LEGAL MEASURES ON AUTHENTICATION OF ELECTRONIC FUND TRANSFER

BY
MR.WATTHANON KITBUNCHA

AN INDEPENDENT STUDY PAPER SUBMITTED IN
PARTIAL FULFILLMENT OF THE REQUIREMENTS
FOR THE DEGREE OF MASTER OF LAWS
(BUSINESS LAW)

GRADUATE SCHOOL OF LAW
ASSUMPTION UNIVERSITY

JULY 2017

LEGAL MEASURES ON AUTHENTICATION OF ELECTRONIC FUND TRANSFER

BY

MR.WATTHANON KITBUNCHA

AN INDEPENDENT STUDY PAPER SUBMITTED IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE DEGREE OF MASTER OF LAWS (BUSINESS LAW)

GRADUATE SCHOOL OF LAW

ASSUMPTION UNIVERSITY

JULY 2017

Independent Study Paper Title : Legal Measure on Authentication of Electronic Fund Transfer

Author : Mr.Watthanon Kitbuncha

Major : Master of Laws (Business Law)

Advisor : Assoc.Prof.Nattapong Posakabutra

Faculty of Law, Assumption University approves this Independent Study Paper as the partial fulfillment of the requirement for the Degree of Master of Laws.

..... Dean, Faculty of Law

(Assoc.Prof. Pornchai Soonthornpan)

Committee:

..... Chairman

(Prof.Suchart Thammapitagkul)

..... Committee

(Mr.Pruettipong Srimachand)

..... Advisor and Committee

(Assoc.Prof.Nattapong Posakabutra)

Independent Study Paper Title : Legal Measure on Authentication of Electronic Fund Transfer

Author Mr.Watthanon Kitbuncha

Major Master of Laws (Business Law)

Advisor Assoc.Prof.Nattapong Posakabutra

ABSTRACT

The objective of this Independent Study is to learn the problems of concerning authentication of the electronic fund transfer and to suggest the solutions to strengthen authentication methods in the electronic fund transfer and to resolve the problems.

It was found that the authentication has the technical process to verify the authenticity of the users before they made the transactions and it has not yet had the specific provisions to determine the requirement measures for the authentication in the electronic fund transfer. In the EU' Directive, it has taken the technical process of authentication to the form of regulations, which they called the Strong Customer Authentication. It is the using of two or more authentication factors together and it was obeyed to use when the users have used the electronic payments. Although, we do not have the Strong Customer Authentication but we have Section 9 and 25 of the Electronic Transaction Act B.E. 2544.

In these Section, it has been described about the reliable method which is capable of identifying the signatory and indicating that the signatory has been approved the information which contained in such data message as being his own. And, that method can prevent the confidentiality, integrity and availability of electronic information and also prevent non-repudiation between parties and also is used with all electronic transactions. Practically, our bankers have already used the concept of Strong Customer Authentication for their electronic fund transfer.

Meanwhile, it is not essential to have the specific regulation concerning authentication of the electronic fund transfer but the EU Directive could be used as the good guideline to develop the regulation concerning authentication of the

---

European Union.

electronic fund transfer in the future and the bankers shall try to bring the biometric information and selfie as one of their authentication mechanisms.

This article is compiled from the Independent Study Paper, "The Legal Measure on Authentication of Electronic Fund Transfer," submitted in partial fulfillment for the degree of Master of Laws (Business Law program) Graduate School of Law, Assumption University, 2017.

ACKNOWLEDGEMENT

I would like to express my sincere thankful to my independent study advisor, Assoc.Prof.Nattapong Posakabutra for his invaluable help and constant encouragement throughout the course of my research on the topic of Legal Measures on Authentification of Electronic Fund Transfer. I am most grateful for his teaching and advice, not only the research methodologies process but also many other methodologies in life for living. I would not have achieved this so far and this Independent Study would not have been completed without all the supports that I have always received from him.

Furthermore, I am grateful for the very well teaching, advising and helping of Prof.Suchart Dhammapitakkul, Mr.Pruettipong Srimachand, Assistant Governor of Bank of Thailand and Mr.Pakorn Dharmaroj, Provincial Public Prosecutor attached to the Office of the Attorney General.

Lastly, I most gratefully acknowledge to my parents and my friends for all their supports throughout the period of this research.

Watthanon Kitbuncha

Table of Contents

Pages

Pages

Chapter 1
Introduction

1.1 Background and General Statement of the Problems

In today's busy World , when people do not have much time even for personal work , electronic banking especially electronic fund transfer appears as a beneficial of them. Electronic Banking was introduced in the early 80s and from the time it has been introduced, many people have started to avail its facilitate, make money transaction and also to pay bills like electron city, phone, and etc. The best thing about electronic banking is fast and available to a person in any part of the World, at any time he or she needs it. In this study, we will research about electronic banking at electronic fund transfer in kinds of internet banking on website and phone.

Electronic Fund Transfer is a distant Juristic Act, which we can separate it in two big groups of transfer. First of all, having transfer between the customers and the bank. Secondly, a transfer between the customers.

Electronic Fund Transfer uses the computer and electronic technology such as tablet and smart phone in place for checking and other paper transactions. It has let the user to make the common fund transfer between accounts by its service. It is initiated through devices by internet and application. In this electronic process, there is a procedure to control and authentic the access person by using token, card, password, pin or other credentials for the customer to authentic himself as an authority person to enter the account and make the electronic fund transfer. This process is called measure on authentication.

The measure on authentication is aimed at determining whether someone or something is who or what he or it is claims to be. Its function is worked for establishing the validity and assurance of a claimed identity of a user, device or another entity in an information or communication system. More broadly, measure on authentication is critical tool in achieving trust and online identity protection, which are essential to foster electronic fund transfer such as to prevent fraud on a transaction.

The measure on authentication in manner can separate in two processes which are

1. Identification is the process to let the user show the evidence, device or information to secure who he or she is such as username.

2. Authentication is the process to examine the evidence that he or she is the same person he claim to be.

The authentication mechanism can separate in three qualities which are

1. Possesion Factor (Something the claimant have) such as key, card, token
2. Knowledge Factor (Something the claimant know) such as password or pin
3. Biometric Factor (Something the claimant is) such as fingerprint, Retinal pattern of Voice pattern

Even through the electronic fund transfer are benefit and convenience but it can cause the several problems such as the fraudulent in a cyber-crime and identity theft. In Thailand, there is also have the problems about electronic fund transfer which are fraudulent and unauthorized electronic fund transfer. Therefore to solve the problems, we have to improve the measure of authentication to be stronger and legal. In our country, the measures of authentication is only a technical process not a legal because first of the notification from the Bank of Thailand about measure on authentication in electronic fund transfer is not a law and its framework is not clear, specific and concise enough. So the bank can create his measure on authentication by himself and it make our banking have no standard of authentication. Second, we have some specific regulation about the electronic transaction and the proper measure on authentication which is the Electronic Transaction Act. Nevertheless, its content is not cover enough about the electronic fund transfer and the proper measure on authentication, which will use for the electronic fund transfer which are clear, concise and cover enough to establish the trust among customers.

Nontheless, there are the directive and guideline to specify the measures on authentication, which are used for the electronic fund transfer which are the Draft Revised Payment Services Direction (PSD2) and the European Banking Authority's Guild lines on the security of internet payments (EBA Guild lines). These regulations will determine the definitions, minimum standards and the types of electronic transaction which should to be used with the stronger measure on authentication and also the exemptions. Moreover, in the point of liability between the parties in the electronic fund transfer contract , there are many acts of foreign country such as the

United State of America, Public of Korea and Public of Singapore which will describe about the duty of party which have to bear the liability in the authorized electronic fund transfer and the exemptions. Because we recognize that the electronic fund transfer is risk and it is a time to have the legal measure on authentication and the specific law to concern about the liability in the contract to be written as a specific regulation.

1.2 Hypothesis of the Study

The authentication of electronic fund transfer is a process to identify and verify the user before making the transactions. The authentication's procedure of electronic transactions is found in the Section 9 of the Electronic Transaction Act. And, the problem is its procedure is too widely and not up to date for the transactions at this moment. Moreover, the guideline about authentication of the electronic fund transfer issued by the Royal Decrees and the Proclamations are too board and is not specified properly in its legal standard requirements. Besides, if we have the regulations which are more specific and up to date about the authentication of the electronic fund transfer, they standardize the authentication, decrease the problems of unauthorized access and fraudulent and also increase the trust of customer.

1.3 Objectives of the Study

1. To study on Background, Concept, Theory and Regulation about Measures on Authentication in Electronic Fund Transaction.
2. To study Foreign Regulation about Measures on Authentication in Electronic Fund Transaction.
3. To study the requirement and problems of Measure on Authentication in Electronic Fund Transaction.
4. To suggest the regulation to make strong authentication and to solve the problems of Measure on Authentication in Electronic Fund Transaction

1.4 Study Methodology

This independent study is made by collecting and analyzing of background, concept, theory and regulation about measure on authentication of both Thailand and Foreign countries.

1.5 Scope of the Study

This independent study is to study background, concept, theory and regulation about measures on authentication of both Thailand and Foreign States. And, also studying the problems, solution and suggestion about measure on authentication.

1.6 Expectations of the Study

1. To know background, Concept, Theory and Regulation about Measures on Authentication in Electronic Fund Transaction.
2. To know Foreign Regulation about Measure on Authentication in Electronic Fund Transaction.
3. To know the problems of Measure on Authentication in Electronic Fund Transaction.
4. To have the regulation to make strong authentication of Electronic Fund Transaction.

Chapter 2

Background, Concept of Security, Security Authentication, System and Regulation about Electronic Fund Transfer

2.1 Background of Electronic Fund Transfer

2.1.1 Background of Electronic Banking

What is an Electronic Banking (E-Banking) [2]

Traditional banking business has been assumed that we have to have the customer desk at bank's building, and that we have the office hours from 8.00 AM to 7.00 PM. On the other hands, our customers have their jobs during the day and they have family activities after the job. As you can notice that there is obvious collision between customers' demands and our capabilities.

E-Bank has transformed the banking business into e-Business through utilizing various e-Channels. E-channels are:

- Internet,
- WAP based mobile network,
- Automated telephone,
- ATM network,
- SMS and FAX messaging,
- Multipurpose information kiosks,
- Web TV and others...

These e-Channels enable financial transactions from anywhere, and they allow a non-stop working time. If we remember that customers require non-stop working time, and that they want to be able to use services from anywhere, we can clearly see that in e-Banking business we now have a perfect match between their requests and our capabilities.

---

[2] Skundric Nikola, MilutinovicVeljko, Kovacevic Milos, Klem Nikola. E-Banking, E-Business on the internet, p. 3-7., (E Banking), at http://http://www.grfibg.ac.rs/--milos/papers/ebankbook.pdf, (last visited 5 July 2016).

Obviously, this is not the only advantage of e-Banking. You also have the possibility to extend your market (even out of country) because, among other things, you do not need any more an office in every single town. Also, you have the possibility to process more financial transactions, and last, but not at least, you have to possibly for the lower of your transaction cost because its transaction process by using internet or access through a PC, Mobile devices or Web Television is safe more than transaction in ordinary branch as well.

