Lauri Kaipainen

EFFECTS OF PSD2 ON SECURITY ARCHITECTURE OF MOBILE BANKING: A REVIEW OF LITERATURE

JYVÄSKYLÄN YLIOPISTO
INFORMAATIOTEKNOLOGIAN TIEDEKUNTA
2017

TIIVISTELMÄ

Kaipainen, Lauri
PSD2 vaikutukset mobiilipakkien tietoturva-arkkitehtuuriin
Jyväskylä: Jyväskylän yliopisto, 2017, 49 s.
Tietokäsittelytiede, progradu -tutkielma
Ohjaaja: Siponen, Mikko

Tämän progradu-tutkielman tarkoituksen on selvittää, mitä muutoksia maksupalveludirektiivi (PSD2) tuo mobiilipankkien tietoturva-arkkitehtuurille. Astuessaan voimaan PSD2 luo tilanteen, jossa mobiilipankkien tietoturvamekanismit ovat erillään varsinaisesta mobiilipankkisovelluksesta. PSD2 mukaan maksupalveluiden tarjoajien on annettava pääsy heidän tietoturvamekanismeihinsa ulkopuolisille sovelluskehittäjille API:n (Application Programming interface) avulla. PSD2 vaatii myös, että maksupalveluiden tarjoajat luovat vahvan asiakkaan tunnistautumisen, joiden pitää olla erillisiä ja itsenäisiä toimintoja mobiilipankkisovelluksesta. Tieteellisessä tutkimuksessa ei esitetä tietoturva-arkkitehtuuri mallia, jossa erilliset tunnistautumissovellukset toimisivat erillisen mobiilipankkisovelluksen kanssa. Tieteellinen tutkimus voi kuitenkin tarjota ratkaisun PSD2:n vaatimuksiin tiedon salaamiseksi ja viestiliikenteen virheettömyyden takaamiseksi. Tämä voidaan tutkimuksen perusteella toteuttaa PKI:n (public key infrastructure) tai sertifikaatittoman epäsymmetrisen salausjärjestelmän avulla. Tässä progradu-tutkielmassa käytettään systemaattista kirjallisuuskatsausta selvittämään PSD2 tuomat muutokset. Vertailu toteutettiin listaamalla PSD2:n turvallisuuteen liittyvät vaatimukset ja velvollisuudet, joita sitten vertaillaan kirjallisuudesta löydettyjen teemojen kanssa. Tutkielma löysi lopulliseksi tutkimusmateriaaliksi 22 tieteellistä artikkelia mobiilipankkien tietoturva-arkkitehtuurin toteuttamiseksi.

Asiasanat: Maksupalveludirektiivi, Tietoturva-arkkitehtuuri, Mobiilipankki

ABSTRACT

Kaipainen, Lauri
Effects of psd2 on Security Architecture of Mobile Banking: A Review of Literature.
Jyväskylä: University of Jyväskylä, 2017, 49 p.
Information System Sciences, Master's Thesis
Supervisor: Siponen, Mikko

This thesis aims to find out the changes that the Payment Service Directive (PSD2) will bring to the security architecture of mobile banking. PSD2 will create a situation where security mechanisms are separated from the actual banking application. Payment service providers must provide their Application Programming Interface for third party developers to give them access to authentication of payment transactions. PSD2 requires payments service providers to offer strong customer authentication with separate authentication mechanism from the banking application. This thesis found that academic literature about the security architecture of mobile banking does not provide a model where a separate authentication mechanism should communicate separately from the mobile banking application. Academic research could however, provide solution to use the Public Key Infrastructure of a certificateless asymmetric encryption to achieve demand of PSD2 to offer strong encryption and means to check the integrity of data and make transactions non-reputable. The research in this thesis was conducted as a systematic literature review, which found 22 academic publications about the security architecture. The comparison between the demands of PSD2 with the academic literature was done by listing security demands and responsibilities of PSD2 and comparing them with themes found from the research material.

Keywords: Payment Service Directive, Security Architecture, Mobile Banking

FIGURES

TABLES

TABLE OF CONTENT

1 Introduction

In the year 2015 the European Union published a new payment service directive called PSD2. The purpose of the directive is encouraging digitalization of banking services and makes sure that the internal markets of the EU function in the same way in the whole Union. The most significant change is that payment service providers must give third party developers free access to their authentication mechanisms. The directive motivation to do this is to create an innovation friendly environment in EU's internal markets. Chapters four and five of PSD2 set security and data protection requirements for payment service providers. The detailed security requirements are in Regulatory Technical Standard document called RTS, which was created European Banking Authority. The legality of RTS is set in article 95 section 3. The directive's measures shall be applied in member states by 13. Of January 2018. (EU 2015/2366)

The change this directive brings will be significant since banks and other payment service providers have a risk to lose contact of their customer and becoming just money transaction authenticators, according to the market research report of Accenture in 2016. On top of the responsibility of the banks Price Water Cooper's CEO André M. Bajora argues in interview in 2016 that banks need to provide reliable and functioning authentication infrastructure even to stay in competition.

The research question of this thesis is how will PSD2 will affect the security architecture of mobile banking. This research problem is divided into following research questions: **The primary question is** "How will PSD2 effect on the security architecture and design of mobile banking?". **The secondary question** "What security demands RTS of PSD2 will set for each party involved?". The goal is to gain an overall picture of relevant changes and what can be used from the academic research.

Information Security architecture (in this text called 'security architecture') is an abstract model of information system's security functions. It is similar with system architecture but it's focus in security functions and procedures. Its purpose is to be a management tool for designing and implementing security relat-

ed responsibilities and policies.(Eloff and Eloff, 2005; Peterson, 2007) Security design on the other hand the principles that are used as the basis of security design of information system. (Siponen, 2006)

The research method used in this thesis is the systematic literature review, which uses predetermined material gathering plan and inclusion criteria to find all the relevant literature related to the research topic. The reason why the systematic literature review was chosen is to provide transparency for material gathering process and the method demands a specific plan for gathering material minimizing the human error (Jesson 2011). In this thesis 22 articles where included out of over 700 articles found in initial search. The limiting factor was that this research only used the free research databases and the databases accessible to students of University of Jyväskylä.

The research found that the academic research does not provide a model where security functions of mobile banking is separate from the banking application itself. This leaves a cap where research does not answer how will separate authentication processes and banking application can cooperate securely even when either of them is compromised. However, it was found that some of the security architecture models proposed in the literature can provide solution to ensure security, integrity and non-reputability of transaction and communication between the bank, the payer and the payee. This could be achieved by using a public key infrastructure or a certificateless asymmetric encryption method. This thesis provides a list of the security responsibilities in PSD2 and provides an overview of what future research should focus on when it comes to mobile banking in Europe.

2 On security architecture and design, mobile banking and PSD2

The purpose of the second chapter is to function as the theoretical basis of this research by giving information on the topics that are necessary to understand the research question. The research question is about the security architecture of mobile banking and how will the second payment service directive (PSD2) effect the security architecture of mobile banking. This chapter is divided into three parts: Security design and security architecture; mobile banking and the second payment service directive.

2.1 Security Design and Security Architecture

Security design and security architecture will be covered in this chapter by first giving introduction to system design and system architecture principles in general. Afterwards, security architecture and security design methods will be covered.

2.1.1 Architecture and Design

Architecture in general, is a description of components and relationships between them. In information systems, this means that architecture should be able to present a concept model of an information system, which would show what system looks like and what it does (Armour, Kaisler and Liu, 1999). Designing an information system is about creating a product and a process, which result in an information system. Designing product means identifying what system is supposed to do and how. The process part is about describing components needed to construct the system. (Walls *et al.*, 2004)

Enterprise architecture contains following perspectives to present information about the system:

- Business view: Why the system exists and how it supports the business goals.
- Work view: How and where each component should be placed by business location and how each component should communicate.
- Information view: What kind of information is processed thought the system and how the different processes are related to each other.
- Function view: How will the system support the business functions by providing information or value.
- Infrastructure view: Description of technical components and technologies that system needs to function (Armour, Kaisler and Liu, 1999).

In IT, architecture can be divided into classes, which are all focused on the different aspects of creating an information system. The classes are: software architectures, network architectures, system architectures and enterprise architectures. Within these classes, system architecture and enterprise architecture are the so-called meta architectures since both focus on presenting the whole information system. On top that, enterprise architecture contains the business goals and processes of system and how it is intended to be used. (Armour, Kaisler and Liu, 1999)

There are different frameworks to guide the use of enterprise architecture, which differ by the ways they approach to solve issue of creating the architecture model (Urbaczewski and Mrdalj, 2006). These frameworks are divided in two frameworks: the classical enterprise framework and the federal enterprise framework. The key difference is that federal enterprise framework was created by government agencies by using existing models of the classical framework (Goethals *et al.*, 2006). Goethals (2006) et al. research shows following, significant frameworks:

- Classical Frameworks:
    - **Zachman:** The point of this framework is to gather information, which would benefit all the parties involved in use of the information system such as business strategy, IT infrastructure etc. All the parties involved are found by using 6x6 table. The beauty of this model is that in reveals possible contradiction between parties during the creation process.(Zachman, 1987)
    - **Kruchten's 4 +1 model:** Consists from views on enterprise architecture: *logical, development, process and physical*. The plus one view is called *scenario*, which presents the use cases of the system. This model ties views closely together thus the views cannot be worked independently (Kruchten, 1995)

- **Soni, Nord, Hoffmeister model:** In this model, each view aka structure can be developed independently while maintaining the relationship between them. The structures are called: conceptual, module, execution and the source code. (Soni, Nord and Hofmeister, 1995)
- **Tapscott and Caston model:** Consists from 5 interrelated views to create enterprise architecture and each view: business, work, information, application and technology. The views contribute to creation of each other thus it should prevent contradictions between the views. (Goethals *et al.*, 2006)
- **RM-OPD (The ISO Reference Model of Open Distributed Processing):** An architectural design model where each view is not a considered as a layer of architecture but a different perspective to show what system does in abstract level.(Farooqui, Kazi; Logrippo, Luigi; de Meer, 1995)
- **OMG's MDA (Model Driven Architecture):** MDA makes the architectural plan by first creating a platform independent model (PIM) of the system, which describes the general functions. After that a platform specific model is created (PSM), which gives technical details about how system should function and be build.(Soley and OMG Staff Strategy Grop, 2000)

- Federal Frameworks:
  - **The Federal Enterprise Architecture Framework (FEAF):** Created to enable interoperability between government agencies. Architecture consists from 2 parts business architecture, which explains purpose and functions and design architecture, which contains technical details on data, application and technology. (obamawhitehouse.archive.gov, 2017)
  - **C4ISR (Command, Control, Computers, Communications, Intelligence, Surveillance, and Reconnaissance):** Now known as DoDAF since version 2.0. Created for US Department of Defence. Describes systems performance and its functional effect on missions. (dodcio.defense.gov)
  - **Treasury Enterprise Architecture Framework (TEAF):** US department of Treasury model aims to manage effetely IT-investments by creating common requirements for the agencies. (opengroup.org)

2.1.2 Security Design and Architecture of Information Systems

The previous chapters introduced what enterprise architecture is, what its used for and how different frameworks portray its use. The purpose of the following chapters is to write about different methods on how secure systems are designed. We first look how the security design methods have evolved from the past until the present day.

