Lithuania, biometrics-based solutions should also be implemented.

Analysis identified two main roadblocks for mobile payments implementation – outdated infrastructure and unwillingness of commercial banks to allow their consumers to directly connect their bank account with other financial service provider. As similar issue is identified in other European Union countries, new Payment service directive will be issued.

3. Comparative analysis of Baltic countries, allowed to identify strengths of Estonia compared to Lithuania and Latvia. Figures indicate that compared to Lithuania and Latvia Estonia has got approximately 17% more people using mobile or smart phone to access internet. Further analysis showed, that this number closely correlates with popularity of mobile payments. Forecasts and data analysis indicated that in 2020 Estonia will have the highest mobile payment value among the three Baltic countries. From 2017 percentage growth rate of mobile payments value for all compared countries demonstrates similar figures. Estonians tend to send around 3 times higher mobile payment amounts and have the highest number of mobile payment users per 1000 inhabitants. These main characteristics allow Estonia to be a leader and great example for Lithuania and Latvia. All three Baltic countries share similarities only in online purchase percentage and making phone calls using internet.

Second part of the case study was supported by word analytics in search engine. Results showed that currently only in Estonia biometrics-based payment confirmation model is implemented. Throughout all three Baltic countries, only "AS Pocopay" company serves

as a role model with biometrics-based payment confirmation model. Primary analysis of "AS Pocopay" company showed that the same services as in Estonia, are provided in Netherlands, Finland and Spain. This lead to comparative analysis of these three countries and Estonia, in order to confirm or deny the condition mentioned in the research question that statistical specifics in digital payments matter, when deciding if new payment confirmation model should be introduced in a particular country. As there were no similarities in main metrics noticed, neither in comparing three Baltic countries, nor in comparing countries where "AS Pocopay" operates, research question was denied. Statistical specifics in digital payments do not play the main role when deciding whether or not implement payment confirmation model in other country. Furthermore, under the service license of "AS Pocopay", the company is eligible to providing services in Lithuania, which leads to stating that model existing in Estonia is suitable to analyze as an example. In such case Estonian company "AS Pocopay" is suitable to be selected as an object for case study for as a role model future growth of Lithuania. Though, the peculiarities of Estonia as a country should be left on the side.

"AS Pocopay" was chosen as an example for case study. Model analysis identified few risks related to the model which is used in Estonia. The main risk is associated with the fact that mobile payment authorization with fingerprint is based on fingerprint data stored in smartphone. Knowing that several different users could have stored their data in smartphone, this leads to situation when payment could be authorized by a person who is not an account holder. To implement model from "AS Pocopay" in Lithuania for C2B mobile payments, there are no roadblocks, as the model is clear and simple. However, identified risks raised concerns about this model. Suggestion was adopting the model, but introducing some changes in process flow in order to address identified risks. To reach this result, new model was created where fingerprint data is stored in service provider databases and is linked to unique customer. This allows to eliminate risk of payment being authorized not by an account holder and also eliminates potential risks which follows after illegal authorization of payment. Furthermore, a new model gives possibility for service provider to control security level by making its own settings of false positive for fingerprint matching.

Final step of case study was to explore practical implementation of a newly created model. Fingerprint is considered as personal data in Lithuania. A new model creates possibility for service provider to store fingerprint data in its database. According to Personal Data Protection law in Lithuania, this action falls under data processor and controller roles, which creates additional requirements for the company which decides to implement the suggested model. Additional technical and staff training measures are required to be enrolled

in order to implement the suggested model. Specific documentation and registration are necessary to be provided to Personal Data Inspectorate.

Overall, newly suggested model is improved on the bases of the existing model in Estonia. Suggested improvements bring less risk in mobile payment authorization, when biometrics is utilized. However, this model creates additional requirements for company choosing to implement this option. Starting from additional database for fingerprint storing to additional technical measures for personal data protection and also turning into personal data controller which is regulated by Personal Data Inspectorate in Lithuania.