2.1.2 Background of Thai Electronic Banking[3]

Background

In business fields, Internet has been widely by masses, and has numerous benefits to offer, especially in Internet Banking services. Nowadays, people are so busy in their work lives, that they don't even have time to go to the bank for conducting their banking transactions. All banks provide online banking facility to their customers as an added advantage. Internet banking enables people to carry out most of their banking transactions using a safe website, which is operated by their respective banks. The services available online vary from bank to bank. Most of the general services are on all banking websites such as —view account balances, pay bills, view records of transactions, transfer money to linked accounts with the same bank, transfer money to specially selected unlinked accounts, check interest in accounts, send money overseas, Change your details, etc.

These are not at all for the services available because each bank has different appearance and in the competitive nature of banks they are always offering new features to attract customers. Banks create their banking interfaces and websites in a viewable and user-friendly manner, which enable customers to conduct their

---

[3] Rangsan.Nochai, Administration and Management College, KingMongkut's Institute of Technology Ladkrabang, Ladkrabang and Titida.Nochai, Department of Business Data Analysis, Faculty of Scienceand Technology, Assumption University., The Impact of Internet Banking Service on Customer Satisfaction in Thailand: A Case Study in Bangkok, International Journal of Humanities and Management Sciences (IJHMS) Volume 1, Issue 1 (2013) ISSN 2320-4044, at http://pdfs.semanticscholar.org/de2a/a0ce9d0f74ad81631b61c477467048353de7.pdf, (last visited 4 June 2016).

financial transactions with ease. All online banking services, provided by some banks, are free of cost.

The Banks in Thailand have entered into internet banking service since 1995. However, many Thai banks have been striving to compete with foreign banks by providing better services to meet new Internet Banking service challenges. With high rate of NPL (Non-Performing Loans) and economic crisis on-hand since 1997, many Thai banks are forced to reduce cost via reduction of human resources. Many experienced workers have retired with early retirement package offered by the bank. Remaining employees with less experience have more work to do and work faster within shorter service hours. Consequently, customers have to wait longer in line and suffer from error prone transactions at the over the counter services inside the banks. The open and closing time of bank service hours also have been changed from between 8:30 a.m. and 4:00 p.m. (7 ½ hours) to 9:30 a.m. to 4:00 p.m. (6 ½ hours).

Therefore, the first four Thai banks (Thai Farmers Bank (TFB), Siam Commercial Bank (SCB), Bank of Asia (BOA) and Krung Thai Bank (KTB)) have decided to initiate, explore and attempt to launch Internet banking service as a mean to reduce waiting time, errors, costs, and improve customer satisfaction since 1997. Their Internet banking services allow customers to access and inquiry about their own accounts and perform simple frequently asked transactions via the Internet from their computers at work or home at their convenience time. However, the feedback from customers in terms of satisfaction, complaints, and suggestions remain unknown and needed to be discovered in order to improve or disprove of internet banking services. The remaining nine Thai banks are in early stages of planning, developing and implementing their first internet banking services to their customers.

In the present day, Banks have a lot of competitors not only other commercial banks but also international bank that open in Thailand, especially in Bangkok. It is better for customers to have more choice to select best brand of bank for them to satisfy their need but for banks, they have to find the ways to satisfy customer and keep competitive advantages above other banks. Bangkok Bank got the first prize from Bank of the year award in year 2010 followed by Siam Commercial Bank and Kasikorn Bank respectively. These imply that customers prefer to use Bangkok Bank, Siam Commercial Bank, and Kasikorn Bank the most so this project is

needed to evaluate customer satisfaction of Internet banking quality among Bangkok Bank, Siam Commercial Bank, and Kasikorn Bank.

2.2 Concept and Goal of Computer Security in Electronic Fund Transfer

2.2.1 Concept of Computer Security in Electronic Banking

Computer Security[4]

Computer security rests on confidentiality, integrity, and availability. The interpretations of these three aspects vary, as do the contexts in which they arise. The interpretation of an aspect in a given environment has been dictated by the needs of the individuals, customs, and laws of the particular organization.

1. Principal of Confidentiality

Confidentiality

Confidentiality is the concealment of information or resources. The need for keeping information secret arises from the use of computers in sensitive fields such as government and industry.

Access control mechanisms support confidentiality. One access control mechanism for preserving confidentiality is cryptography, which scrambles data to make it incomprehensible. A cryptographic key controls access to the unscrambled data, but then the cryptographic key itself becomes another datum to be protected.

Other system-dependent mechanisms can prevent processes from illicitly accessing information. Unlike enciphered data, however, data protected only by these controls can be read when the controls fail or are bypassed. Then their advantage is offset by a corresponding disadvantage. They can protect the secrecy of data more completely than cryptography, but if they fail or are evaded, the data becomes visible.

---

[4] Matt Bishop., "Introduction to Computer Security," First Printing, (U.S.: Addison-Wesley, 2004), pp.1-4.

Confidentiality also applies to the existence of data, resource hiding is another important aspect of confidentiality. Sites often wish to conceal their configuration as well as what systems they are using; organizations may not wish others to know about specific equipment (because it could be used without authorization or in inappropriate ways), and a company renting time from a service provider may not want others to know what resources it is using. Access control mechanisms provide these capabilities as well.

All the mechanisms that enforce confidentiality require supporting services from the system. The assumption is that the security services can rely on the kernel, and other agents, to supply correct data. Thus, assumptions and trust underlie confidentiality mechanisms.

2. Principal of Integrity

Integrity

Integrity has referred to the trustworthiness of data or resources, and it is usually phrased in terms of preventing improper or unauthorized change. Integrity includes data integrity (the content of the information) and origin integrity (the source of the data, often called authentication). The source of the information may bear on its accuracy and credibility and on the trust that people place in the information.

Integrity mechanisms fall into two classes: prevention mechanisms and detection mechanisms.

Prevention mechanisms seek to maintain the integrity of the data by blocking any unauthorized attempts to change the data or any attempts to change the data in unauthorized ways. The distinction between these two types of attempts is important. The former occurs when a user tries to change data which she has no authority to change. The latter occurs when a user authorized to make certain changes in the data tries to change the data in other ways. For example, suppose an accounting system is on a computer. Someone breaks into the system and tries to modify the accounting data. Then an unauthorized user has tried to violate the integrity of the accounting database. But if an accountant hired by the firm to maintain its books tries to embezzle money by sending it overseas and hiding the transactions, a user (the accountant) has tried to change data (the accounting data) in unauthorized ways (by moving it to a Swiss bank account). Adequate authentication and access controls will

generally stop the break-in from the outside, but preventing the second type of attempt requires very different controls.

Detection mechanisms do not try to prevent violations of integrity; they simply report that the data's integrity is no longer trustworthy. Detection mechanisms may analyze system events (user or system actions) to detect problems or (more commonly) may analyze the data itself to see if required or expected constraints still hold. The mechanisms may report the actual cause of the integrity violation (a specific part of a file was altered), or they may simply report that the file is now corrupt.

Working with integrity is very different from working with confidentiality. With confidentiality, the data is either compromised or it is not, but integrity includes both the correctness and the trustworthiness of the data. Thus, evaluating integrity is often very difficult, because it relies on assumptions about the source of the data and about trust in that source—two underpinnings of security that are often overlooked.

3. Principal of Availability

Availability

Availability refers to the ability to use the information or resource desired. Availability is an important aspect of reliability as well as of system design because an unavailable system is at least as bad as no system at all. The aspect of availability that is relevant to security is that someone may deliberately arrange to deny access to data or to a service by making it unavailable. This means that the mechanisms for keeping the resource or data available are working in an environment for which they were not designed. As a result, they will often fail.

Attempts to block availability, called denial of service attacks, can be the most difficult to detect, because the analyst must determine if the unusual access patterns are attributable to deliberate manipulation of resources or of environment. Complicating this determination is the nature of statistical models. Even if the model accurately describes the environment, atypical events simply contribute to the nature of the statistics, A deliberate attempt to make a resource unavailable may simply look like, or be, an atypical event. In some environments, it may not even appear atypical,

2.2.2 Goal of Computer Security in Electronic Banking

Goals of Security[5]

Given a security policy's specification of "secure" and "no secure" actions, these security mechanisms can prevent the attack, detect the attack, or recover from the attack. The strategies may be used together or separately.

Prevention means that an attack will fail. For example, if one attempt to break into a host over the Internet and that host is not connected to the Internet, the attack has been prevented. Typically, prevention involves implementation of mechanisms that users cannot override and that are trusted to be implemented in a correct, unalterable way, so that the attacker cannot defeat the mechanism by changing it. Preventative mechanisms often are very cumbersome and interfere with system use to the point that they hinder normal use of the system. But some simple preventative mechanisms, such as passwords (which aim to prevent unauthorized users from accessing the system), have become widely accepted. Prevention mechanisms can prevent compromise of parts of the system; once in place, the resource protected by the mechanism need not be monitored for security problems, at least in theory.

Detection is most useful when an attack cannot be prevented, but it can also indicate the effectiveness of preventative measures. Detection mechanisms accept that an attack will occur; the goal is to determine that an attack is under way, or has occurred, and report it. The attack may be monitored, however, to provide data about its nature, severity, and results. Typical detection mechanisms monitor various aspects of the system, looking for actions or information indicating an attack. A good example of such a mechanism is one that gives a warning when a user enters an incorrect password three times. The login may continue, but an error message in a system log reports the unusually high number of mistyped passwords. Detection mechanisms do not prevent compromise of parts of the system, which is a serious drawback. The resource protected by the detection mechanism is continuously or periodically monitored for security problems.

Recovery has been divided in two forms. The first of all is to stop an attack and to assess and repair any damage caused by that attack. As an example, if the attacker deletes a file, one recovery mechanism would be to restore the file from

---

[5] Matt Bishop, Ibid., p.8-9.

backup tapes. In practice, recovery is far more complex, because the nature of each attack is unique. Thus, the type and extent of any damage can be difficult to characterize completely. Moreover, the attacker may return, so recovery involves identification and fixing of the vulnerabilities used by the attacker to enter the system. In some cases, retaliation (by attacking the attacker's system or taking legal steps to hold the attacker accountable) is part of recovery. In all these cases, the system's functioning is inhibited by the attack. By definition, recovery requires resumption of correct operation.

In a second form of recovery, the system continues to function correctly while an attack is under way. This type of recovery is quite difficult to implement because of the complexity of computer systems. It draws on techniques of fault tolerance as well as techniques of security and is typically used in safety-critical systems. It differs from the first form of recovery, because at no point does the system function incorrectly. However, the system may disable nonessential functionality. Of course, this type of recovery is often implemented in a weaker form whereby the system detects incorrect functioning automatically and then corrects (or attempts to correct) the error.