In 1993, Richard Baskervile published his paper, which examined the various kinds of IT security design methods. The idea of the paper is to evaluate each design methods and consider their pros and cons. The paper identified three design method types: *checklist, mechanistic engineering and logical and transformational design* (Baskerville, 1993). Baskervile's findings were further examined and thus, two new information security design methods were identified *social-technical design and social and adaptable design* (Siponen, 2005). Following chapters discuss about each generation of methods more in detail.

Checklist method design, presenting generation 1, is based on providing a list of security solutions on listed security issues related to each component of the information system. Checklist also contains a list of viable solutions in the market. This makes checklist method easy to use, since it doesn't require specific IT-skills to use (Baskerville, 1993). Checklist method later evolved into the information security standards and thus BSI 1799 and its follower ISO/IEC 1799 was created. The idea behind standards is to provide organizations a common way and criteria to implement information security in their organization. Its argued that standards give all organizations the minimum level of security. The interesting difference between standards and checklists is that standard needs to be fully implemented without exceptions unlike checklists, which want organization use only necessary parts (Siponen, 2006). Checklists and standards have their weakness in its list-like characteristic. The method doesn't use analysis of system in terms of how it works and what kind of threats are relevant to system. This leads into situation where the security solution is just implemented into system in without considering if it is adequate solution or not when considering what system or its part does and in what environment. Standards fail to see special needs of organizations when it comes to their business and culture. For example, Security functions and organization will be different in military organization and company of just less than 10 people. (Baskerville, 1993; Siponen, 2006)

Mechanistic engineering design, presenting the second generation, approaches security design by identifying all the elements of an information system and evaluating the security needs for each element. Element can be a technical part of a component, a function in software or a server as part of architecture. This complex approach allows to create a custom system, based on its function and needs. Typical way to use mechanistic engineering is to use a systems flow charts and something similar (Baskerville, 1993). The strength of this

kind of design model is that it's based on tested software and methods of information system development. It also helps conducting requirements engineering investigation on the system (Siponen, 2006). Despite the holistic and customizable nature of the second-generation methods its major weakness comes from its poor adaptability. The reason for this is that this method is a separate process when the system or software is created. This puts the development team in situation where they need to familiarize themselves with the method thus, taking time away from the project. The method also requires vast knowledge about information systems, meaning that a separate design team for security would be required. (Baskerville, 1993; Siponen, 2006)

Logical and transformational design, presenting the third generation, is based on creating abstract models of the system and its functions, giving an understanding on what the system does and then, identify the security needs. This method assumes that the security demands of systems are unique. The abstract model then functions as a map to construct the system itself. This model creates an easily maintained security documentation due to its broad expressions. Unfortunately, an abstract level of design becomes problematic when the actual system elements needs to be implemented. Also, some security aspects like encryption are difficult to express in an abstract way. It should be noted that this method is only used when the system is created from the beginning. This system doesn't help with creating a security solution for an existing system.(Baskerville, 1993)

Socio-technical design, presenting the fourth generation, takes human aspect into account when designing the system. This is achieved by using user participation as a tool. In this model, user participation means identifying their responsibilities and tasks as the users of the system. This creates a responsibility model where each employee's tasks are identified, and this leads to the so-called viable system, presented by Karyda et. al in 2001 (Siponen, 2005). The viable Information system design is based on idea where security of a system is designed in a way that it can maintain its most essential functions, even in situation where its integrity has been violated. Using this idea protects organizations main function or organization can recover fast from damages on main functions that system does (Karyda, Kokolakis and Kiountouzis, 2001).

Social and adaptable design, presenting the fifth generation, this method also takes user participation into consideration but extends it beyond responsibility model by taking user into process and having their input. This input is necessary since employees have expertise and special knowledge on their line of work. Using the knowledge of intended users increases the relevance of system's security functions and grows acceptance among the intended users. This also makes security design fit better into organizational culture thus, making it more suitable. The other core goal is to make adaptation of security as effortless as possible. This requires the consultants etc. to have good understanding on software development. The idea is set security design as a natural part of system or software development. (Siponen, 2005)

Information security design methods are heavily theory based and lack serious empirical research to prove their effectiveness. The situation changed when Siponen et al. (2006) presented the Meta-notion design method. It presents a social and adaptable security design system and it has following requirements:

1) Method should protect objects from impacts of the threat considering potential damages;
2) Security design should be based on company's requirements;
3) Should be able to provide an abstract presentation of threats, objects and security features. The levels of abstraction are organizational, conceptual and technical;
4) Method should be able to be integrated into any information system design method and should not require specific training to use it.
5) Maximize autonomy of developer to use any developing method they desire;
6) Should be adaptable to any new and upcoming information system design method to ensure continuity of security design for systems.

This method was empirically tested in a large software company. The research was conducted as an actions research. Meta-notion was implemented into different steps of the process and it was effective independently, making it easier to use within the organization.(Siponen, Baskerville and Heikka, 2006)

Research about creating secure systems are also presented as information security architecture (ISA). ISA is, in its essence, a management process and its purpose is to create an abstract architectural model of security features. For ISA to be affective, ISA should have a model of the business process and its security needs. On top of that, technical solutions should be modelled in the ISA (Eloff and Eloff, 2005). ISA should be used in such a manner that it allows the security designer of the system to use novel ideas, technologies and polices to implement ISA into general enterprise architecture model (Peterson, 2007). Integrating ISA into enterprise architecture in a way that it supports the business functions should be done by using risk management to identify relevant threats against the business process and assets. Only then, an architectural abstraction can be created. When the system is created according to architecture, it is time to measure the performance of the security features and evaluate them. This leads to continuous development cycle. This cycle was made famous by BS 7799-2 *Information Security Management standard(ISMS).* The goal in using this kind of continuous development cycle ideally, constantly improves the security of the system (Eloff and Eloff, 2005; Peterson, 2007).

ISMS integration was also supported in the Hensel's paper in 2010 (Hensel, Lemke-rust and Augustin, 2010). A research paper from Grandry et al. from 2013 proposed integration of information system security risk management into enterprise architecture modelling program. Risk management and security fea-

tures where presented in the program as a concepts, which make them similar with enterprise architecture concepts (Grandry, Feltus and Dubois, 2013).

2.2 Mobile banking

This chapter focuses on providing understanding about what mobile banking is, explaining its evolution as a growing trend globally. The second objective of the chapter is review security threats and issues that mobile banking faces to gain an understanding of the security landscape. The security issues will be discussed by considering research about the security threats and issues of smart phones and mobile applications.

2.2.1 Mobile Banking as a trend

Mobile banking means payment and financial services that can be used via telecommunication device such as a mobile phone (Mallat, Rossi and Tuunainen, 2004). Mobile banking can initiate mobile payments, which are dived in two categories: micro- and macropayments. Micropayments are the first form of the mobile payments, which are focused on small transactions. Micropayments usually consist of payments of small services and goods such as public transportation tickets, vending machines, kiosk payments and other on-the-spot-services. Apple's iTunes purchases are also one of the early examples of micropayments. The most notable feature of micropayments is that user's bank account is not directly used for transactions. Macropayments are similar with purchases that would usually be done with payment card. Examples of macropayments are e-commerce, gaming, e-tickets, restaurants and retail-shopping (Mallat, Rossi and Tuunainen, 2004).

Research has shown that since the year 2000, interest towards mobile baking has increased. This was seen when number of publications and conventional news articles about mobile banking was steadily increased. It is argued that mobile banking will eventually become a common practise. Mobile banking as a trend has not evolved fast due to technical limitation. Research points out that significant interest about mobile banking was sparked when the computing and the network capabilities of devices were adequate support more sophisticated baking actions and make them more convenient for the users. (Dewan, 2010; Moser, 2015)

2.2.2 Technical Elements of Mobile Banking

The following will be an explanation to how mobile banking works on a technical level. Security details will be discussed and modelled after the research result chapter. The idea is to provide a picture of technical elements what is needed for mobile banking to operate. The drawn model is based on research paper issued Chung et. al. (2005). Their proposal offers a general framework to model and understand mobile banking architecture.

The use of mobile banking requires ability to use a network connection on the move. Ideally, user would not even notice when the network is changed. Mobile devices can access internet by using the mobile IP mechanism. When using mobile IP, a device receives one IP address regardless what network the device has been in. The mobile IP address comes from home network, which is called Home Agent (HA). When the device visits a new network, it's called Foreign Agent (FA). The device searches its HA with help of FA and when it's found, a tunnel connection is established between HA and FA. By doing this, all the data packet will go through HA and thus maintaining its IP address the same, even in a new network.(Chang, Chen and Tseng, 2005) Picture 1 visualizes the concept and it's based on Chang et. al (2005) research paper.