LIST OF LITERATURE

1. "AS Pocopay" terms and conditions (2016). Retrieved from https://pocopay.com/en/terms-and-conditions/
2. 360 Biometrics. (2016). Frequently asked questions. Retrieved from http://360biometrics.com/faq/biometrics.php
3. Agarwal, S., Khapra, M., Menezes, B., Uchat, N., (2014) Security issues in mobile payment systems Department of Computer Science and Engineering, IIT
4. Alimi, V., Rosenberger, C., Vernois, S., (2013), A mobile contactless point of sale enhanced by the NFC and biometric technologies Inl. J. Internet Technology and Secured Transactions, Vol. 5, No, 1
5. Bolle, R., Jain, A., Pankanti, S. (2006). Personal Identification in Network Society 978-0387-28539-9
6. Breebaart, J., Buhan, I., Groot, K., Kelkboom, E. (2011), Evaluation of a template protection approach to integrate fingerprint biometrics in a PIN-based payment infrastructure
7. Buchmann, N., Rathgeb, C., Baier, H., Busch, C., (2014), Towards electronic identification and trusted services for biometric authenticated transactions in the Single Euro Payments Area, CASED
8. Central Bank of Lithuania (2016). Best Practice Principles. Retrieved from https://www.lb.lt/gerosios_praktikos_principai
9. Central Bank of Lithuania (2016). National Payment Strategy. Retrieved from https://www.lb.lt/n27462/konsultacija_del_strategijos.pdf
10. Cybercrime statistic portal. (2015). Cybercrime statistics. Retrieved from http://www.cbs.com/shows/csi-cyber/news/1003888/these-cybercrime-statistics-will-make-you-think-twice-about-your-password-where-s-the-csi-cyber-team-when-you-need-them-/
11. Dennehy, D., Sammon, D., (2015), Trends in mobile payments research: A literature review Journal of Innovation Management 49-61
12. European consumers ready to use biometrics for securing payments, research by Visa, (2016)
13. Eurostat database. Mobile broadband - subscriptions and penetration. Retrieved from http://appsso.eurostat.ec.europa.eu/nui/show.do?dataset=isoc_tc_mbsupe&lang=en
14. FINANTSINSPEKTSIOON (2016). Supervised Entities. Retrieved from http://www.fi.ee/index.php?id=13581&action=showentity&eid=96373
15. Finextra. (2013). Danske Bank brings mobile payments to Lithuania. Retrieved from https://www.finextra.com/news/announcement.aspx?pressreleaseid=52428

16. Statista. (2016). Mobile Payments Lithuania. Retrieved from https://www.statista.com/outlook/331/143/mobile-payments/lithuania#
17. Garg, R., Garg, N., (2015) Developing a Secured Biometric Payments Model Using Tokenization, Whitepaper
18. Goode, A., (2014), Bring your own finger – how mobile is bringing biometrics to consumers, Biometric Technology today, Volume 2014, Issue 5
19. Invest Lithuania. (2015). Lithuania Europe's No. 1 in fiber-optic internet penetration. Retrieved from http://www.investlithuania.com/news/lithuania-europes-no-1-in-fibre-optic-internet-penetration/
20. Jain, A. K., Flynn, P., Ross, A. (2008). Handbook of biometrics 978-0-387-71041-9
21. Jain, A., Ross, A., Prabhakar, S., (2004) An introduction to biometric Recognition, IEEE Transactions on Circuits and Systems for Video Technology, Vol. 14, No. 1
22. Kou, W., Introduction to E-Payment: An Essential Piece of the E-Commerce Puzzle, (2003), 978-3-662-05322-5
23. Li, Y., Xu, X., (2009) Revolutionary information System Application in Biometrcis, IEEE International Conference on Networking and Digital Society
24. Mayhew, S. (2015). Lithuania to deploy MorphoTOP fingerprint scanners for visa requests. Retrieved from http://www.biometricupdate.com/201503/lithuania-to-deploy-morphotop-fingerprint-scanners-for-visa-requests
25. Mobile Payments: Risk, Security and Assurance Issues, (2011), An ISACA Emerging Technology White Paper. Retrieved from http://www.isaca.org/Groups/Professional-English/pci-compliance/GroupDocuments/MobilePaymentsWP.pdf
26. Nordlund, S. (2016), Mobile biometrics has finally come of age, European Payments Council Newsletter Issue 30
27. Personal Data Notification and Protection Act of 2015, U.S., Mar. 26, 2015, H.R.1704
28. Personalization center. (2008). Biometrics in eID cards. Retrieved from https://www.dokumentai.lt/viewpage.php?page_id=79
29. Raina, V. K., (2011) Integration of Biometric authentication procedure in customer oriented payment system in trusted mobile devices, International Journal of Information Technology Convergence and Service (IJITCS) Vol, 1, No. 6
30. Republic of Lithuania Payments Law (2016). Valstybės žinios, 1999-11-17, No. 97-2775. Retrieved from https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.89775/dimqMSiPWp
31. Republic of Lithuania Law on Legal Protection of Personal Data (2016). 11 June 1996 – No I-1374 (As last amended on 12 May 2011 – No XI-1372)