2.2.3 Security in Electronic Banking

Security Issues[6]

Overview of Security Problems

Electronic banking, as you understood by now if you have not known already, relies on a networked environment. A computer network is simply an arrangement in which multiple computers are connected so that information, applications, and equipment can be shared. By design, networks can increase efficiency, convenience and access, but at the same time, the design also limits the degree to which the environment can be controlled. Network access can be performed through a combination of devices such as personal computers, telephones, interactive television equipment, and card devices with embedded computer chips. The connections are completed primarily through telephone lines, cable systems, and in

---

[6] Skundric Nikola, MilutinovicVeljko, Kovacevic Milos and Klem Nikola. E-Banking, E-Business on the internet. p.7-11., at http://http://www.grf.bg.ac.rs/—milos/papers/ebankbook.pdf, (last visited 5 July 2016).

some instances wireless technology. Whether the system is informational or transactional, these systems facilitate interaction between the bank and the user, often with the support of third-party service providers.

It is important to note that not all networks carry the same degree of risk; not all networks are equally vulnerable; not all networks are equally critical; and not all networks contain data that is equally sensitive.

Internal attacks are potentially the most damaging because a bank's personnel, which can include consultants as well as employees, may have authorized access to critical computer resources. Combined with detailed knowledge relating to the bank's practices and procedures, an internal attacker could access value transfer systems directly, or exploit trusted relationships among networked systems to gain a level of access that allows him to circumvent established security controls. After that, the attacker could potentially transfer money or other assets inappropriately. That is why the first thing you should do is to review and evaluate the security of internal networks.

The use of public networks poses additional risk to those of internal networks. It is important to note that the use of dedicated or leased lines may provide inappropriate sense of security relating to the confidentiality of data transmitted over them. These lines use the infrastructure of public networks; therefore, they are vulnerable to same attacks as the public networks themselves. Risks include line tapping and the possible interception and alteration of data. Therefore, it is wise to encrypt sensitive data transmitted via public networks.

The Internet is a public network of networks that can be accessed by any computer equipped with a modem—so like with any pubic network, the communication path is non-physical and may include any number of eavesdropping and active interference possibilities. Also, it is an open system where the identity of the communicating partners is not easy to define. Thus, as Ed Gerck nicely said "the Internet communication is much like anonymous postcards, which are answered by anonymous recipients." However, these postcards, open for anyone to read — and even write in them — must carry messages between specific endpoints in a secure and private way. Having all that in mind, in e-Banking business we can define three main problems:

1. Spoofing - "How can I reassure customers who come to my site that they are doing business with me, not with a fake setup to steal their credit card numbers?

2. Eavesdropping - "How can I be certain that my customers' account number information is not accessible to inline eavesdroppers when they enter into a secure transaction on the Web?"

3. Data alteration - "How can I be certain that my personal information is not altered by online eavesdroppers when they enter into a secure transaction on the Web?"

Generally, what we have to achieve is following:

Authentication - to prevent spoofing.

Privacy - to prevent eavesdropping.

Data integrity - to prevent data alteration.

Non-repudiation - to prevent the denial of a previous act.

The solution is to use Digital Certificates and Digital Signatures for Web servers, to provide authentication (that is to provide that communication is happening between the desired endpoints), data integrity and non-repudiation service; and to use cryptography algorithms to provide privacy. All these concepts will be explained in a little while. After that, you will see how Secure Sockets Layer in your Internet browser uses these techniques to achieve trusted communication.

2.2.4 Threat in Electronic banking

Threat analysis [7]

This section introduces the Threat Landscape of the identified threats relevant to eIDA method. The most relevant threats and attack scenarios concerning online banking authentication, especially those regarding its ICT infrastructure are then introduced in the following sections.

This section has been collected only those threats directly related to authentication methods used by citizen in e-Finance applications.

---

[7] Threat Analysis, eID Authentication methods in e-Finance and e-Payment services, Current practices and Recommendations, by European Union Agency for Network and Information Security (ENISA), Report, (n.p.: n.p., 2013), pp.18-19.

Threat Categorization

1. Threats against end-users' devices

The below mentioned threats primarily target the devices of end users (e.g. PC, mobile device, tokens, etc.):

1) Physical theft of token or device: End-users may be victims of theft of their token device and their mobile device (or even the piece of paper with their passwords written down).

2) Tampering (or replication) of token or device: PIN brute force attacks, side channel attacks and hardware key loggers are some attack examples of this threat.

3) Malicious software (malware): Malware authors increasingly target online banking. Malicious code with took it features, i.e. as Man-in-the-Browser (MitB), and mobile banking Trojans which can hijack two-factor authentication, i.e. Man-in-the-Mobile (MitMo), are the most prominent threats for e-banking identity theft and fraud

2. Threats against remote banking services.

These threats target the ICT infrastructure of the bank that hosts the web banking service and the respective data stored.

1) Web code injections against banking servers: Attackers exploit vulnerabilities of the web-banking server through SQL injection, cross-site scripting, cross-site request forgery, redirection to a malicious URL and other web exploitation techniques. The adversaries placing such attacks try to extract data such as credentials.

2) Denial of service attacks (DoS): Brute force DoS attacks against online banking server do not pose a direct threat to the components of the end users' authentication process. Nevertheless, DoS attacks can be launched as a diversion as part of a larger attacks and can be reinforced by the misuse of open DNS resolvers.

3) Bank data breaches: bank internal or external threat agents as well as third parties can compromise sensitive information (e.g. end users' credentials, account information, social security numbers etc.)

2.3 Measure on Authentication of Electronic Fund Transfer

2.3.1 Authentication[8]

The stability and security of computer

In the moment, the computer system is easy to threaten, partly from computer virus or the bad person. The computer security help and resolve the computer hardware together with any relevant instruments and especially for the information in the computer or information security.

The core objective of computer system is confidentiality, integrity, availability and non-repudiation.

Confidentiality is to certify that the information will be kept secretly and only the authority person shall access to that information.

Integrity is to certify that the information will not be changed or destroyed whether by accident or intention.

Availability is to the information and other services will be available for use in the needed time.

Non-Repudiation is the communication procedure to express that the information has already sent and the receiver has already receive that information and recognize of who is the sender. Therefore between the sender and the receiver cannot deny the relationship related to that information thereafter.

Authentication

Authentication is the process to certify the authentic of evidence or identity to prove that the user is the person that he or she claim to be.

In practically, the authentication is separated in two processes;

1. Identificationis the process that the user show the evidence who he or she claim to be such as username.

2. Authentication is the process to examine the authentic of that evidence that the user is the same person that he or she claim to be. So that if the

---

[8] Sirporn Jitjarerntham, Saowapa Panchan, and Lesak Limwiwatkun, The introduction of authentication. Publish 28 April 2004, at http://thaicert.netec.or.th/paper/authenJauthentication guide.php, (last visited 15 May 2016).

evidence is direct and authentic that person will be allowed to access the system but if it does not, the system will deny that access.

The identification can separate in two types;

1. Actual identity is the evidence which can indicate that in the reality who is that person.

2. Electronic identity is the electronic evidence which can indicate the information of person. Each people can have more than one electronic evidence such as user account.

Authentication mechanism

Authentication mechanism can separate in three qualities which are:

1. Possession factor is something that the user have such as key, credit card etc.

2. Knowledge factor is something the user know such as password or PINs etc.

3. Biometric factor is something the user are such as retinal pattern or voice pattern etc.

In the process of authentication is to combine the three-kind-factor to certain the claimed evidence and also it depend on the system and the way to use them. The single-factor authentication is to the way to use only one factor that has a limit of use such as for the possession factor, it could be loss or stolen, for the knowledge factor, it could be intercepted, guessed, or stolen from the computer and for the biometric factor, it is the highest security but it is cost expensively. Therefore , it is initiated the idea of combining of qualities of each factors called multi-factor authentication such as combine of possession factor with knowledge factor such as the using of ATM card and PINs or Credit card and signature etc. The combine of more than one factor will make encourage the efficiency in information security.

Authorization

Authorization is the process to allow each person to access the information or system in a limit condition but priority it need to know that person is who in the process of authentication and to confirm that he or she is authentic.

Encryption

Encryption is the process to keep the information privately from the unauthorized person.

There is two things to help that information become confidential are the authorization and authentication because before allowing the user access to the information or encryption the information , it need to certify that the user is who and whether he or she has authority to access or not.

Integrity

Integrity is to certify that the information will not be changed or destroyed from the source either by gross negligence or intention. The integrity threatening is that the unauthorized person can access and control the secured information.

Audit

Audit is the process for examining the electronic evidence, which can use to look after and investigate the process for the accuracy such as the examining of user account by the auditor for certification that electronic evidence is created and sent by the allowed person and to check the connection between person and incidents.

Authentication is arranged as the most important in five standard of examination of evidence in controlling of security. Therefore if there is an good authentication, the efficiency of security of information will increase.

Authentication Types

The common containers of full authentication is consisted of three parts which are

1. Authentication is the most important part because it is the first process of access the system and the user has to be certified from the system that he or she can access and to examine the electronic evidence which was claimed by the user is authentic.
2. Authorization is the limit and control process of user who access the system that how much capability each user have to do in the system.
3. Accountability is to record the detail of using of system and including the access to any information by the user which have done in the system to examine and investigate whether the user changes or revises the information in which parts or not.

2.3.2 Authentication Mechanism used in eFinancial and ePayment Service

Authentication mechanisms used in eFinance and ePayment services[9]

The process that allows an entity to establish the identity of another entity is known as authentication. Current eIDA methods are based on some combination of something that you know, something that you have, and something that you are. When two or more of the aforementioned elements are combined, this procedure is known as strong authentication (two-factor or multi-factor authentication).

In the following sections a short description of each authentication mechanism suitable for e-banking and e-financial systems are introduced. These eIDA methods have been included in the survey, and are categorized according to their type of credentials, as they were shown in the survey.

I. Password/PIN

An eIDA method based on what you know, and consisting of a combination of a valid and unique identifier (username) and a secret pass-phrase (password/PIN), where end-users are requested to enter a private pass-phrase in order to be authenticated. Additionally, two important security enhancements might be implemented:

- Virtual Keyboard - consists of a software based keyboard displayed on the screen (to prevent key loggers), and
- Partial password, the user is asked to enter only some of the digits or characters from the PIN/password, a common partial password approach requests different positions for each session.

2. Biometrics

An eIDA method based on what you are, i.e. end-users are authenticated through their characteristics such as body biometry or behavioral biometry (recognition of fingerprint, voice, face, hand geometry) or behavioural

[9] Threat Analysis, eID Authentication methods in e-Finance and e-Payment services, Current practices and Recommendations, by European Union Agency for Network and Information Security (ENISA), Report, (n.p.: n.p., 2013), pp. 9-13.

biometry (keystroke dynamics, handwritten signature). Herein follow some explanations of the most commonly used techniques:

1) Behavioural biometry

Analyses how the user behaves, interacting with the computer:

1.1 Keystroke dynamics

Also known as typing biometrics, this authentication mechanism uses typing patterns (elapsed time between pairs of keystrokes) in order to authenticate a user.