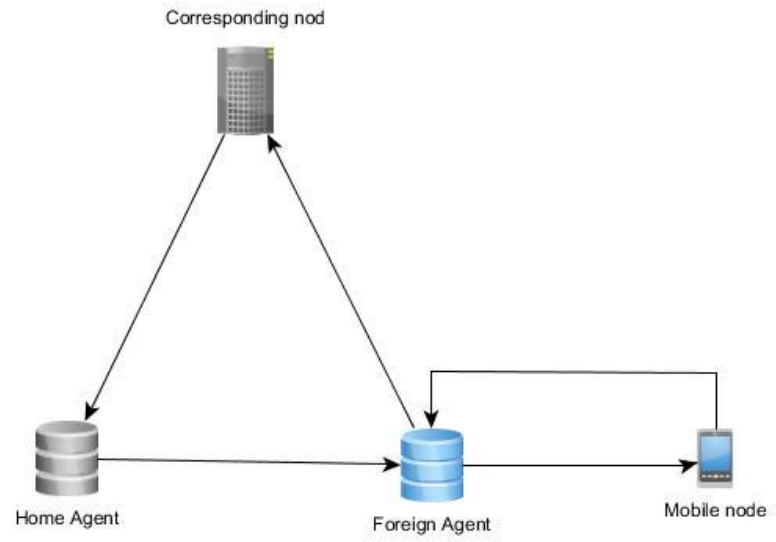

FIGURE 1 Mobile IPv4

Web Service is a standardized model to bind applications together with the use of existing infrastructure. Purpose of Web Services is to solve the technical issues of inter-application interaction and interoperability. Basically, services are published and found by using a discovery agent. If some applications service is wanted, the request will be sent to the discovery agent and if services are published in a service agent. The model also has intermediary functions, which provide functions like routing and security etc. Picture 2 visualizes Web Service Architecture based on the paper written by Chang et al. (2005) research.

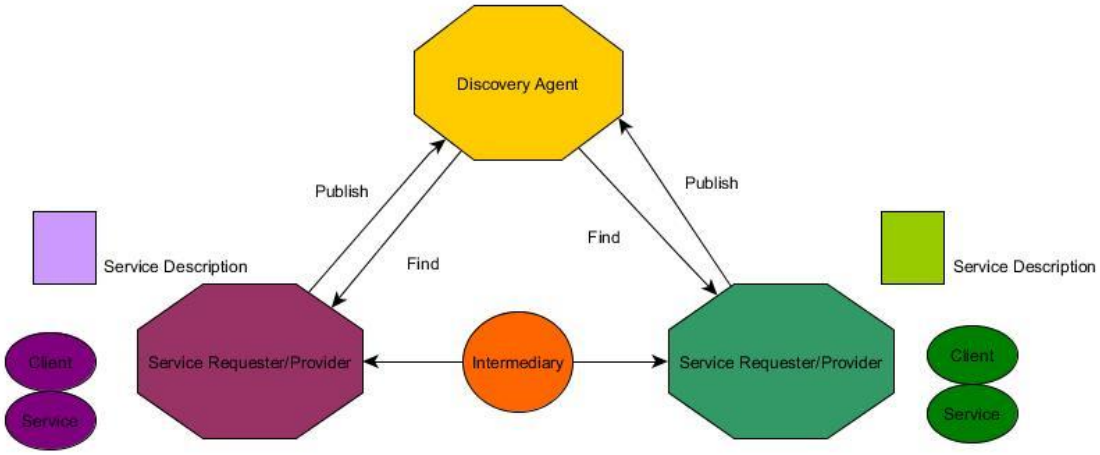

FIGURE 2 Web Service Architecture

2.2.3 Security threats against smartphones

Security threats are actions that cause harm against a smartphone or data that it holds. Threats are caused either initiated intentionally by an attacker or initiated unintentionally by user (Jeon *et al.*, 2011). Table 1 contains a list and description of security threats against smartphone. Its content is based on the research paper published by Jeon et al. (2011) and all further information is cited additionally.

TABLE 1 Security threats against smartphones

Threat	*Description*	*Agent*
Threats initiated by attacker		
Malware	A malicious program designed to send information to attacker from user's phone. Potential for loss of sensitive information or financial losses. Divided to viruses, trojans and spyware.(Jeon *et al.*, 2011; Wang, Streff and Raman, 2012)	User is tricked to download a malicious application using disguise of a popular app, game etc.(Wang, Streff and Raman, 2012)
Wireless network attack	An attacker can listen or even modify wireless communication between 2 parties.	An attacker needs to redirect communication to go through his/her computer. This redirection allows to break encrypted data traffic. (Kieseberg *et al.*, 2015)
Denial of Service	An attacker can make a smartphone unavailable to user.	This can be done by flooding smartphone with incoming call or text messages. (Wang, Streff and Raman, 2012)
Break-in	In a case where an attacker gains full or partial control over a smartphone. The attack can be done by abusing flaws in the application code.	Attacker can try corrupting memory to execute arbitrary code in memory or use Jail-Break program to gain root-access.(Wang, Streff and Raman, 2012)
Threats initiated by unaware user		

Phishing	Attempt to gain user's confidential information.	For example, attacker can lure user into phishing site to press button that is disguised as Facebook's like button. Then user will fill his/her information to 'login' Facebook.(Wang, Streff and Raman, 2012)
Loss of device	User can loss their smartphone, giving attacker physical access to try break into it.	
Platform alternation	User alter the system of smartphone by using so called jail breaking, which gives them root access to operating system allowing user to have access to all capabilities of the operating system.	Jail breaking programs are popular and produced very fast. Jailbreaking is used to bypass security restrictions. (Wang, Streff and Raman, 2012)

All the security threats mentioned above are relevant to the mobile banking applications as well as mobile applications in general. However, there is research on cyberattacks especially against mobile banking applications. The most used form of attack, according to research, is the so-called repackaging attack. The idea in this attack is to take a popular application, create a malicious version of it and lure user to get it. This way, an attacker can either inject unwanted code into application or get a trojan horse into user's mobile phone and communicate the information the attacker wants. These attacks are difficult to stop since Android's Google Play is open platform to publish applications. Attack is basically done by creating malicious code (replaces so called smali-file), download targeted app, compile the app with the malicious code, get the permissions of the original application, contained in the original application. (Zheng, Pan and Yilmaz, 2017)

2.2.4 Security Features of Android and iOS

Android system's security model enforces a sandboxing of applications in its system. This means that all the applications are limited to only certain resources thus, making them unable to interact with the resources of each other. An application cannot tamper resources or data held by another application making them immune to viruses (not the phone itself). Sandboxing is also

implied to user who is restricted from getting the root-access, making user's downloaded virus incapable of using system commands in the root.(Flynn and Klieber, 2015) Apple's iOS operating system also uses a sandboxing of applications that have been made by the third party developers. (Apple, 2017)

Despite the sandboxing, Android applications can communicate with each other. All functionalities such as camera, telephone and system mechanisms etc. work as an application. The communication between Android applications is done by using the so-called 'intents'. An intent means that application will send a request to use a part of application's functionalities, which are called components. If sn application wants to use camera, it needs to express its intent to use it. However, an application can only use a component if it has a permission to do so. This permission-based security mechanism basically creates access control list for applications if both applications have matching access right list to component, permission is granted. Notice, that denial to access the components of the application is not based on naming applications, which would be problematic because developer cannot know what applications user will have in the phone. The access control list is created during installation and when intent is initiated, IPC mechanism will check if both of the applications have matching security policy.(Eneck, Machigar and McDaniel, 2009)

In Apple's iOS operating systems, third party applications can interact with user information such as contact details and iCloud with a specific key pair, letting Apple know the developer who uses these resources. If a third-party application wants to communicate or use resources of another third-party application, they need to be in an application group. In an application group, all the apps share a unique key, which enables them to recognize each other. This way iOS ensures that no unwanted application get to handle resources of application. (Apple, 2017)

Previously mentioned security features in Android and iOS demonstrate their ability to protect applications from each other. Both operating systems allow developers to make applications communicate by using TLS/SSL protocol to protect their data traffic (Apple, Google, 2017). This still leaves some holes. Android has divided all its functionalities into applications and default applications. They are in risk, since they are openly known by developers. This gives malware applications resources to work with microphone and camera etc. Android's security systems was created to protect apps from themselves, not the whole system(Amer *et al.*, 2008). Android has been given critique for not being able to black or white list applications within the system (Ongtang *et al.*, 2012). Apple's developers need to be registered thus, making malware creation risky because system makes malicious developer easy to find since they need to be registered by a real person or registered organization (Apple, 2017).

2.3 PSD2 and EU-law

This chapter introduces the second Payment Service Directive (PSD2) in terms of how it will change mobile banking and what security requirements PSD2 will enforce for mobile banking and similar applications. This chapter also gives a brief introduction to how the European Union law creation and implementing works.

2.3.1 Legislation process in EU

The legislative power of the European Union (EU) was the first time established in the treaty of Maastricht in the year 1992 and its latest and current form was given in the treaty of Lisbon in 2009. The treaty of Lisbon established so called Codecision process, which aims to make EU's legislation legitimate in terms of principles of democracy. EU law consists of primary and secondary legislation. The primary legislation is basically the treaties, which give EU its legitimate power to do the secondary legislation, which consists of the directives, regulations and decisions. Codecision process begins from the proposal of EU Parliament. This proposal is given to commission, which presents the law proposal to the Council, which consists of representatives of member states. After the Commission has gave the initiative, parliament and the Council start review process. The point of review is to function as means to negotiate about the content of proposed law. When agreement has been achieved, law is passed. If agreement will not be found after two rounds of review, a separate negotiation will be held by the conciliation, which has representatives from member states and from parliament, 28 in total. When a proposal is in a drafting state, Commission conducts impact assessment, which considers economic, social and environmental effects. During the drafting period business' and citizens can use the public consultation period to express what should be taken into consideration. The Commission consults experts, Non-governmental organizations and the local authorities during drafting process. (the EU, 2017)

2.3.2 The Second Payment Service Directive

The EU directive 2015/2366 aka the second Payment Service Directive(PSD2) is the continuum of previous Payment Service Directive 2007/04/EC. PSD2 was created because the previous directive didn't offer clear rules about payments done over internet or by using a multipurpose device such as mobile phone or tablet. Directive's introduction argues that this ambiguous state of regulation hinders the development of electronic payments methods. The directive emphasises willingness to encourage innovation within the mobile payment industry. PSD2 states that it has following goals:

- Create a common responsibility model in all the member states;

- create a strong consumer protection when using electronic payment services;
- bring clarity to the regulation;
- ensure that electronic payment is done in a secure way.