32. Rose, S., Spinks, N., Canhato, A., (2015) Management Research: Applying the Principles. Retrieved from http://documents.routledge-interactive.s3.amazonaws.com/9780415628129/Chapter%206%20-%20Case%20study%20research%20design%20final_edited.pdf
33. Schneier, B., (2009). Biometrics. Retrieved from https://www.schneier.com/blog/archives/2009/01/biometrics.html
34. Schouten, B., Jacobs, B., (2009), Biometrics and their use in e-passports, Image and Vision Computing, Volume 27, Issue 3
35. Sourcesecurity. (2016). Biometric companies in Lithuania. Retrieved from http://www.sourcesecurity.com/companies/search-results/company-search/pa.biometrics,c.lithuania.html?page=1
36. Statista. (2016). Digital Payments Lithuania. Retrieved from https://www.statista.com/outlook/296/143/digital-payments/lithuania#
37. Statista. (2o16). Mobile Payments Estonia. Retrieved from https://www.statista.com/outlook/331/134/mobile-payments/estonia
38. Statista. (2016). Mobile Payments Latvia. Retrieved from https://www.statista.com/outlook/331/142/mobile-payments/latvia
39. Statista. (2016). Mobile Payments Lithuania. Retrieved from https://www.statista.com/outlook/331/143/mobile-payments/lithuania#
40. Tellis, W. (1997) Introduction to case study. Retrieved from http://www.nova.edu/ssss/QR/QR3-2/tellis1.html
41. The Statistics Portal (2016) Number of Smartphone users worldwide from 2014 to 2020. Retrieved from https://www.statista.com/statistics/330695/number-of-smartphone-users-worldwide/
42. The Statistics Portal. (2016). Statistics and Market Data on Cybercrime https://www.statista.com/markets/424/topic/1065/cyber-crime/
43. Uludag, U., Pankanti, S., Jain, A.K., Prabhakar, S. (2004) Biometric cryptosystems: issues and challenges IEEE, vol. 92, no. 6
44. Verslo Žinios (2015). Mobilieji atsiskaitymai: permainos neišvengiamos. Retrieved from http://vz.lt/sektoriai/informacines-technologijos-telekomunikacijos/2015/12/20/mobilieji-atsiskaitymai-permainos-neisvengiamos
45. World Payments Report 2015 (2015), Royal Bank of Scotland
46. Yang, W., Hu, J., Yang, J., Wang, S., Shu, L., (2013) Biometrics for Securing Mobile Payments: Benefits, Challenges and Solutions 6th International Congress on Image and Signal Processing

47. Yin, K., (2009) Case Study Research design and Methods, 4th edition, Applied Social Research Methods Series, Volume 5 ISBN 978-1-4129-6099-1
48. Zainal, Z., (2007) Case study as a research method. Retrieved from http://psyking.net/htmlobj-3837/case_study_as_a_research_method.pdf

SUMMARY

Novelty and relevance – Biometrics based payment confirmation in mobile payments is not new subject in global technology and payments market. For long time, mobile payments in Lithuania are not in top selected payment methods, this is reflected in data which shows that only 0.01% of all payments in Lithuania are mobile in 2016. Currently biometrics in Lithuania are used mainly by government authorities but not by companies operating in payment industry. Market research in Europe, shows that business and consumers are willing to adopt and use biometrics as security measure in financial sector and also in making payments. Biometrics based payment confirmation model would be new product in Lithuanian payments market and knowing that security is important concern for companies and consumers, new model might increase reliability and usage of mobile payments. **Problem statement** – Option to authorize mobile payments using biometrics, is not offered to Lithuanian consumers, this results in not fully utilizing security measures, which could increase reliability and usage of mobile payments. **Research purpose** – to create biometrics based mobile payment confirmation process model, which could be adopted in Lithuanian. **Research object** – biometrics and biometrics based payment confirmation model, which could be implemented in Lithuania according to existing legal and mobile payments environment. Research on object is supported by scientific articles, legal documents, statistical data analysis. **Structure of thesis** consists of five parts dedicated to separate fields of research. Scientific literature and legal documents review and analysis, statistic data analysis and case study were used in this thesis. **Research objectives** - analyze biometrics and determine most suitable biometrical feature to be used in person authentication; review environment for mobile payments in Lithuania; identify, biometrics based payment confirmation model, which could be used as an example in creating process model to Lithuania.