1.2 Handwritten Signature

A graphical image of a handwritten signature, or the analysis of the speed of the strokes used to generate it, is used to authenticate the user.

2) Body biometry

Analyses how the user "is", i.e. some characteristics of his/her body, that can't be changed easily:

(1) Fingerprint recognition

The user's fingerprint is scanned for the authentication process.

(2) Voice recognition

This mechanism processes (spectral analysis) the user's voice in order to verify the identity of the speaking user.

(3) Facial recognition

The biometric system scans user's face and analyses specific facial features/pattern in order to authenticate her.

(4) Hand geometry

The geometric shape of the user's hand is used for verifying his/her identity.

3) One Time Password (OTP)

This eIDA method is usually based on what you have, and it consists of generating a different, and essentially random password, known as a One Time Password or OTP that is only valid for one session or transaction, and it is also referred as dynamic authentication. A typical OTP implementation is based on one of the following algorithms: event-based OTP, time-based OTP, or challenge-response OTP. Additionally, OTPs can be delivered in several ways, providing different benefits

in terms of usability, security and costs. Static OTP approaches are commonly based on TAN26 code lists, while Dynamic OTP approaches include SMS-based OTP, Hardware Token, Software Token and QR-codes.

(1) TAN code list or coordinates card

The user has a physical document with the list of codes (OTPs) s/he has to use to reply the challenge from the web banking application. The challenges are generated randomly, and so the corresponding reply looks also random.

(2) Mobile SMS based

A different random OTP is sent to the user via SMS message to the registered phone number of the user, each time a transaction requires authentication.

(3) Specific Token device

The user has a physical electronic device, which generates a specific Password (OTP) each time the user requests it. There are different types of devices that may be used for this purpose:

a. Hardware (special Token — time based OTP)

The user has a dedicated/special physical electronic device that generates a specific Password (OTP) each time the user requests it. The generated OTP in this case is a unique value, e.g. a six-digit number that changes at fixed intervals (for example every minute).

b. Hardware (special Token — challenge/response OTP)

The user has a dedicated/special physical electronic device that generates a specific Password (OTP) each time the user requests it. In this case, a challenge-response protocol is used: at first, the web banking application generates a challenge (e.g. a random number); this challenge has to be typed in the token, in order to get the correct response for that time; finally, the response is sent back to the web banking application that will authenticate the user based on the response.

c. Mobile OTP Application (Token)

The user has a software application installed on his/her mobile telephone handset that generates a specific password (OTP) each time the user requests it. The user may need to type in a challenge code displayed on the computer by the e-Banking application website. Note that, in mobile-based solutions the

registration of the mobile device is highly recommended in order to reduce the associated security risks that are inherent in mobile devices.

d. QR codes

The user scans a two-dimensional bar code of the challenge that is displayed on the screen of the e-Banking application (as shown in Figure 4), with the mobile phone handset application, which generates a specific Password (OTP) based on that challenge. This avoids the user having to re-type the challenge. It is worth mentioning that the security strength of the token highly depends on the way it is implemented. In QR codes, the mobile app/mobile device should be authenticated (i.e. registration to link it to a specific user) to avoid the QR code to be scanned from any malicious mobile app/device.

4) e-Signature Certificate

This eIDA method is based on what you have, where end-users are authenticated through e-Signatures. The user's private key can be stored in: Computer stored key, Mobile phone, USB memory card, and Crypto-card

(1) Local / Computer store of Key

The e-Signature is made using the private key of the user that is stored at his/her computer Hard Disk.

(2) Device stored key

a. Memory Token (USB, memory card)

The e-Signature is made using the private key of the user that is stored in a USB or a memory card (removable memory storage).

b. Chip card token (e-Identity card)

The e-Signature is made using the private key of the user stored in the chip of his/er e-Identity card or specific smart card (with cryptographic embedded functions).

c. Mobile phone

The e-Signature is made using the mobile phone of the user, where the user's private key is stored.

5) Device Authentication

If the user accesses the e-Banking service through previously registered/used devices and platforms or through a specific mobile application for that service, then some authentication steps may be avoided.

(1) Device Registration

The user identity is reinforced through registration of the device(s) that user has used before. Attempting to access the e-Banking application from a new device, platform or browser will cause a warming and/or require additional authentication mechanism.

(2) Mobile e-Banking Application

The user accesses the e-Banking service from an application, specific for that Service, running on the mobile telephone handset.

2.3.3 Context authentication mechanisms used in eFinance and ePayment services.[10]

In this section we provide short explanations for the additional context authentication mechanisms which are hidden to the customer. They improve the level of confidence of the service provider on the identity of the customer independently of the user credentials that the customer may have or know. These mechanisms are normally implemented on the server side, in order to check the authenticity of the customer, based on the behaviour, location or device used and other parameters of the operations performed by the user during the interactive session with the service. The users do not easily recognise these mechanisms during the interaction with the service, so they normally are not aware that those authentication mechanisms are protecting them from being victims of fraud or from being impersonated.

1. User behaviour analysis parameters

These parameters are used by the financial services to authenticate users by tracking their overall e-banking operation and transaction history when using/interacting with the service. Thus, through deviations from expected online behaviour, fraudulent activity can be detected and prevented. This category of authentication parameters includes:

---

[10] Threat Analysis, eID Authentication methods in e-Finance and e-Payment services, Current practices and Recommendations, by European Union Agency for Network and Information Security (ENISA), Report, (n.p.: n.p., 2013), pp.14-16.

1) Time between sessions

User's account/transaction operations may be rejected based on their frequency of access to the service within a time window.

2) Destination account filter

Based on the user's transaction history, transactions to account numbers other than those preferred or most used money transfer destinations for the current user are restricted.

3) Total amount in operations

Based on a user's profile, if the total amount in operations of this user within a period of time is above the threshold for that profile, the transaction is rejected.

4) Time of day

Each user interacts with ePayment services and makes transactions in a personalized way, e.g. some specific times during the day. Thus, the transactions and operations that do not take place within his/her usual times of the day may be rejected.

5) Keystroke dynamics

This authentication parameter uses typing patterns (elapsed time between pairs of keystrokes) in order to identify and authenticate a user.

2. Sessions analysis parameters

'These parameters are used to authenticate the user by separately monitoring each of his/her session. This category of authentication parameters includes:

1) Amount filter

Amount transaction thresholds (bigger than, usual) are derived from the user's profile. The user's transactions that do not comply with these thresholds are rejected / restricted.

2) Blacklisted bank accounts

The financial institution may have a blacklist of bank accounts know to be associated with fraudulent activities.

3) Time between operations within one session

An average time between user's operations is compared with the normal value for his/her profile, which is used to detect abnormal or fraudulent activity. If a malicious program hijacks the identity of the user then the time between operations could be shorter.

3. Network analysis parameters

These parameters are used to authenticate users by analyzing networking characteristics. This category of authentication parameters includes:

1) White listed IP addresses

Current customer IP address is checked against white listed IP addresses.

2) Blacklisted IP addresses

The user's transactions/operations may be rejected because his/her IP address is blacklisted (commercial blacklists, lists with compromised computer, blacklisted IP addresses due to previous fraudulent activity, etc.).

3) Anonymous proxy

Transactions from anonymous proxies are rejected since their IP addresses are blacklisted.

4) High risk country classification

A transaction may be rejected if it is carried out from an IP address block that is allocated to a high risk country.

5) Time between sessions from one source IP address

The transaction/operation activity from a single IP address may be marked as fraudulent or suspicious if its frequency is high, or if it is used to access several customer accounts.

6) Geographical distance between operations

Current customer IP address geolocation is checked against the last recently used by that customer. Customer's transactions and operations may be rejected based on the geographical distance between them.

4. Device Authentication

If the user accesses the e-Payment service through a previously registered/used device, or platform, or browser, then some authentication steps may be avoided.

1) Platform identification

The user identity is reinforced through registration of the platform (mobile device, browser, operating systems, etc.) that the user has used before. Attempting to access the e-Banking application from a new device, platform or browser will cause a warning and/or require additional authentication mechanisms.

2) Storage of user key in a device

The device of the user (e.g. mobile or tablet) is authenticated in order to allow the user to make transactions and operations storing a security key in the device or mobile phone SIM card.

5. User Profiling

In this category of contextual analysis mechanisms, some parameters that characterize the interaction of the users with the service are profiled, and the user behavior is analyzed and compared against specific patterns of behavior, i.e. profiles of user. We may have several approaches, depending on the type and amount of information stored by the server.

1) Single behavior pattern

User behavior is analyzed only during the current session and it is compared against only one user profile in the whole system, resulting in users being profiled with a single pattern.

2) Multiple behavior patterns

User behavior is analyzed only during the current session and it is compared against one of the several standard user profiles defined in the whole system. Thus, users are associated to one of those patterns or segments (e.g. company profile, end user profile, investor profile). If the behavior of the user in the current session does not match with the profile associated to this user, then the operations are restricted.

3) Individual behavior pattern

Users are profiled (their behavior is analyzed) in all sessions, in order to create an individual pattern for each customer. Thus, an individual user profile (history) is stored in the system and the user's current and historical sessions are compared.

2.3.4 Analysis to specific emerging authentication mechanisms

1. Biometrics adoption related risks'

In Europe, a specific authorization from customers is required, which is a difficult task, since the majority of people do not feel comfortable with granting permission on the storage of their biometric information (i.e. personal body patterns). This, in general, is only manageable if a strong juridical base exists and the use is adequate, relevant and not abusive in correspondence with the goals and reasons for biometric data to be collected, used or saved, resulting in an important challenge to be addressed.

Moreover, there exist high associated risks, mainly due to the potential attacks to a centralized data base storage of biometrics parameters. The risk of compromise of the biometric information DB (even if it's encrypted, hashed, etc.) is real and non-acceptable for CISOs and directors of the e-banking sector. The sensitive nature of biometric information: data is compromised forever (i.e. it's not possible to change the hand print, Iris, fingerprints, etc.), resulting in both high risk, and great responsibility to be accepted, especially if other eIDA methods are suitable.

Another important factor is the usability, since current technologies do not provide 100% of accuracy at the first try. There are still open issues related to the False Rejection Rate (FRR) and the False Acceptance Rate (FAR), which remain open even in scientific experiments or proof of concepts.

Threat Analysis, eID Authentication methods in e-Finance and e-Payment services, Current practices and Recommendations, by European Union Agency for Network and Information Security (ENISA), Report, (n.p.: n.p., 2013), pp.31-33.

In summary, because of the associated risks, the financial sector is still not prepared to use biometry neither as a unique authentication factor nor a second authentication factor.

Biometry is used in emerging countries, where there are no other means of unique identification of the persons, due to lack of governmentally supported credentials, and also in countries where Personal Data protection is not a priority, like it is in EU.

Specialists are working in finding a solution to the high risk associated to using the biometry, and one solution that is being analysed and starting to be implemented is the local storage of biometric identification profiles. This has three advantages: 1) the responsibility of the storage is transferred to the end user, 2) the chances of a successful threat to steal large amount of biometric information is low, because the threat should be successful on many devices and stores, 3) the biometric identification vector doesn't have to travel over the network.