PSD2 will not be concerned of mobile payments where phone operators act as payment medium through subscription bills. Service payment cards that are exclusive payment cards for specific service provider. PSD2 is made to legislate electronic payment done remotely from service provider or financial institution. PSD2 defines remote payment transaction as "a payment transaction initiated via internet or through a device that can be used for distance communication". Role of financial institutions as the operators of payment industry will not change because of PSD2 (EU 2015/2366). Parties and terminology relevant to PSD2 is listed and explained in table 2.

TABLE 2 PSD2 parties

Term	**Abbreviation**	**Explanation**
Payment institution		Legal entity that has been authorised to carry out payment transactions and supervise them. For example, a bank.
Payer		A Natural or a legal person who gives a payment order to other party
Payee		Party that has been intended to receive funds through an ordered transaction
Payment service user	PSU	Either payer or payee of service which uses a payment service
Account Information Service	AIS	An online service to provide consolidated information on one or more payment accounts held by the payment service user in one or more PSP.
Payment Service Provider	PSP	Services enabling funds to be placed on a payment account as well as all the operations required for operating a payment account
Account Servicing Payment Service Provider	ASPSP	Same as PSP but it also holds and maintains a payment account for payer.
Payment Initiation Service Provider	PISP	A service, which makes payments request to PSP to transfer money to another bank account
Account Information Service provider	AISP	A service which makes a request to PSP to show his/her payment account information.

PSD2 states the need to ensure the authentication of remote payment users to create trust for the consumer. Authentication is defined by PSD2 as a procedure where PSP verifies the identity of PSU from a specific payment instrument. The payment instrument refers to a multipurpose device in which payment services are used. PSD2 mandates that PSPs need to use a strong customer authentication(SCA) where more than one authentication element is used. Each authentication element must be independent of each other, meaning that compromising one element will not affect the other elements.

PSD2 article 98 sets Draft Regulatory Technical Standards(RTS), the official document to provide technical details for security demands. The final draft of RTS was published in 23rd of February 2017 after public consultation. PSD2 has set following goals for RTS:

1. Ensure appropriate security measures for PSU and PSP by using risk assessments to determine strength of the security features;
2. Ensure the safety of funds and personal information of PSU;
3. Technical demands should be technology and business neutral;
4. Maintaining faire competition among PSPs;
5. Encourage innovation of payment methods.

RTS explains details of strong customer authentication in article 7, 8 and 9. There are three elements and at least two needs to be implemented by PSPs in their authentication method. The elements are knowledge, possession and inherence. **Knowledge** is something that only the PSU knows. Knowledge must be protected from disclosure to unauthorised parties, including staff of PSP. **Possession** is something the PSU has. This functions as a key to be used with another authentication method. RTS gives one-time password generator as an example. Replication of possession element should not be possible. **Inherence** is something that user is, which means basically use of biometric sensors to authenticate PSU.

The application and the device should be highly resistant against attempts of an unauthorised user to pretend to be the payer or payee. Combination of more than one of these elements should result in an authentication key that cannot be forged and is unique is such a way that knowledge of a previous keys does not allow creating new valid keys. Keys should be Independent of each other meaning that compromising one element should not affect the other. This also means that the compromised authentication element cannot be used the forge other authentication elements. RTS aims to secure banking application by making use of a separate secure execution environment mandatory within multipurpose devices such as a smartphone. The separate secure execution environment is created during the installation of the application. PSP must create mechanisms to recognise if application used in authentication is tampered within PSU's device. (EBA/RTS/2017/02)

According to article 27 of RTS, the strong customer authentication must take place in a communication interface created ASPSP. The point is that the services that need to use ASPSP to authenticate their users and thus, it is re-

sponsibility of the ASPSP to make authentication of payer reliable for service providers to use. The communication interface must ensure confidentiality and integrity of personalized security credentials when they are sent to the PISP or the AISP. All the PISP, AISP etc. need to have equal access and have the same level of security, performance and availability to the communication interface to let their user to link their payment account to payment service, stated in article 28 of RTS. Paragraph 3 of article 28 says that the dedicated communication interface fulfils the requirements stated in ISO20022. (EBA/RTS/2017/02)

In article 5 of RTS, it is required that the PSP needs to implement a dynamic linking process. The idea of dynamic linking is to enforce confidentiality, authenticity and integrity of transaction amount and payee. Payer is made aware of the amount of money transferred to payer. This is further enforced by using an authentication code specific to the amount of money transferred. Article 5 of RTS explains that the purpose of binding authentication code to amount of transferred money is to give the PSU an opportunity to give consent to do the payment. RTS goes further in securing the payments in article 26 by demanding the PSPs to create a mechanisms to make transactions traceable by using unique identifiers, which consists of information relevant to the sessions, which includes transaction information and a timestamp (unified time synchronisation). Naturally, there are more self-explanatory requirements, which were not discussed. These and discussed security requirements are fully listed in annex 1.

3 Research plan and method

The purpose of this chapter is to explain the research plan and how the systematic literature review will be used to answer the research question. This chapter begins from introduction to previous research related to effect of PSD2 to security landscape of mobile banking. The chapter also explains the motivation for this research and explains its relevance. Later chapters introduce the research plan.

3.1 Previous Research

The previous research about the effects of the PSD2 on the security of mobile banking has been focused on authentication and understanding potential risk that new legislation brings. PSD2 has been criticised being too vague about security criteria and responsibilities(Mansfield-Devine, 2016). This concern was raised before Regulatory Technical Standard was introduced in the year 2017. PSD2's requirement for strong customer authentication has been discussed in research papers, which propose authentication schemes for multi-purpose devices (e.g. Smartphone). Use of biometrics to authenticate the user is supported in some papers. The main argument for biometrics is its strength compared to regular passwords and it is easy to use, which is claimed to be necessary because it would enable more frequent use of mobile payment while guaranteeing sufficient level of protection (Cook, 2017; Hung, 2017). One way to satisfy the requirement of PSD2 for the strong authentication is to use two-factor authentication where authentication elements are independent from each other. This can be achieved by using sandboxing. However, sandboxing can be broken if attacker gains access to system level and if application cannot recognize if the system is tampered or not, attacker will get access to application data (Haupert and Müller, 2016).

Based on the previous research this thesis will address to recognize technical demands for making mobile banking secure while comparing them to

how current research suggest the best way to make mobile banking secure. Research related to the security architecture and designing secure mobile banking will be covered during the systematic literature review.

3.2 Motivation

The point of this comparison is to demonstrate what kind of changes banks and application developers should be prepared for. Each member state of the EU needs to implement PSD2 by 13.8.2018(EU 2015/2366). PSD2 will be one of the most significant changes in the European banking since it opens the IT infrastructure of the banks thus making banks possibly lose contact with their customers, according to survey of Accenture (2016) and Price Water Coopers (2016). Price Water Cooper's report further states via an interview with André M. Bajora, the CEO of Figot mobile banking app, that the only way for banks to be successful after PSD2 is to provide the best solutions and reliable infrastructure. PSD2 gives banks responsibility to open their infrastructure and are responsible for proper customer authentication and security as it is stated in article 95 of PSD2.

3.3 The research question and goals

The chapter introduces the research problem and the research questions to answer that problem. This chapter also sets research boundaries.

3.3.1 The Research Question

the aim of this literature review is to explore possible difference between the current research on how the security of mobile banking is designed and what demands EU's second payment service directive(PSD2) sets for mobile baking. The European Union has issued a new directive called PSD2, which shall regulate responsibilities of the banks and the application developers when providing mobile baking services(EU 2015/2366). PSD2 states that it shall also set technological demands to improve the security of mobile banking apps. This document is called RTS (regulatory technical standards) and it's been issued by European Banking Authority(EBA) This document is the main source for new technical security requirements(EBA/RTS/2017/02).

Considering the upcoming legislation to mobile banking and the significance pointed out in the chapter 3.1.2 this research has two questions: the primary and secondary research question. **The primary question is** "How will PSD2 effect on security architecture and design of mobile banking?". **The sec-**

ondary question "What security demands RTS of PSD2 will set for each party involved?"

3.3.2 Research boundaries

Research is focused on mobile banking done via application. Article 3 of PSD2 lists the types of mobile payments that PSD2 will not address. The exceptions are the following:

- Service based payments that are not used for common purchases or the payment instrument is usable only in a single member state;
- Payment service where mobile operators send invoices to their subscribers;
- Cash withdraw.

Article 3 excludes minor payments that are less than 50 Euros. This will not however limit the research since the point of this research is to understand security design of mobile payment technology.

This research then identifies the security demands of PSD2 presented in RTS document and then identifies the differences to academic research. Based on arguments above the main research question is "How will PSD2 effect on security architecture and design of mobile banking". Comparison is done by first creating abstract architecture picture on security features of mobile bank to demonstrate features. This picture will be later compared with finding of the research. Therefore, the secondary research question is "What security demands RTS of PSD2 will set for each party involved?" The abstract security architecture of the demands will be introduced in chapter 2, since it works as a theoretical basis.

The research will be carried out as a systematic literature review (see chapter 3.4) to identify what kind of solutions academic research has created to make mobile banking secure. This way, a general understanding will be obtained. Research material for academic papers will be gathered by using access to publication portals provided by Jyväskylä University. Theoretical bases will be conducted as traditional literature review where the goal is to gather information on following topics: Information security architecture and design, Mobile banking and threats, Payment Service Directive 2 and Mobile operating system security. Articles will be search from publication portals provided by University of Jyväskylä.