Main findings of thesis – adjusted biometrics based payment confirmation model is suggested for Lithuania case, as it is related with less risk and requires only additional investment from service provider to create database where fingerprint would be stored.

Key words: biometrics, mobile payments, payment authorization, security, payment model, biometrics based model.

SANTRAUKA

Darbo naujumas ir aktualumas – Biometriniais duomenimis paremti mobilių mokėjimų tvirtinimo būdai yra viena iš aktualiausių temų mokėjimų rinkoje. Jau ilgą laiką, mobilūs moėjimai Lietuvoje nėra dažniausiai naudojamas mokėjimo būdas, tai vaizduoja ir duomenys, rodantys, kad 2016 metais mobilieji mokėjimai sudaro tik 0.01% visų skaitmeninių mokėjimų. Šiuos metu bioemtriniai duomenys Lietuvoje naudojami pagrinde valstybės įstaigose atsakingose už tapatybes dokumentus, bet ne privačiose įmonėse veikiančiose mokėjimų rinkoje. Rinkos tyrimai Europoje rodo, kad verslas ir vartotojai yra pasiruošę naudoti biometrinius duomenis kaip apsaugos priemonę mokėjimuose. Biometriniais duomenimis paremtas mobiliųjų mokėjimų tvirtinimo modelis būtų naujas produktas Lietuvos mokėjimų rinkoje ir žinant, kad saugumas yra vienas iš svarbiausių dalykų tiek įmonėms tiek vartotojams, naujas modelis galėtų tarnauti mobiliųjų mokėjimų metodų populiarumo augimui. **Tyrimo problema** – Mobiliųjų mokėjimų tvirtinimas naudojant biometrinius duomenis nėra siūlomas Lietuvos vartotojams, todėl ne visos saugumo priemonės yra panaudotos užtikrinti sklandžius mobilius mokėjimus. **Tyrimo tikslas** – sukurti biometriniais duomenimis paremtą mokėjimų tvirtinimo modelį, kuris būtų įgyvendintas Lietuvoje. **Tyrimo objektas** – egzistuojantis bioemtriniais duomenimis paremtas mokėjimų tvirtinimo modelis, kuris galėtų būti pritaikytas, atsižvelgiant į esama eknominę ir teisinę situaciją Lietuvoje. **Tyrimo struktūra** susideda iš penkių skyrių, kuriuos aptariami skirtingi aspektai susiję su darbo tema. **Tyrimo uždaviniai** – išanalizuoti kas yra biometriniai duomenys ir nustatyti, kokio tipo duomenys yra tinkamiausi atpažinimo technologijose; peržvelgti mobiliųjų mokėjimų ir teisinę aplinką Lietuvoje; identifikuoti, biometriniais duomenimis paremtą mokėjimų tvirtinimo modelį, kuris galėtų būti išanalizuotas ir panaudotas kaip pavyzdys pritaikymui Lietuvoje.

Pagrindinės išvados – Lietuvos atveju yra siūlomas pakoreguotas, biometrinius duomenis mokėjimų tvirtinimui naudojantis modelis, todėl, kad naujai siūlomas modelis eliminuoja tyrime įvardintas rizikas ir reikalauja tik papildomų investicijų iš paslaugų teikėjo į turimas duomenų bazes, kurios bus skirtos biometriniams duomenims saugoti.

Raktiniai žodžiai: biometriniai duomenys, mobilūs mokėjimai, mokėjimų tvirtinimas, sauga, mokėjimų modeliai, biometriniais duomenimis paremti mokėjimų modeliai.