2. Mobile phones related risks

Advances in mobile technology, currently allow the use of mobile devices in a wide range of services and applications. An important reason for involving mobile phones in authentication systems such as OTP systems, is that, most users already have one, and therefore, no extra hardware needs to be bought, deployed or supported. Moreover, since a mobile phone is considered a highly personal device, the number of incidents due to losing it are relatively low, especially compared with the hardware token devices.

The most common authentication solution involving mobile devices is the SMS-based OTP. A user willing to make an online transaction will receive an OTP from the server. The OTP will be delivered to the mobile device on an SMS. As it can be observed from this study the SMS-based OTP is one of the most implemented authentication methods by the financial sector, nevertheless, SMS-based OTP also convey clear disadvantages, which include, the associated costs, roaming, latency and more importantly the associated security risks, SMS-based OTPs are vulnerable to a different attacks, such as, the Man-in-the-middle (MITM) attacks. The "Euro grabber" incident showed how two factor authentication based on SMS-OTP was circumvented, resulting in a 36 Million Euros loss. To avoid this threat customers

and e-Banking applications should avoid displaying phone numbers associated to the bank account through Internet, whether displayed or modified, even with assumed secure communication channel. Adequate training on this sense has to be launched to both of them.

An alternative to the SMS-OTP is the Mobile phone e-Signature, which greatly reduces the possibility of a successful MITM attack since credentials are protected in the secure element (SE) of the mobile phone. However, the majority of SE implementations rely on a third party, which does not provide a suitable solution to stakeholders such as the financial institutions, as they would certainly like to have more autonomous and cost effective solutions for their mobile payments implementations. Moreover, the limited size of physical SE dramatically affects the number of applications that could be placed in those SE. Financial institutions should promote joint ventures with the organizations that manage the content of those SE, in order to improve the trustworthiness between them.

Another currently implemented solution is the mobile e-banking application, which is able to provide enhanced security if a private key is installed. However due to the nature of mobile devices, important security risks are also present, such as malware hosted on fake applications. Moreover, the development of applications is not always aligned with current security best practices. Best practices like "security by design", secure storage and all actors involved in the process must guarantee delivery and integrity of applications: software developers, financial institutions and customers.

Following the same direction, an emerging solution is the mobile OTP, which consists on installing the software tokens on the mobile phone. A key advantage of the mobile software token is that there are no new devices for customers, since customers already own the device, which they already carry everywhere. Another advantage regarding the mOTP solution is the ability for the software tokens to be distributed and updated immediately, and without logistical planning, since the mOTP token consists of an application that only need to be loaded on the mobile device. Thus, mOTP have become a more reliable deployment method than hardware tokens, nevertheless, as in mobile e-banking application, the software tokens also inherit the same security vulnerabilities from the mobile phone. In fact mOTP could be considered a particular case of mobile e-Banking application.

Many organizations use mobile phones as support for the second authentication factor. Mobile phones may be considered "something the user possesses" for the purpose of implementation of two-factor authentication, from the technical perspective. However, from the legal perspective, mobile devices cannot necessarily be acceptable for attributing a specific transaction to its originator. For that purpose, e-signature tools have to be used, and they can be implemented in mobile devices or PCs. The mobile device on its own is not able to deliver evidence that a specific transaction could only have occurred with the approval of the legitimate owner of the mobile, it requires specific software and adequately installed private key to do so.

In summary, mobile device is an emerging authentication solution that can be seen as "something the user has", when using it for identification purposes. Nevertheless, for attributing a specific operation to its originator, it's not able to provide enough non-repudiation evidence that a specific operation has been performed by the owner of the device.

2.3.5 Recommendation of Authentication by European Union Agency Recommendation'[12]

1. Use Two Factor Authentication (2FA) for medium to high-risk transactions

For medium and high risk operations, a strategy of using at least two authentication mechanisms that are mutually independent, where one is non-replicable and other non-reusable, exchanging credentials through different communication channels or devices should be implemented. Non-re-usability may be implemented by linking the authentication (e.g. OTP challenge) to the amount and payee of every transaction.

Many organisations use mobile phones as support for the second authentication factor. The adequacy of the authentication mechanisms for low,

---

[12] Threat Analysis, eID Authentication methods in e-Finance and e-Payment services, Current practices and Recommendations, by European Union Agency for Network and Information Security (ENISA), Report, (n.p.: n.p., 2013), pp.34-38.

medium or high risky operations is described in section 5.4 above. It shows that the selection criteria used by the financial institutions already takes into consideration the different profiles of customers as well as the efficiency and strength of the eIDA method proposed. The aim of this recommendation is to shift the criteria to select the eIDA method used for medium level of strength: from its usability, to its covered risk and efficiency in protecting customers' assets.

Most banks already apply more than one authentication mechanism to grant access to different types of operations. Currently most used combinations are PWD, sometimes with additional security improvement methods like Virtual Keyboard, complemented with: SMS OTP (29%), TAN (25%), Hw. OTP (18%), MeBA (11%), Mob. OTP (9%), Chall.Hw OTP (8%), whilst other combinations are also reported. Figure 12 shows the relative weight of the different combinations of authentication mechanisms reported in the survey through the size of the circles.

2. Improve the knowledge and the behavior of customers and professionals

1) Continuous training of professionals, to improve their perception of the actual risk associated to the e-Finance transactions, and the authentication mechanisms, keeping in mind the last threat patterns discovered by criminals. Professionals should also share their awareness with customers, to keep them continuously informed about incidents caused by common threats such as phishing or social engineering.

2) The professionals of the e-Financial institutions should inform their customers about the usability and need of the safer authentication mechanisms required to have an adequate protection to their assets, in order to make them to feel comfortable enough using them.

3. Improve the security of the e-Finance environment

1) Environment risk analysis

Financial organizations and e-commerce merchants must perform specific risk analysis for their environments, taking into consideration the actual loss, number of incidents, number and skills of customers involved, and actual vulnerabilities of the authentication methods available, in order to be able to choose

the ones that most effectively reduce the number of incidents and loss, i.e. the risk to lose money.

2) Context based or continuous authentication

Customer authentication should be complemented with the implementation of a context-based authentication strategy, tailored to customer behavior profile (e.g. transfer destination account), segment (e.g. total amount in operations) and the operation risk (e.g. destination country, black lists).

3) User device security testing and evaluation

The security testing and evaluation of the device used to access the service has to be validated directly or indirectly by the PSP.

Mobile devices are becoming vulnerable to several security threats such as malware attacks (see section 6.2. Mobile phones related risks), where attackers abuse them for transactions without any interaction of the legitimate owner of the mobile phone, just as it has been possible in normal PCs since years ago. In June 2012, ENISA recommended financial institutions to "Assume all PCs are infected"43. Therefore, static security analysis of any device used by the customers to access e-Banking services should be performed, in order to estimate the degree of compromise of user's device. Some kind of analysis can be done remotely by the server accessed by the customer (e.g. browser version), but only customers can install and run anti-malware software on their devices, and for this purpose have to be trained and convinced about their own interest on having their devices protected against infection.

4) Device registration

The concept of "something the user has" can be extended to the platform used to access the service, and thus it is recommended to register any Device, Browser, or Mobile Application used by the customer. A real time validation of the authenticity of the device would be required.

This registration will prevent customers from being impersonated by somebody that has been able to replicate some credentials of the customer, using specific different credentials and process to authorize new devices for the user.

4. Improve the security of e-Finance application development and distribution

1) Secure e-banking application development

Technology providers must guarantee secure e-banking application development, taking into consideration actual threats to Operating Systems (e.g. mobile attack vectors).

Special emphasis has to be given to managing personal data, for which purpose specific data security analysis (persistency, access control) have to be implemented during the development phases.

Another security issue that may have strong impact on the adoption of strong eIDA methods is the implementation process and tools, for two reasons:

- eIDA method incorrectly implemented may have security back doors or vulnerabilities
- eIDA method with inadequate or too complex implementation tools will not be accepted by customers.

In the case of mobile phone applications, it is also recommended to develop applications to be executed within Secure Execution Environment, using available secure elements that will make them more robust against emerging threats, before those threats become reality.

2) E-Banking applications distribution

Distribution of e-Banking applications has to be made through trusted channels, reputable sites that guarantee that applications have been tested for security.

It is very difficult for customers to validate the authenticity of e-Banking applications on their own, because criminals have demonstrated their ability to sign fake applications with trustworthy software signing certificates that can overcome the normal installation filters in many devices.

For this reason the use of software distribution platforms (software marketplaces or e-Banking websites) that guarantee that they have performed security tests on the applications is very important for the security of the device on which the application is installed and to guarantee that the application will be executed as expected by the developers.

2.4 System of Electronic Fund Transfer

2.4.1 Wholesale Electronic Fund Transfer

1. Inter Bank Fund Transfer S.W.I.F.T.

[14]Inter-bank EFT uses on-line transactions carried out on private networks to transfer funds; the bank plays the role of both payer and payee. Such transfers occur between a bank and its customers, or a bank and another bank. In contrast to a check payment, which requires several actual cryptographic processing days and manual efforts like signature verification, check sorting, and information capture, EFTs are same-day, almost instantaneous payments. Figure 1 illustrates one method used for such transfers to conduct payments.

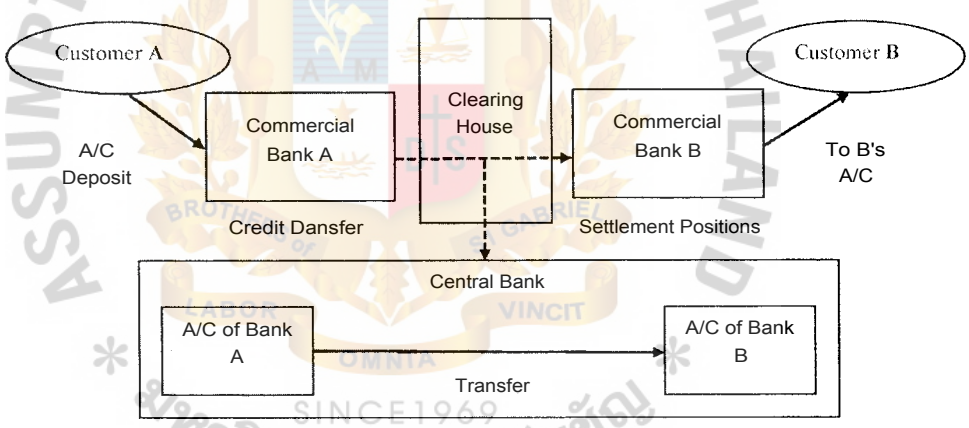

Figure 1. A method of funds transfer to conduct payment

As shown in Figure 1, customer A uses commercial bank A to remit a fixed amount of money to customer B and his/her commercial bank B. After receiving the remittance amount plus any fees, commercial bank A sends an electronic credit transfer message to commercial bank B through a clearinghouse. According to the credit instruction, commercial bank B credits the remittance amount to customer B's account

---

[14] Dan Zhu, "Security Control in Inter-Bank Fund Transfer," Department of Logistics, Operations and MIS Iowa State University, Journal of Electronic Commerce Research, Vol. 3 No.1 , 2002 , at https://pdfs.semanticscholar.org/877a/b6159e3e31b18c 493bd769497b6ff36af72d.pdf, (last visited 30 June 2016).