3.4 Systematic literature review as a method

This research will be conducted as a systematic literature review. Systematic literature review is a review of academic literature on a well-defined subject and gives a transparent report on gathering the articles examined in the review. This makes systematic literature review a repeatable research thus increasing its validity since anyone can repeat the process. In comparison, traditional literature review doesn't have clear structure and material searching is not documented. Primary purpose of traditional literature review is present the current state of research in specific field of study without reported plan to find relevant literature. (Jesson 2011)

In a systematic literature review, the process should be documented well. The process document of a systematic literature review contains information on:

- Data bases used to search literature
- Search terms
- Number of found literature
- Explanation on criteria which dictates what literature is included and what excluded. (Jesson 2011)

Listing data bases used for searching suitable articles gives the reader an understanding on used sources and number of articles found with the search terms (Jesson 2011) The search terms and data bases are presented later.

3.4.1 Inclusion and Exclusion Criteria

Systematic literature review gets is systematism from transparent and documented criteria on when found literature is included or discarded (Jesson 2011).

The criteria for including and excluding research papers are the following:

Included:

- Paper is doctoral thesis at least
- Is an academic paper
- Published latest in a year 2000
- Published in English or Finnish
- Paper and its publishing platform is free to use
- Is a patent model
- Paper is result of research done by major IT-company
- Paper has clear and scientific research method in use
- Discuses mobile banking security architecture or its design
- Discuses mobile banking security solutions

Excluded:

- Thesis is written by lesser academic than doctoral student
- Has not gone through academic publication process
- Is published in other language than English or Finnish
- Paper is only accessible by paying a fee of any amount
- Paper is not done with valid research method
- Published before year 2000
- Is not research model or a patent
- Papers that do not discuss about architectural design or components of mobile banking

The reason for setting publishing year limit to year 2000 is motivated by paper published by Florian Moser (2015) where points out that in the year 2000 only 8 % of consumers used mobile banking(Moser, 2015). It could be argued that no significant research towards mobile banking security architecture has been done before that. Articles that are included into this research are academic and peer-reviewed papers. Academic and peer-reviewed paper are checked and challenged before publication thus making them more reliable (Jesson, 2011).

Since this research doesn't have any funding, academic papers, which requires payment fee of any amount, will not be used in this research. Patents and company based research is also included to get make sure that this research takes commercial point of view into consideration. However, each paper or model need to be properly researched with open methods, which justify the reasoning for the model.

3.4.2 Research Material gathering and critical assessment of search

The search term is generated by focusing on the research question and finding the key terms (Jesson 2011). The key words in this case are 'mobile banking' paired up with 'security architecture' or 'security design'. Use of quote marks unify search term making it possible to search whole sentences (Google Search Help 2017). Because online data bases are used search terms when using google scholar are modified by using Google's search operators which follow boolean operators which string together more sophisticated search results with just using one search instead of multiple searches (Google Vault 2017). The table 3 list below shows how searches were constructed for each online database.

TABLE 3 Search phrases

Source	**Search phrase**
Google Scholar	"mobile banking" AND "security architecture" OR "security design"
IEEE Xplore	"mobile banking" AND "security architecture" OR "security design" OR security
Researchgate.net	"mobile bank security"; "mobile bank architecture"
Web of Science	mobile banking security OR mobile banking architecture

Elsevier	mobile banking OR mobile banking architecture

3.4.3 Research Material analysis: Narrative Synthesis

The most important part and the essence of research is analysing, interpreting and making conclusion out of the research material. This is what all research aims to do since it provides possible answers to research question (Hirsjärvi, 2009). The following chapter describes each of these three steps.

Analysis in its essence, means that the researcher takes the gathered material and does the following: describes the material, categorises it in justified manner, combines it. These steps make it possible come into research conclusion (Hirsjärvi, 2009). Analysis can be done in two different goals:

- To explain the material: This method is commonly used in quantitative research by using statistical tools.
- To understand the material: This one is used more often in qualitative research and aims to provide conclusion about the material to find common factors (Hirsjärvi, 2009)

When all the previous steps of the analyses are done, the results received from analysed material should be interpreted by the researcher for the readers. In this context interpreting means that the researcher discusses the conclusion he or she can make based on the interpretation of the analysed material. The conclusion should be the answer to the research questions. In case where no definitive answer can be drawn from the material, the conclusion informs the reader about it. (Hirsjärvi, 2009)

In systematic literature review, making synthesis out of the analysed material is the same as making a conclusion. Jesson (2011) defines synthesis as 'the act of making connections between parts. It's not simply mater of re-assembling them back into original order but finding new order'. This basically means that the researcher should make a justified interpretation from the analysed material, which would provide new knowledge or point out lack of knowledge in current research (Jesson, 2011).

All previous statements considered, it should be noted that one of the factors that affect analysis and interpretation of the research material is the chosen research topic and the goal of the research (Hirsjärvi, 2009). In this research, the goal is to identify the current state and understanding of mobile banking architecture and because of that literature review is suitable way to identify current academic understanding on elements of mobile banking architecture, which will be later compared with new demands of PSD2.

4 Results

This chapter functions as a report of the research material gathering process and what themes were found from selected articles. The chapter also includes comparison of PSD2 security requirements with the themes found from selected literature.

4.1 Description of Research Material Gathering

Research material was gathered by using online databases, which included all the sources, which were accessible and free to use by students of University of Jyväskylä or are free to use by registration to service. Used data bases are listed in chapter 3.4.2. Naturally, the list is not comprehensive since the main library of University of Jyväskylä does not keep comprehensive records of research article databases they have in use and because of it, Google Scholar search engine became a necessity.

In all database searches, advanced search methods were used to limit the number of search results as much as possible to relevant research papers. This also eliminated the risk of checking the same results with different searches from database. All but one database had advanced search option to limit the search results except Researchgate. In its case, separate searches were used and examined to get the relevant search results.

Search results had to be checked manually to make sure that only the relevant research papers were downloaded. The manual exclusion and inclusion was based on predefined criteria established in chapter 3.4.1, which were followed during the elimination process. The first round of elimination process was to check relevance of each search result based on the title and the abstract. Before the first elimination round, the total number of search results of all databases were 784 articles. From those articles, 42 papers remained. The second elimination round was based on speed reading the articles to gain general understanding of its content. The purpose of this was to eliminate those papers

where the relevance of the paper was not certain during the first elimination. The second elimination round left 22 papers to use for this research. Table 2 below lists number of search results from each database. Attachment 2 shows the list of chosen papers after both elimination rounds. List of chosen literature is in annex 2.

Source	**Hits**	Notes
Google Scholar	582	
Researchgate.net	13	
Web of Science	167	
Elsevier	22	
Total	784	
1. elimination	42	Based on the abstract and the title
2. elimination	22	Based on fast reading

4.2 Material synthesis

This section presents results of the systematic literature review. The first chapter explains the ideas literature has proposed to conduct secure mobile banking. These themes are used for making the comparison between the PSD2 and academic models of mobile banking.

4.2.1 Themes found from literature

Academic research about the ways creating security for mobile banking focuses on guaranteeing customer authentication and ensure validity of messages going between bank and customer. All the papers emphasize the importance of encryption in wireless communication between mobile device and customer's bank. The ways to secure banking session varied and following explains the themes of securing mobile banking.

Theme 1: Preference to asymmetric encryption against symmetric. Public Key Infrastructure(PKI) was suggested the most out of the papers, five time in total. PKI is an asymmetric encryption method where messaging parties have a public and a private key. Public key is used to send encrypted messages to its owner. This means that anyone can have the public key. Secret key is used to decrypt the messages. This eliminates the risk of exposure present in symmetric encryptions where each communication party needs to have the same secret key. Beauty of PKI is that the secret key can be used to sign messages that can be verified with the public key. If any information is altered in the messages, the value of signature changes. This ensures integrity of communication and prevents man-in-the-middle attacks (Schuba and Wrona, 2002; Narendiran, Rabara and Rajendran, 2009; Rice and Zhu, 2009; AL-Akhras *et al.*, 2011; Ray, Biswas

and Dasgupta, 2016). Symmetric encryption was suggested in java application demonstration (Itani and Kayssi, 2004).

Theme 2: Use of PKI without certificates. The significance of certificate-less cryptography is that it uses much less key pairs. The problem of PKI is the distribution and generation of key when number of users grow significantly. This can be solved by not giving users their own keypair. Instead, user requests to use the public key of the bank. The user's banking application generates a symmetric session key and sends it to the bank along with a random number. The random number is then signed by the bank with its private key. When a new secure communication channel is established the user checks the signature for authenticity. This method saves number of keys and offers equal level of protection. (Hassouna *et al.*, 2013; Thakur, 2015)

T**heme 3: Use of smartcards or SIM-cards for encryption.** The point to use these is to create an isolated environment from the smartphones system to improve security. The SIM or smartcard would contain encryption keys and the program in the microchip would take care of communication and verification between client and bank. Using this method would protect the encryption keys in situation where banking application is compromised (Ngo *et al.*, 2011; Weerashinge, Rakocevic and Muttukrishnan, 2012; Saka, Sadikin and Windarta, 2017). Interesting fact from the research material is that SIM-card is suggested only in one security architecture where mobile phone operator is in a central role for authenticating the user.(Weerashinge, Rakocevic and Muttukrishnan, 2012)

Theme 4: A little use of biometrics. In chapter 3.1 it was noted that some papers suggested that use of biometrics would be the key solution for strong customer authentication. However, according to the literature review conducted in this thesis it is not that popular method since only 3 security architectures suggest this. In these papers biometrics are used to give additional authentication. Biometrics in these security architectures are used by making a hash value out of biometric sample like fingerprint or iris. (Ngo *et al.*, 2011; Ray, Biswas and Dasgupta, 2016; Saka, Sadikin and Windarta, 2017)