(or advises customer B to pick up the check). After a fixed accounting period, the computer system at the clearinghouse will calculate the settlement positions for participating banks and send them to the central bank via telecommunication channels. The system at the central bank will use the accounts held by commercial banks to perform debit/credit operations for clearing the difference of transfer amount among banks, thus completing the funds flow of remittance process. EFTs can achieve immediate payment across two remote sites by the telecommunication facility under some credit line arrangement, but there must be some way to ensure the security of the remittance. Such protection should prevent the revelation of the information as well as illegal modification of it, by both external attackers and internal betrayers.

Large amounts of money are involved in everyday funds transfer transactions, therefore, the security of systems and the smooth of operation must be maintained. In general, there are five central requirements of network security (1) Confidentiality: Data should not be disclosed to unauthorized persons; (2) Access control: Operation of the system is under some control mechanism to prevent illegal access of data; (3) Integrity: Message information should remain original to carry designated transaction details. (4) Data origin authentication: Some way is used to prove the source of data; (5) No repudiation: System should provide some features to ensure that nobody can deny involvement in an electronic transaction so that the legal effect of an EDI transaction can be relied on.

Cryptography has been widely applied in data communication to meet the above security requirements. In the following sections, some key technologies of cryptography are introduced and the security features of SWIFT are studied.

SWIFT Code"

Inter Fund Transfer with SWIFT Code

The payment system of the Bank of Thailand has deemed the meaning of S.W.I.F.T (Society for Worldwide Interbank Financial Telecommunication) as the financial communication system between banks via computer system which has a network covered all the World serviced by Society for Worldwide Interbank Financial Telecommunication. SWIFT Code is a standard form of Bank Identifier Codes (BIC)

[13] SWIFT Code, at http://www.theswiftcodes.com, (last visited 29 August 2016).

which is used in electronic inter fund transfer. The banks which use SWIFT Code is more than 7,500 around the World and when includes with the partnership banks which connect to BIC network, there is the bank which use the SWIFT Code in electronic inter fund transfer more than 10,000.

SWITF Code is contained of 8-11 letters. By the way, the first 8 letters is meant a head office. The meaning of letter 8-12 digit is explained as follow:

The first 4 alphabets mean the code of the banks.

The 2 alphabets latter mean the country code or ISSO 3166-1 alpha-2 code.

The latter one alphabet and a digit mean an area code.

And the last 3 letter will refer to the branch code and if it was xxx , it means the head office.

In the electronic inter fund transfer from one country to another country, the customer has to inform and fill the detail of the beneficiary, account number and the name of the beneficiary's bank. In the case to transfer money to another country, the customer has to have the same detail for informing the beneficiary's bank in that country for receiving the detail of targeted beneficiary. The detail should be consisted of:

1. Name and address of the customer including with the contract phone number for the convenience of the bank's employee to inform in the case of error;
2. The beneficiary's account number;
3. Name and address of the beneficiary's bank;
4. The SWIFT Code of beneficiary's bank. In the case that the customer do not understand English or hesitate and embarrass to ask the officer or do not understand about the importance of SWIFT code, the customer can check the SWIFT code they need from the website: http://www.theswiftcodes.com.

However, in the case that the customer inform the wrong name, address or SWIFT code of the beneficiary's bank and want the bank to revise the problem, the customer has to bear the cost of expectation with the beneficiary's bank. The cost is upon the service fee of each bank and the cost to revise the name and address of the beneficiary bank which is about 25-30 coins of each currency.

2. Bank of Thailand Automated High-Value Network-Bahtnet

[14]BAHTNET (Bank of Thailand Automated High-value Transfer Network) is a financial infrastructure serving for Real-Time Gross Settlement (RTGS) of large value funds transfer between financial institutions or other organizations maintaining deposit accounts at the Bank of Thailand (BOT).

Prior to the introduction of BAHTNET, payments among financial institutions were mainly executed by cheques where the payees could not receive their funds immediately due to collection and settlement process between paying and receiving banks. Consequently, payees were exposed to considerable risk because the payment finality had not immediately achieved, and this would possibly lead to a greater risk in payment systems as a whole.

Channel Access

BAHTNET members can link to the BAHTNET System via two channels as follows:

1. S.W.I.F.T. network which is an international financial telecommunication network, given that members will have to send message in accordance with S.W.I.F.T. (Society for Worldwide Interbank Financial Telecommunication) message standard. Members are able to develop internal systems to link with the BOT in Straight-through Processing (STP).

2. BOT WEB PORTAL through Bank of Thailand Electronic Financial Services (BOT- EFS) provided by the BOT. Members will send and receive messages through BAHTNET Web service, provided that the BOT has developed the message format in accordance with S.W.I.F.T, message standard. However, all BAHTNET members, both S.W.I.F.T. or non-S.W.I.F.T. members, are required to install BAHTNET Web service for the purpose of inquiry for account balance and movement of deposit accounts, including queue management and reports.

Security Measurement

Since BAHTNET system is designed for high-value funds transfer, thus BOT maintains high security standard, given that members transmitting messages to BAHTNET via S.W.I.F.T. channel must apply S.W.I.F.T. security standard which

---

[14] Bahtnet System, Bank of Thailand Press., at https://vvww.bot.or.th/English/ AboutBOT/LawsAndRegulations/Pagesidefault.aspx, (last visited 29 August 2016).

is an internationally-accepted standard. For members transmitting messages via BOT-EFS WEB channel, digital signature is employed where members sending messages are required to have Private Key in their tokens to create digital signature for verifying electronically their activities to BAHTNET system. By adopting this technology, BAHTNET is capable of assuring members with integrity, confidentiality, authentication, non-repudiation including continuous audit trail for all transactions to be kept as evidence.

Settlement Procedure

BAHTNET is an irrevocable funds transfer system, which operates on a Real Time Gross Settlement (RTGS) basis. It requires greater level of liquidity than the traditional net settlement system. Therefore, the transferor has to have an adequate amount of funds in its current account at BOT in order to be able to successfully execute the funds transfer order. However, the transferor may momentarily face liquidity shortage, which would halt the transfer order. The BAHTNET utilizes the following mechanisms for handling such a situation.

A Queuing Mechanism is used to help prioritize an executable funds transfer orders, which are placed in a queue until such time as the account balance has enough funds to cover the funds transfer orders.

A Gridlock Resolution system is an optimization process to help resolve a gridlock situation due to liquidity shortage. The system searches the queue for a combination of funds transfer orders that have a manageable net clearing position, in which case these funds transfer orders are executed simultaneously

3. Electronic Cheque Clearing System E.C.S. [15]

Cheque clearing system by an electronic process or E.C.S is developed for used in Bangkok and nearly provinces area and operated by Electronic Cheque Clearing Center.

The System of Electronic Cheque Clearing

[15] Sangket Pookrissana, "The Liability of Bankers Concerning the Fund Fransfer by Electronic Machine," Thesis Degree of Master of Law, Ramkhamhaeng University, 1997, pp.23-27.

The banks, member of Electronic Cheque Clearing Center, will have electronic instrument online connected to their sub-branches and in the same time the general head office of these banks will also have electronic instrument online connected to the Thai Electronic Cheque Clearing Center. When the sub-branch deposited a cheque from customer, it will encode the cheque's number, paying bank number, paying sub-branch number, paying account number and the amount of money with the deposited bank will receive. After that these information will be sent to the head office and the Electronic Cheque Clearing Center respectively.

The Electronic Cheque Clearing Center by E.C.S system, after receiving the information above, will process those information and make claiming sheet of each banks and counting the claiming credit until the end of a day . Then it will analyze the sheet to be a final sheet and send this sheet back to the paying banks for checking and waiting for the confirmation within 45 minutes. If there is any modifications, the center will process and send the sheet back by the same way. Last but not the lease, the center will clear the sheet by debit the paying account and take the money to credit the receiving account by using Baht-net system.

The Advantage of Electronic Cheque Clearing System

This system is benefit to the credit banks because they can process all working time and so the bank and their sub-branches could be deposited the cheque almost the day because they can send and receive the information between each other online and immediately.

2.4.2 Retail Electronic Fund Transfer

1. Automated Teller Machines

[16]An ATM is simply a data terminal with two input and four output devices. Like as any other data terminal, the ATM has to connect to, and communicate through, a host processor. The host processor is analogous to an Internet Service Provider (ISP) that is the gateway through which all the various ATM networks become available to the cardholder (the person wanting the cash).

---

[16] How do ATM machines work, at http://https://www.quora.com/How-do-ATM-machines-work-internally, (last visited 19 October 2016).

When a cardholder wants to do an ATM transaction, he or she provides the necessary information by means of the card reader and keypad. The ATM forwards this information to the host processor, which routes the transaction request to the cardholder's bank or the institution that issued the card. If the cardholder is requesting cash, the host processor causes an electronic funds transfer to take place from the customer's bank account to the host processor's account. Once the funds are transferred to the host processor's bank account, the processor sends an approval code to the ATM authorizing the machine to dispense the cash. The processor then ACHs the cardholder's funds into the merchant's bank account, usually the next bank business day. In this way, the merchant is reimbursed for all funds dispensed by the ATM.

Besides, when you request cash, the money moves electronically from your account to the host's account to the merchant's account.

ATM Security

ATMs itself keep your personal identification number (PIN) and other information safe by using encryption software such as Triple DES (Data Encryption Standard). But there are lots of things that you can do to protect your information and your money at an ATM.

For safety reasons, ATM users should seek out a machine that is located in a well-lighted public place. Federal law requires that only the last four digits of the cardholder's account number be printed on the transaction receipt so that when a receipt is left at the machine location, the account number is secure. However, the entry of your four-digit personal identification number (PIN) on the keypad should still be obscured from observation, which can be done by positioning your hand and body in such a way that the PIN entry cannot be recorded by store cameras or store employees. The cardholder's PIN is not recorded in the journal, but the account number is. If you protect your PIN, you protect your account.

2. Mobile Banking[17]

[17] TAIWO DAYO AJAKAIYE and KARL SENANU KUDZO KRAUSE, Online Based Authentication and Secure Payment Methods for M-Commerce Applications, Master of Science Thesis in the Programme Secure and Dependable computer systems, Chalmers University of Technology, University of Gothenburg, p. 8., Publish 2011. at

M-Banking is used for a variety of products and services ranging from basic applications such as mobile fund transfer to high security mobile payment applications. Mobile payments are now becoming a widely used medium for carrying out financial transactions. Ericsson, a telecommunication giant and a major player in the mobile payment industry, estimates that the mobile payment market will yield a profit of 20 billion Euros by 2015 and a turnover of 600 billion Euros. A mobile payment application must provide means for carrying out secure authentication and financial transactions.