Theme 5: Use of established credit card system. Three papers suggest that mobile payments could be done simply by integrating credit card into mobile phone. This would allow the use of established credit card system supported by Europay, Mastercard and Visa. This system is called EMV. In EMV model a merchant would possess a device to read credit cards, which is called Point of Sale (POS). When credit card is integrated into mobile phone the POS can be used. Security architecture is adapted from EMV model. However, this model only allows payments to merchants and does not support banking features. (Olanrewaju *et al.*, no date; Yang, 2014) Except for one mobile payment scheme where each mobile phone also acts as a POS by using Bluetooth for communication. This would allow money transfers person to person. (Martínez-Peláez *et al.*, 2015)

Theme 6: Separate authentication medium: Two papers suggest using a separate authentication medium for security. The Chines paper suggest that

mobile banking could be done by using the so-called e-key, which is a separate device and its purpose is to encrypt the messages between the client phone and the bank server. The e-key is used as module, which could communicate with banking application in the phone. E-key would contain encryption keys necessary to authenticate users and ensure the integrity of communication. (Wan, Yin and Sun, 2009) The Indian research paper suggest use of code sheet, which would contain separate authentication codes. These codes are mixed with a PIN-code of the user, which offers protection in case if code sheet is stolen from the user. The model is an improvement of earlier embellished mobile banking scheme in India.(Thakur, 2015)

Theme 7: effort to enhance authentication systems. The **r**est of the papers offer solutions to improve passwords or add other authentication schemes along with the password. Location based authentication adds element where the payment can only be conducted if the location of phone matches to location of payment This works when payment needs to be done near the POS. The scheme would also use location probability similar what banks use. (Prasad and Aithal, 2017) research paper by Ku (2013) present a graphical one-time password system where the password is based on pictures. Basically, the pictures present ASCII digits. The user would only need to remember the pictures and find them from random pallet where digit behind the pictures changes.(Ku *et al.*, 2013) Lee's (2005) paper suggest using a dynamic authentication system to enhance password. The Dynamic system is based on constantly changing values behind the cells. (Lee and Park, 2005) One paper suggests banking scheme which would allow anonymity of payments using bind signed certificates and secure wireless payment protocol. This requires also anonymous bank account. (Layeghian Javan and Ghaemi Bafghi, 2014) Scheme is not usable due to PSD22 requirements to identify payer and payee.

4.2.2 Comparison with PSD2

In this research, none of the research papers suggests a model where the bank opens its application programming interface (API) like PSD2 mandates. Therefore, it is clear that no security architecture, suggested in the academic papers, is designed in a way where mobile banking application is separate from security mechanisms. In all cases, banking application is provided by the bank itself. Picture 3 illustrates main security functions. Detailed security functions are explained in annex 1.

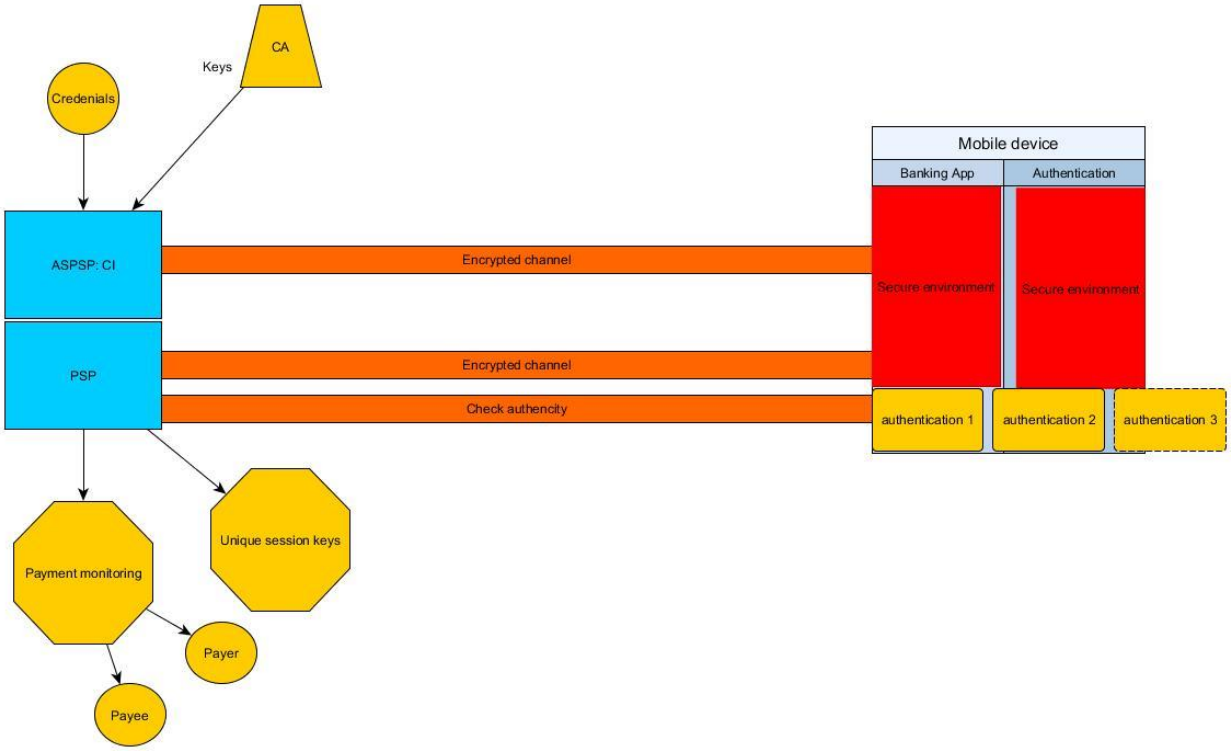

FIGURE 3 PSD2 Security Architecture

ASPSP (Account Service Payment Service Provider) is also PSP (Payment Service Provider) but the difference is that ASPSP provides Payment Service User's (PSU) bank account. The only difference between ASPSP and PSP is the customer relationship. This means that both have the similar functions, but these functions are separated in PSD2 directive. Therefore, security architecture presented here has them both separated. The idea is that ASPSP provides a communication interface where bank's API calls the authentication function. ASPSP needs to take care of encryption between all the parties involved in the transaction. The encryption keys are provided by known Certification Authority (CA) and needs to use proven encryption method. PSP must monitor all the transaction, and this requires knowing the payer, payee, time of transaction and amount. PSP needs to make sure that all the transaction sessions are protected with a unique key of the transaction in question. This requirement is made to make sure that no transaction can be done based on knowledge of previous transaction and their encryption keys. PSP is responsible for checking authenticity of the strong customer authentication medium. For example, if authentication to banking service requires use of randomly generated number used once (nonce), PSP needs to have a way to check that the nonce generator has not been compromised.

The mobile device that hosts the banking application needs to run the application in a 'secure execution environment' within the system. The idea is that compromising authentication will not affect banking application and vice versa. It should be noted that there is no current industry definition for 'secure execu-

tion environment'. However, PSD2 is written in vague manner on purpose to give room for new innovations to the mobile payments. Mobile banking needs to have at least two authentication methods but three is also possible. These authentication methods must be based on either on knowledge, possession or inherence.

Reflecting the current research on the mobile banking security to demands of PSD2, the biggest cap is the centralized responsibility of banks to take care of the security. The application developer just needs to use the API of the bank. PKI-system based solution presented in the academic papers could be used as they are to secure mobile banking. PKI provides opportunity to use encryption and signatures to make ensure security and integrity. PKI systems presented in papers also have considered ways to make transaction unique and traceable with random number generation, which would fit into PSD2 requirements presented in RTS article 26 and 30. If key distribution is considered a problem research has shown that mobile banking can be conducted without certificates without losing ability to create uniquely encrypted transactions. Academic research also provides ideas to use passwords and biometrics to further enhance the security. PKI based system would allow banks to use signatures to their authentication application to make sure their integrity. PSD2 requires through RTS article 29 to use 'qualified certificates and electronic seals', which makes use of PKI systems valid option.

Academic research papers do not provide solution on maintaining secure communication of strong customer authentication and the separate banking application, developed by a third party. PSD2 creates a unique situation where security features and the responsibility of transaction security are separated from the banking application. However, PSD2 attempts to fight this risk by demanding in article 97 to use strong customer authentication. Research papers used in this thesis does not offer security architecture model where authentication methods are designed to be separate from the banking application.

5 Conclusion

The conclusion of the thesis presents summary of the results and evaluates how the research related to PSD2 security architecture could be continued. The writer also presents critical evaluation of the whole research including the theoretical background, the use of research method and the results.

5.1 Conclusion of the research results

Chapter 4 presented 22 research articles about the security architecture of mobile banking and categorised major themes based on what technologies these security architectures relied on. The research discovered that the academic security architecture models that use PKI or certificateless asymmetric encryption could provide security for mobile banking in terms of authenticity, integrity and non-reputability, which are one of the core features that PSD2 demands in terms of achieving strong customer authentication. Academic research also provides some models to use innovative password systems such as dynamic passwords and even introduces model, which uses biometrics.

None of the papers used in this thesis provided model where security features of mobile banking are separate function, only imbedded into mobile banking application via API. This is raises questions about the security since academic paper don't discuss how the strong customer authentication elements can be made independent from each other and how to make sure that compromising one authentication element wouldn't affect the mobile banking application itself or the other authentication elements. Overall authentication and security methods used in these academic models could be used effectively as part of the security architecture of mobile banking.

It should be noted that PSD2 changes security design of mobile banking systems in to list-based security design introduced in chapter 2.1. List-based security design doesn't encourage innovation due to external pressure to be compliant with security check list now imposed by PSD2.

5.2 Evaluation of the research

Systematic literature review was chosen for this research to obtain understanding of the status of academic research on the security architecture of mobile banking. Finding the current state will make it possible to evaluate the suitability of research security architecture models. The aim was to see possible cap between the research and the demands of PSD2 and its regulatory technical standard (RTS).

Conducting the research as a systematic literature review gives the research process transparency, which enables evaluate the process. The other reason to use systematic method was to ensure that as many relevant articles as possible were found. This compensated lack of previous knowledge of the writer about the subject. Systematic literature review is demanding in terms of how much material needs to be read to find relevant papers.