Authentication and secure payment is a major security issue when it comes to carrying out mobile financial transactions remotely. Developers of such applications are always faced with questions such as; how do we ensure that the person requesting to carry out a financial transaction is who he claims to be? How do we carry out secure financial payments from a mobile device? There are several mobile payment applications providing some form of authentication/payment function, and installed on various Smart phones (iPhone, BlackBerry, Android phone, etc.) today.

However, most existing solutions are platform dependent and each has its unique implementation for secure authentication and payment. For example, a solution implemented in java for an Android phone will have to be re-implemented in Objective C in order to be used on an iPhone due to language restrictions. Another question which is obvious at this point is; how do we implement a method for secure authentication or payment which is compatible with all Smart phones?

1) Mobile Device Authentication[18]

---

https://gupea.ub.gu.se/bitstream/2077/27863/1/gupea 2077 27863 1.pdf, (last visited 19 April 2016).

[18] TAIWO DAYO AJAKAIYE and KARL SENANU KUDZO KRAUSE, Online Based Authentication and Secure Payment Methods for M-Commerce Applications, Master of Science Thesis in the Programme Secure and Dependable computer systems , Chalmers University of Technology, University of Gothenburg, p. 10-12. at https://gupea.ub.gu.se/bitstream/2077/27863/1/gupea 2077 27863 1.pdf, (last visited 19 April 2016).

We have studied various research works that have been done in the area of authentication with a focus on mobile devices. The studies were conducted on how a secure financial transaction is carried out. The essence of this section of the thesis work is not to only cite some of the important results that were obtained, but to also see their relevance to the research problem.

1. Two-factor authentication

FadiAloul, S.Z and Wassim El-Hajj has been demonstrated that the problem of carrying out secure authentication via mobile devices. They proposed the use of a two-factor method of authentication which makes use of something you have (mobile phone) and some-thing you know (one-time password). The method involves the use of a mobile phone for the generation of a one-time password (OTP), or the use of SMS in retrieving a remotely generated OTP from a server. Results showed this two-factor authentication method to be a more secure form of verifying users than traditional password systems. They also showed how this method can be used to eliminate the problems that one-factor authentication methods (e.g. passwords) face. Their method provides a cheaper alternative to current two-factor authenticating systems (tokens, cards) widely used today. It does this by making use of the users' mobile phone for OTP generation, therefore eliminating the extra cost involved in purchasing additional tokens and cards.

2. Single sign-on system

When a user has several user accounts with different service providers, he would need to remember and use different user-ids and passwords while connecting to those accounts. The single sign-on (SSO) mechanism relieves users of having to undergo unnecessary multiple authentications for each service. In the paper titled "The study of multi-level authentication-based single sign-on system", the authors pointed out that systems which have a single sign-on experience, assign the same level of security to each service providers within a distributed network. This accorded to the authors is not really secure. If one of the service provides within the distributed net-work becomes compromised, then the single sign-on experience will tend to pose a threat to other service providers that require a higher level of security. The authors proposed a multi-level authentication mechanism (MLA-SSO), in which different security levels that are required by different service providers can be

automatically analyzed and assigned by a server. This improves the flexibility, performance and security of the network.

3. Strong authentication

In the Research carried out by Do van Thanh et al, the authors introduced the concept of using the mobile phone device as a token for authentication instead of a traditional hardware token. The overall cost of using an additional device to carry out authentication is very high for organizations that have to maintain thousands of to-kens. Also, users will have to carry around hardware tokens whenever they need to carry out authentication on the fly. The authors proposed the use of mobile phones as a replacement for hardware tokens as a way of solving the various issues described above. They also discussed various ways that the mobile phone could be used as de-vice tokens in a secure two-factor authentication process.

4. Social Authentication

A study carried out by two researchers from McGill University in Canada pro-posed an additional authentication factor to an already existing two-factor authentication (see 2.1). The authors Muthucumaru Maheswaran and Bijan Soleymani suggested that this additional authentication factor (someone you know), should be high-ly dependent on the social network the particular individual belongs to. That is, every individual who uses a mobile device as an authenticator needs to belong to a particular social network. In the case when a member of that particular network has lost his secret credentials or the mobile device, that person will require someone to vouch for him. During the process of vouching for someone, the secret credential is not sent to the voucher but to the individual who needs to be vouched for. This maintains the secrecy and privacy of the credentials and thus adds an additional level of security to the already existing system.

2) Threat Model in Mobile Banking

Whenever a security analyst is called upon to evaluate the security of a system, he first would have to create a threat model of the application he intends to evaluate or design.[19] This is necessary to enable him to fully assess the

[19] TAIWO DAYO AJAKA1YE and KARL SENANU KUDZO KRAUSE, Online Based Authentication and Secure Payment Methods for M-Commerce

possible threats that may occur by looking at the system from the attacker's point of view. We will describe a threat model in the next section in order to identify the kind of threats that can be faced by the authentication system. In order to successfully create a threat model for an m-commerce application, one would first need to understand the target system. We did this by first identifying the system assets, system users and vulnerable points. We weren't able to come up with possible attacks for the threat model based on this information and from the various mobile threats that we have identified to exist today (see 5.1). We have also investigated and documented possible ways of mitigating attacks identified in the threat model.

1. Assets to be protected

In order for users to successfully prove who they are during an authentication process, they will have to provide certain authentication data and in some cases personal data. The security of these data must not be compromised during the authentication process or via vulnerabilities in the authentication method.

User data

The confidentiality, integrity and availability of user data must be assured at all times. For examples of such data included with the names, telephone number, address, credit card details etc.

Authentication data

A system verifies a user during authentication by requesting for some secret information (OTP, password, pin, etc.) which only the user knows. For that reason, these authentication data must be securely protected from getting into the hands of any other person.

2. Users

A system cannot be fully evaluated unless a clear picture of all those that will be using the system is available. In a secure system, security privileges, access and data are made available only to a certain group of users while it is blocked for others. Therefore, a good understanding of the different users that can

---

Applications, Master of Science Thesis in the Programme Secure and Dependable computer systems, Chalmers University of Technology, University of Gothenburg, pp.28-29.

and will interact with a system must be taken into consideration when designing secure systems.

Legitimate users

A legitimate user is the person who is the rightful owner of an asset, or that has exclusive access to certain system privileges. An example of a legitimate user is the owner of a credit card used in a financial transaction.

Adversaries

This is the person who intentionally tries to acquire assets which does not belong to him, or maliciously tries to gain system privileges which he is not entitled to.

Administrators

Administrators are persons who have been legally mandated by the organization to handle day to day running of the m-commerce system. Tasks carried out by administrators include system modification, account deletion and so on.

3. Vulnerable points

Inputs and output points are avenues in which users or data centers or leave the system's trusted network. These entry points are vulnerable to attacks because they serve as the only way the attacker can have access to the system resources.

Communication channel

Smart phones provided access to applications via several communication channels. These channels serve as entry and exit points to In-commerce applications and are vulnerable to different types of attacks. Examples of communication channels on Smart phones include short message service (SMS), Bluetooth, http etc.

Web browsers

Most m-commerce applications reside on remote servers and are accessed via web browsers such as opera mini, safari and so on. Thus, vulnerabilities in these browsers will also affect the security of the m-commerce application.

Mobile phone OS

In most cases, an application implemented on a mobile phone is dependent on the mobile phone operating system (OS) for communications

with the system processes and hardware. Popular OS include Android, iPhone, Symbian etc. A security hole in any of these operating systems could be used as an entry point into attacking the m-commerce application that resides on them. An example of such a case is when an adversary gains administrative rights to an OS. He can for instance configure the security settings of the default Internet browser to allow connections to unsecure web-sites.

3. The Use of Internet and Mobile banking in Thailand[20]

The experts showed some satisfaction with the introduction of Internet Banking services in Thailand in terms of customer awareness (62.50%), the development of Internet Banking services from the past to the present (75.00%), the current number of Internet Banking users (62.50%), and the growth of the number of Internet Banking users from the past 5 years (75.00%). There was no significant evidence of the experts' satisfaction in terms of techniques or strategies that banks employ to introduce and influence customers to use Internet Banking services in Thailand.

In the next five years, the three features of Internet Banking services that will be used most are inquiries about outstanding balances, fund transfer between accounts within the same bank, and transfer payment for public utilities respectively. These are as same as the three features that will also be used most in the next ten years. These are the basic features, which every customers who wish to execute with his bank account. In the next five years, bank branches, ATMs, and telephone banking will be the retail banking channels that will be used most respectively, and Internet Banking service was ranked at No.4. In the next ten years, bank branches, ATMs, telephone banking, and WAP technology (mobile phone) will be the retail banking channels that will be used most respectively, and Internet Banking service was ranked at No. 5. This can be supported by the findings which found that the experts thought

---

[20] Boonyarat Samphanwattanachai, Department of Marketing, School of Management, Assumption University., "Internet Banking Adoption in Thailand: A Delphi Study," Special Issue of the International Journal of the Computer, the Internet and Management, Vol.15 No. SP4, (November, 2007): 12.5-12.6 and Proceedings of the 24th South East Asia Regional Computer Conference, November 18-19, 2007, Bangkok, Thailand.

that the Internet Banking service is quite important towards the future of retail banking in Thailand but that it cannot replace the other distributional channels of retail banking. Moreover, from the findings, WAP technology (mobile phone) is the channel that will probably grow up well in the future as it was ranked at No. 4 in next ten years. The main advantages of Internet Banking service for a bank were to reduce of transaction costs, to increase the number of customers, to search for new innovative services, to increase competitive advantage, and to have a better image respectively. The banks that want to provide efficient Internet Banking services should have a good information technology infrastructure and clear objectives and goals. Moreover, laws and regulations, and the overall market situation also affect Internet Banking adoption of the bank.

There was no significant agreement from the experts that Internet Banking services offer the same advantages as established retail banks and new entrants to the banking industry in Thailand. But from the mean and median scores, many experts disagreed that Internet Banking services offer the same advantages as established retail banks and new entrants to the banking industry. Internet banking services can be one factor that influence a customer to open a bank account with this bank. The experts thought that Internet Banking services are convenient and can help customers save costs and time. The experts also thought that the main factors that affect customer's adoption of Internet Banking in Thailand are the number of Internet users, customer's trust, Internet Banking services quality, security, costs and fees, variety of products/services, and a bank's image respectively. The experts also wanted Internet Banking services to improve security, advertise about Internet Banking services more, provide more variety of products/services, improve the ease of use of Internet Banking services, improve accessibility, should not charge any fees or only charge reasonable fees, improve the website's design, and have a call centre or staff directly responsible for Internet Banking services.

To increase the number of Internet Banking users in Thailand, there are many factors to consider. From the findings, the number of Internet users is quite an important factor because there are only a small number of Internet users in Thailand. But the important thing for banks at the present is to influence Internet users in Thailand to use Internet Banking services. They have to improve the Internet Banking process and pay more attention in Internet Banking services. The question of

fees is also important. The banks should not charge any fees for Internet Banking services or only charge at lower rates than other distributional channels. This could help banks keep existing Internet Banking users and influence other customers to use Internet Banking services. But they have to advertise Internet Banking services better than at present and have clear and outstanding objectives and goals for providing Internet Banking services.