There is no denying that there is possibility of error when one person is going through over 700 papers. The risk of error was minimized by making clear criteria for exclusion and inclusion. Pre-determined methods of including and excluding papers in latter states made finding correct papers as precise as humanly possible. The most limiting factor on finding suitable research was access to papers that required payment access. Some databases were not available for the writer.

Theoretical background contributed well in terms of understanding the subject. The structure of theory chapter provided information about security architecture and design. In addition, the chapter discussed how mobile networks work and explains the development of mobile banking. Theory chapter also contributed to the security threats and features of smartphones. The most important part of the theory chapter introduced the security demands of PSD2 giving basis to do the comparison between the academic literature and the directive. The demands were categorised in clear manner and included as an annex to the thesis.

The research result gave a clear overview about how the current academically created security architectures could support PSD2 security demands. In addition, the results point out aspects of security demands of PSD2 where academic security architecture models don't provide the answer. Considering factors presented in this chapter it can be said that the research was successful in reaching its goal to find cap between academic research and security demands of PSD2. This thesis offers an overview of security technologies that can be used to achieve compliance with security demands of PSD2. However, it should be noted that the Technical Regulatory Standard of PSD2 is in its final draft and its possible that changes will come to RTS.

5.3 Future research

The future research related to PSD2 could focus on security threats against strong authentication and how this separated model where security is based on only API could be vulnerable. Haupert and Müller published a paper in 2016 where they demonstrated that separate authentication application can be compromised. The paper points out that since the separation of authentication application and banking application in same device is based on sandboxing. This sandboxing can be broken with jailbreak tools. This give attacker access to the root of the system allowing unwanted interaction of the applications. Paper demonstrates that compromising the authentication application breaks the encryption and compromises the transactions (Haupert and Müller, 2016).

The other thing to research in perspective of the directive is the question what can be counted as strong customer authentication precisely. This is however, question of how law is interpreted. The research should focus on creating stronger authentication schemes and evaluate current ones to find possible flaw in algorithms or protocols themselves.

SOURCES

Doing Your Literature Review: Traditional and Systematic Techniques. (Jesson 2011, Sages publications Ltd, London)

AL-Akhras, M. T. *et al.* (2011) 'Innovative Secure Mobile Banking Services', *International Journal of Interactive Mobile Technologies (iJIM)*, 5(1), pp. 12–22. doi: 10.3991/ijim.v5i1.1516.

Amer, S. H. *et al.* (2008) 'Understanding Security Architecture', *Proceedings of SpringSim 2008*, pp. 335–342. doi: 10.1145/1400549.1400596.

Armour, F. J., Kaisler, S. H. and Liu, S. Y. (1999) 'A Big-Picture Look at Enterprise Architectures', *IT Professional*, 1(1), pp. 35–42. doi: 10.1109/6294.774792.

Baskerville, R. (1993) 'Information systems security design methods: implications for information systems development', *ACM Comput. Surv.*, 25(4), pp. 375–414. doi: 10.1145/162124.162127.

Chang, Y., Chen, J. and Tseng, W. (2005) 'A Mobile Commerce Framework Based on Web Services Architecture', *IEEE Computer Society*.

Cook, S. (2017) 'Selfie banking: is it a reality?', *Biometric Technology Today*. Elsevier Ltd, 2017(3), pp. 9–11. doi: 10.1016/S0969-4765(17)30056-5.

Dewan, S. M. (2010) 'Past , Present and Future of M-Banking Research : A Literature Review', *Association for Information Systems*, (21st Australasian Conference on Information Systems).

EBA (2017) 'Final Draft RTS on SCA', 2366(23 February 2017), pp. 1–153.

Eloff, J. H. P. and Eloff, M. M. (2005) 'Information security architecture', *Computer Fraud & Security*, 2005(11), pp. 10–16. doi: 10.1016/S1361-3723(05)70275-X.

Eneck, W., Machigar, O. and McDaniel, P. (2009) 'Understanding Android Security', *IEEE Security & Privacy*, pp. 51–78. doi: 10.1109/MSP.2009.26.

European Parliament (2015) 'Directive 2015/2366 (Payment Service Directive 2)', *Official Journal of the European Union*, L 337/35(260), pp. 35–127.

Farooqui, Kazi; Logrippo, Luigi; de Meer, J. (1995) 'The ISO Reference Model of Open Distributed Processing: an introduction', 27(Computer networks ans ISDN systems), pp. 1215–1229.

Flynn, L. and Klieber, W. (2015) 'Smartphone Security', *IEEE Pervasive Computing*, 14(4), pp. 16–21. doi: 10.1109/MPRV.2015.67.

Goethals, F. *et al.* (2006) 'An Overview of Enterprise Architecture Framework Deliverables', *SSRN eLibrary*, pp. 1–20. doi: 10.2139/ssrn.870207.

Grandry, E., Feltus, C. and Dubois, E. (2013) 'Conceptual Integration of Enterprise Architecture Management and Security Risk Management', *Enterprise Distributed Object Computing Conference Workshops (EDOCW), 2013 17th IEEE International*, pp. 114–123. doi: 10.1109/EDOCW.2013.19.

Hassouna, M. *et al.* (2013) 'An End-to-End Secure Mail System Based on Certificateless Cryptography in the Standard Security Model', 10(2), pp. 264–

271. doi: 10.5120/12910-9890.

Haupert, V. and Müller, T. (2016) 'On App-based Matrix Code Authentication in Online Banking'. Available at: https://ww1.cs.fau.de/appAuth.

Hensel, V., Lemke-rust, K. and Augustin, S. (2010) 'On an Integration of an Information Security Management System into an Enterprise Architecture', *Workshop on Database and Expert Systems Applications (DEXA), 2010*, pp. 354–358. doi: 10.1109/DEXA.2010.75.

Hung, T. (2017) 'Shifting shape of banking biometrics', *Biometric Technology Today*. Elsevier Ltd, 2017(4), pp. 5–8. doi: 10.1016/S0969-4765(17)30073-5.

Itani, W. and Kayssi, A. (2004) 'J2ME application-layer end-to-end security for m-commerce', *Journal of Network and Computer Applications*, 27(1), pp. 13–32. doi: 10.1016/S1084-8045(03)00030-4.

Jeon, W. *et al.* (2011) 'A Practical Analysis of Smartphone Security', *Human Interface anf the Management of Information*, pp. 311–320.

Karyda, M., Kokolakis, S. and Kiountouzis, E. (2001) 'Redefining information systems security: viable information systems', *Proceedings of the 16th international conference on Information security: Trusted information: the new decade challenge*, (October 2016), pp. 453–468. Available at: http://portal.acm.org/citation.cfm?id=512350.510799%5Cnhttp://portal.acm.org/citation.cfm?id=510799.

Kieseberg, P. *et al.* (2015) 'Security Tests for Mobile Applications - Why using TLS / SSL is not enough .', (Asqt), pp. 2–3. doi: 10.1109/ICSTW.2015.7107416.

Kruchten, P. (1995) 'The 4+ 1 view model of architecture', *Software, IEEE*, November 1(November), p. 9. doi: 10.1109/52.469759.

Ku, Y. *et al.* (2013) 'Two-factor authentication system based on extended OTP mechanism', *International Journal of Computer Mathematics*, 90(12), pp. 2515–2529. doi: 10.1080/00207160.2012.748901.

Layeghian Javan, S. and Ghaemi Bafghi, A. (2014) 'An anonymous mobile payment protocol based on SWPP', *Electronic Commerce Research*, 14(4), pp. 635–660. doi: 10.1007/s10660-014-9151-6.

Lee, S. and Park, S. (2005) 'Mobile Password System for Enhancing Usability-Guaranteed Security in Mobile Phone Banking'. Springer-Verlag Berlin Heidelberg, pp. 66–74.

Mallat, N., Rossi, M. and Tuunainen, K. (2004) 'Mobile Banking Services', *Communications of the ACM*, 47(5), pp. 42–46. doi: 10.1145/986213.986236.

Mansfield-Devine, S. (2016) 'Open banking: opportunity and danger', *Computer Fraud and Security*. Elseveir Ltd, 2016(10), pp. 8–13. doi: 10.1016/S1361-3723(16)30080-X.

Martínez-Peláez, R. *et al.* (2015) 'P2PM-pay: Person to Person Mobile Payment Scheme Controlled by Expiration Date', *Wireless Personal Communications*, 85(1), pp. 289–304. doi: 10.1007/s11277-015-2738-y.

Moser, F. (2015) 'Mobile Banking', *International Journal of Bank Marketing*, 33(2), pp. 162–177. doi: 10.1057/9781137386564.

Narendiran, C., Rabara, S. A. and Rajendran, N. (2009) 'Public key infrastructure for mobile banking security', *2009 Global Mobile Congress*, pp. 1–6. doi: 10.1109/GMC.2009.5295898.

Ngo, H. H. *et al.* (2011) 'Formal verification of a secure mobile banking protocol', *Communications in Computer and Information Science*, 132 CCIS(PART 2), pp. 410–421. doi: 10.1007/978-3-642-17878-8_42.

Olanrewaju, T. *et al.* (no date) 'Security modeling of mobile payment system architecture'.

Ongtang, M. *et al.* (2012) 'Semantically rich application-centric security in Android', *Security and Communication Networks*, 5(6), pp. 658–673. doi: 10.1002/sec.360.

Peterson, G. (2007) 'Security Architecture Blueprint', *Business*, pp. 1–12. doi: 10.1007/s11859-006-0126-x.

Prasad, K. K. and Aithal, P. S. (2017) 'A Study on Enhancing Mobile Banking Services using Location based Authentication A Study on Enhancing Mobile Banking Services using Location based Authentication', X(X), pp. 48–58. doi: 10.5281/zenodo.583230.

Ray, S., Biswas, G. P. and Dasgupta, M. (2016) 'Secure Multi-Purpose Mobile-Banking Using Elliptic Curve Cryptography', *Wireless Personal Communications*. Springer US, 90(3), pp. 1331–1354. doi: 10.1007/s11277-016-3393-7.

Rice, J. E. and Zhu, Y. (2009) 'A proposed architecture for secure two-party mobile payment', *IEEE Pacific RIM Conference on Communications, Computers, and Signal Processing - Proceedings*, pp. 88–93. doi: 10.1109/PACRIM.2009.5291393.

Saka, K. P. D., Sadikin, M. A. and Windarta, S. (2017) 'S-Mbank: Secure Mobile Banking Authentication Scheme Using Signcryption, Pair Based Text Authentication, and Contactless Smartcard', (August).

Schuba, M. and Wrona, K. (2002) 'Security for Mobile Commerce Applications'.

Siponen, M. (2006) 'Secure-System Design Methods : Evolution and Future Directions', *IT Professional*, 8(3), pp. 40–44. doi: 10.1109/MITP.2006.73.

Siponen, M., Baskerville, R. and Heikka, J. (2006) 'A Design Theory for Secure Information Systems Design Methods', *Journal of the Association for Information Systems*, 7(11), pp. 725–770. doi: Article.

Siponen, M. T. (2005) 'Analysis of modern IS security development approaches: Towards the next generation of social and adaptable ISS methods', *Information and Organization*, 15(4), pp. 339–375. doi: 10.1016/j.infoandorg.2004.11.001.

Soley, R. and OMG Staff Strategy Gropu (2000) 'Model driven architecture', *OMG white paper*, (April), pp. 1–12. Available at: http://elrond.tud.ttu.ee/material/enn/IDY0201/Lecture2/00-11-05.pdf.

Soni, D., Nord, R. L. and Hofmeister, C. (1995) 'Software Architecture in Industrial Applications', *Proceedings ICSE '95*, pp. 196–207.

Thakur, T. (2015) 'Mobile Banking System based on certificateless Chameleon Hash Function', 121(7), pp. 1–5. doi: 10.5120/21549-4543.

Urbaczewski, L. and Mrdalj, S. (2006) 'A comparison of enterprise architecture frameworks', *Issues in Information Systems*, 7(2), pp. 18–23. doi: 10.1227/01.neu.0000410082.42657.aa.

Walls, J. G. *et al.* (2004) 'Assessing Information System Design Theory in Perspective : How Useful W'.

Wan, Z., Yin, W. and Sun, R. (2009) 'Design and implementation mobile payment based on multi-interface of mobile terminal', *WSEAS Transactions on Computers*, 8(1), pp. 93–102.

Wang, Y., Streff, K. and Raman, S. (2012) 'Smartphone Security Challenges', *Computer*, 45(12), pp. 52–58. doi: 10.1109/MC.2012.288.

Weerashinge, D., Rakocevic, V. and Muttukrishnan, R. (2012) 'Security Framework for Mobile Banking'. London: Atlantais Ambient and Pervasive Intelligence: Truestworthy Ubiquitous Computing, pp. 79–98. doi: 10.2991/978-94-91216-71-8.

Yang, M. H. (2014) 'Security enhanced emv-based mobile payment protocol', *Scientific World Journal*, 2014. doi: 10.1155/2014/864571.

Zachman, J. A. (1987) 'A Framework for Information Systems Architecture', *IBM Systmes Journal*, 26(3), pp. 454–470. doi: 10.1147/sj.263.0276.

Zheng, X., Pan, L. and Yilmaz, E. (2017) 'Security analysis of modern mission critical android mobile applications', *Proceedings of the Australasian Computer Science Week Multiconference on - ACSW '17*, (January), pp. 1–9. doi: 10.1145/3014812.3014814.

Price Water Coopers. Catalyst or threat? The strategic implications of PSD2 for Europe's banks retrieved 14.8.2017 from https://www.strategyand.pwc.com/media/file/Catalyst-or-threat.pdf

McKinsey. Technology innovations driving change in transactions banking. Retrieved 14.8.2017 from http://www.mckinsey.com/industries/financial-services/our-insights/technology-innovations-driving-change-in-transaction-banking

Accenture. Seizing the opportunities unlocked by the EU's revised payment service directive. Retrieved 14.8.2017 from https://www.accenture.com/t20160831T035645Z__w__/us-en/_acnmedia/PDF-19/Accenture-Banking-Opportunities-EU-PSD2-v2.pdf#zoom=50

White House President Obama Archive. Federal Enterprise Architecture Framework. Retrieved 17.08.2017 from https://obamawhitehouse.archives.gov/sites/default/files/omb/assets/egov_docs/fea_v2.pdf

US Department of Defense. Department of Defense Architectural Framework. Retrieved 17.08.2017 from http://dodcio.defense.gov/Portals/0/Documents/DODAF/DoDAF_v2-02_web.pdf

The Open Group. Federal Enterprise Architecture Framework (FEAF). Retrieved 17.08.2017 from

http://www.opengroup.org/architecture/0210can/togaf8/doc-review/togaf8cr/c/p4/others/others.htm#FEAF

Google Incorporated. Android Security white paper. Retrieved 31.8.2017 from https://static.googleusercontent.com/media/enterprise.google.com/en//android/static/files/android-for-work-security-white-paper.pdf

Apple Incorporated. iOS Security iOS 10. Retrieved 30.8.2017 from https://www.apple.com/business/docs/iOS_Security_Guide.pdf

The European Union. EU law. Retrieved 4.9.2017 from https://europa.eu/european-union/eu-law/decision-making/procedures_en

Google Vault: Using search operators. Retrieved 18.9.2017 from https://support.google.com/vault/answer/2474474?hl=en

Google Search Help: Refine web search. Retrieved 18.9.2017 from https://support.google.com/websearch/answer/2466433?hl=en

ANNEX 1 DEMANDS OF PSD2

Requirement	Responsible
Strong Customer Authentication - 2 or more authentication elements - Elements are independent - Elements are unforgeable - Max 5 consecutive login attempts - Account locked or terminated - Less than 5min of inactivity after login - Element knowledge is protected from unwanted disclosure - Element possession cannot be replicated - Element inherence is protected by device and software	PSP
Dynamic Linking - Payer is aware of payee before transaction; - Authentication code is unique to transaction amount - Any change to paragraphs will change the authentication code	PSP
Monitoring - Transactions from payment instruments are monitored - Remote and non-remote payments are separated - Exemption transactions are monitored - Stored at least 90 days - Available for authorities	PSP
Confidentiality and integrity of the payment service users' personalized security credentials - Security credentials are masked during PSU's input; - Security credentials are not stored in plaintext - Secret cryptographic material is protected from unwanted disclosure - Encryption process and management is documented - Credentials are created in secure envi-	PSP

ronment - Association of credentials to PSU is done in secure environment - Association via remote payment channel to PSU is done by using SCA or with personalized security credentials and authentication device - Credentials are delivered in secure manner - Authenticity of authorization software is verified - Delivered credentials and authentication medium is activated by PSU - Reactivation and renewal follows same procedure as creation - Credentials Destroyed in secure manner - Authentication device or software reuse needs to be secure - PSP holds a database of revoked credentials	
Secure Communication - Identify payer and payee - Communication and transactions need to be traceable	PSP
Specifics of Secure communication - Provide Communication Interface - Communication interface offers secure communication to PISP Follow communication standards of European or international organisations - Offer openly interface documentation - PSPs need to use qualified electronic certificates - Communication is secured using known encryption method - Open session is terminated as soon as possible - Communication interface needs to be connected securely when multiple parties involved - Staff shouldn't be able to read credentials. se	ASPSP

Security and operational risk management - Framework to show to authorities - Provided in annual basis - Incident management procedures - Identification of major operational and security incidents	PSP

ANNEX 2 LIST OF CHOSEN ARTICLES

Title	Author
Security modeling of mobile payment system architecture	Temitope Olanrewaju, Pavol Zavarsky, Ron Ruhl, Dale Lindskog
Security Framework for mobile banking	Dasun Weerasinghe
A Proposed Architecture for Secure Two-party mobile payment	J.E. rice
Innovative Secure Mobile banking service	Mousa Al-Akhras
Public key infrastructure for mobile banking security	Narendiran, C
A Secure Mobile Banking Scheme based on Certificateless Cryptography in the Standard Security Model	Eihab Bashier Mohammed Bashier Faculty
Security for Mobile Commerce Applications	MARKO SCHUBA, KONRAD WRONA
Design and Implementation Mobile Payment Based on Multi-Interface of Mobile Terminal	ZHONG WAN WEIFENG YIN RONGGAO SUN
Mobile Banking System based on certificateless Chameleon Hash Function	Tejeshwari
Formal Verification of a Secure Mobile Banking Protocol	Huy Hoang Ngo, Osama Dandash, Phu Dung Le, Bala Srinivasan, and Campbell Wilson
Useable Secure, Low-Cost Authentication for Mobile Banking	Saurabh Panjwani, Edward Cutrell
The missing link: Human Interactive Security Protocols in mobile payment	Chen Bangdao, A.W.Roscoe, Ronald Kainda, L.H. Nguyen
S-Mbank: Secure Mobile Banking Authentication Scheme Using Signcryption, Pair Based Text Authentication	Dea Saka Kurnia Putra
Secure Multi-Purpose Mobile-Banking Using Elliptic Curve Cryptography	Sangram Ray
A Study on Enhancing Mobile Banking Services using Location based Authentication	Sreeramana Aithal Srinivas
An anonymous mobile payment protocol based on SWPP	Samaneh Layeghian Javan
Two-factor authentication system based on extended OTP mechanism	Yunlim Ku, Okkyung Choi
A secure end-to-end SMS-based mobile banking protocol	Sriramulu Bojjagani
Mobile Password System for Enhancing Usability-Gurtanteed Security in Mobile Phone Banking	SangJun Lee
J2ME application-layer end-to-end security for m-commerce	Wassim Itani

Security Enhanced EMV-Based Mobile Payment Protocol	Ming-Hour Yang
P2PM-pay: Person to Person Mobile Payment Scheme Controlled by Expiration Date	Rafael Martı ´nez-Pela ´ez