Conclusion

Internet is now an important device in the modern businesses including banking sector. It has become one of retail banking distributional channel that the banks and the customers can use it to communicate and interact each other. There are many commercial banks in Thailand have provided Internet Banking services to Thai customers. But Internet Banking in Thailand is still an early stage and there is no research studied about Internet Banking Adoption in Thailand from the experts' view. This paper uses the Delphi Study to investigate the experts' opinion about Internet Banking Adoption in Thailand. The members of panelists came from both bank executives and the academicians.

The main findings are Internet Banking is quite important distribution channel of retail banking in Thailand but it cannot replace the other distribution channels Moreover, the Internet Banking users will use the following basic Internet Banking features most in the future: inquiries about outstanding balances, fund transfer between accounts within the same bank, and transfer payment for public utilities respectively. The number of Internet users in Thailand is the most important factor that affect the number of Internet Banking users in Thailand followed by customer's trust, Internet Banking services quality, security, costs and fees, variety of products/services, and a bank's image respectively. The banks should have a good information technology infrastructure and clear objectives and goals to provide Internet Banking services to the customers.

This paper suggests that at the present, the banks should influence the current Internet users in Thailand to use Internet Banking first. Simultaneously, they must improve Internet Banking process and put their concentration on Internet Banking services more. They also should charge the fees of Internet Banking services at reasonable rate or lower than other distribution channels in order to keep the existing Internet Banking users and increase the number of new Internet Banking

users. The future research might focus on customer's trust towards Internet Banking in Thailand. Because from the findings, it was the second important factor that affects customer's adoption of Internet Banking in Thailand.

2.5 Laws and Regulations related to Measures on Authentication of Electronic Fund Transfer

2.5.1 The Civil and Commercial Code

The Thai Civil and Commercial Code and The measure on authentication of electronic fund transfer. In this law, there are some sections which related to the measures on authentication of the bankers for the fund transfers by cheques.

A cheque is a written instrument by which a person, called the drawer, orders a banker to pay on demand a sum of money to, or to the order of, a person, called the payee. It is a duty of the holder of a cheque to present it for payment to the bank within one month or three month after the date of issue due to it is payable in the same town or elsewhere. And after the cheque was presented at the bank, the banker is bound to pay a cheque drawn on the holder unless there are some cases regulated in section 991 and 992. In the section 991 and 992, if there is not enough money in the account, the cheque is presented for payment later than six months after the date of issue, notice is given that the cheque has been lost or stolen or there is countermand of payment, the drawer is death and there is a publication of an interim receiving order or bankruptcy order against the drawer, the banker has not pay drown to the holder.

In the other hands, according to section 1009, when is not any cases in the section 991 and 992 occurred and the banker pay the bill to the holder with good faith, without negligence and in the ordinary course of business. The bank has not to bear the liability although such endorsement of the bill has been forged or made without authority because it is not duty of the bank to prove that the endorsement of the payee or any subsequent endorsement was made by or under the authority of the person whose endorsement it purports to be.

Moreover, according to section 994, there is a type of cheque that the payment of it can only be made to a banker, called a crossed cheque. For the authentication methods for the crossed cheque, the banker has to check two things.

First, to check it is a crossed cheque or not, if it is a crossed cheque, its payment only be made to a banker. Second, if between such lines a name of any particular banker is inserted, it is a special crossed cheque, the payment of it can only be made to that banker only.

The duty of the banker for the crossed cheque is to check it is a crossed check or special crossed check and the payment can only be made through the bank's account. Therefore, where a cheque is presented for payment which does not at the time of presentment appear to be crossed, or to have had a crossing which has been obliterated, or to have been added to or altered otherwise than as authorized by law, the banker paying the cheque in good faith and without negligence shall not be responsible or incur any liability.

In conclusion, the authentication of cheque's payment, the banker only has to prove that the cheque which was presented at that time, in front of him, has totally consisted of the conditions which specify by law but the authentic of compositions of each condition, it is not the duty of the banker to prove. For example, by the law, the banker has to prove that the cheque is uninterrupted series of endorsement, the cheque is not prohibited to be paid according to section 991 and 992 and if the cheque is be crossed, its payment only has to be made to a banker, but the banker has no duty to prove every endorsement which shew on the back of the cheque are authentic or not or the cross is be obliterated or not. If the banker has paid to the holder in good faith, without negligence and in the ordinary course of business, the banker is deemed to have paid the bill in due course.

2.5.2 Computer-Related Crime Act B.E. 2550

The Computer-Related Crime Act and the measure on authentication of electronic fund transfer. Because of computer is an electronic machine that easily to threaten, therefore they though to initial the concept of protection of internal computer system. These protection concepts mainly cover following principles which are Confidentially principle, Integrity principle, Availability principle and Non-Repudiation principle.

In Thailand, we took these concepts and adapt in the form of regulation to solve the initial of computer crime express following in Computer — Ralated Crime Act B.E.2550in section 5, 7, 9 and 1 0.In section 5 and 7, they regulated that whoever

accesses to a computer system or a computer data which have specific security measures are faulted. These sections are come from the principle of confidentially that undergoing the information will be kept secretly and only the authorizer can access to the information. And in section 9 and 10 regulated that whoever act in manner that cause damage , impairment , deletion , alteration or addition either in whole or in part of computer data and suspension , deceleration , obstruction or interference of a computer system of another person so that it cannot function normally are faulted. These sections are come from the principles of integrity and availability that guarantee any information will not be changed or damaged either act in accidently or intention and guarantee any information or services are ready to use in the time that need to use. And about the principle of non — repudiation is the assurance that someone cannot deny something. Typically, non - repudiation refers to the ability to ensure that a party to a contract or a communication cannot deny the authenticity of their signature on a document or the sending of a message that they originated are regulated in section 7 of Electronic Transactions Act B.E. 2544 (2001) that Information shall not be denied legal effect and enforceability solely on the ground that it is in the form of a data message.

2.5.3 Electronic Transaction Act B.E. 2544

1. Electronic Transaction Act B.E.2544 and the Authentication of Electronic Fund Transfer

The Electronic Fund Transaction Act B.E. 2544 has an aim to cover and support the electronic communication which could be occurred in the future. Due to the recent transactions are trended to change the methods of communication which used the coming innovation of technology which is more comfortable, fast and efficient. But the electronic transactions are different from normal transactions which were supporting by existing law. Therefore it is necessity to have a legal support and certify to treat the electronic information same as the normal information in writing.

The authentication is the process to certify the authentic of evidence or identify to prove that the user is the person he/she claim to be and has an aim to establish the association between a person and a data message for the purpose of

identifying the signatory who involves in such data message and showing that the signatory approves the information contained in such data message.

In this act, there are some sections which related to the measure on authentication that are the section 9 and sections about electronic signature.

According to the Section 7 of the Act, electronic information shall not be denied legal effect and enforceability like information in the form of paper. So, together with the Section 7, the Section 9 is prescribed about the entering of signature on the electronic information that in the case where a person is to enter a signature in writing, it should be deemed that such data message bears a signature if:

1) The method used is capable of identifying the signatory and indicating that the signatory has approved the information contained in such data message as being his own and

2) As such method is a reliable one. From the content in the section 9, this method is the authentication in the electronic transaction. It determines the authentication process widely for any electronic transactions. But the electronic payment transaction is different and risky than others. So, the problems are:

(1) The content in the Section 9 can be used for the authentication of the electronic payment transaction efficiently cannot it and

(2) It is a time to revise the recent regulations to have more specific in detail and up to date for the moment situation and also prepare for the new kinds of electronic transaction in the future isn't it.

The electronic signature is letter, character, number, sound or any other symbol created in electronic form and affixed to a data message in order to establish the association between a person and a data message for the purpose of identifying the signatory who involves in such data message and showing that the signatory approves the information contained in such data message. It is used to certified and confirm the authentic and exist of the electronic information and it is a method used is capable of identifying the signatory and indicating that the signatory has approved the information contained in such data message as being his own. Due to the section 7 and 9 of this Act have an aim to make an equality between the electronic information and the written information, so the electronic information has a same legal effect and enforcement as the written information. But where the case that a person is enter to sign for the electronic information, it has to have a method that can identify

the signatory and indicate that the signatory has approved the information contained in such data message as being his own and that method is electronic signature.

Nevertheless, the electronic signature which can use to sign for the electronic information and make it has a legal effect must be the reliable electronic signature which has the requirements in section 26 and be the signature that has legal effect which has the criteria in section 27-29.

2. Electronic Transaction Act B.E.2544 and the Electronic Fund Transfer Services

In this Act, there are some sections which related to the electronic fund transfer business service. In the section 32, persons shall have the right to operate service business relating to electronic transaction which includes the electronic fund transfer service. And to maintain financial and commercial stability, or for benefit of strengthening the credibility and acceptance of electronic transactions system , the law has prescribed that this kind of services has to have a Royal Decree to specify that which electronic transaction business shall be subject to prior notification, registration or license. Therefore the electronic fund transfer is kind of the electronic transaction business which has to follow the section 32 of the Act.

Due to the section 32 of this Act, the needed to operate the electronic fund transfer business have some related law as follow:

1. The Royal Decree on the control in electronic payment service business
2. The Proclamation of the electronic committee about
3. The Proclamation of the Bank of Thailand at Sor Ror Khor. 3/2552 about the policy and measure about the information security for service provider in the electronic payment business
4. The Royal Decree on Secured Procedure in Electronic Transaction B.E. 2553

1. The Royal Decree about the control in electronic payment service business

This Royal Decree is issued according to the section 37(2) of the Electronic Transaction Act which empowers the electronic committee to look after the

business about electronic transaction which including the electronic transaction business in section 32 of the same Act. And in the section 32, it is classified the electronic transaction business in 3 types which are the electronic transactions which shall be subject to prior notification, registration or licence.

In this Royal Decree, it is regulate about a kind of business which issue from the section 32 of the Electronic Transaction Act which is the electronic payment service business. The electronic payment service means the service about the transferring of money possession or the right of withdrawing or the right to debit one's account to another account.According to the definition of electronic payment, the electronic fund transfer which is the transfer of fund from one's account to another account is the kind of electronic payment, So the electronic fund transfer is under the control of this Royal Decree too.

Moreover, for the benefit of control, this Royal Decree has separate the kind of electronic payment business into three annexes which are the service which shall be subject to prior notification (A) , registration (B) and license (C). Which the electronic fund transfer is about the transfer of fund from one's account to another account through the electronic devices, so it is in the annex c that is the service business which subject to prior licence before servicing.

2. The Proclamation of the electronic committee about the criteria, methods and conditions in the electronic payment service business enterprise B.E. 2552

This proclamation is regulated about the criteria, methods and conditions for the electronic payment service business to follow and there are some contents which related to the authentication of electronic fund transfer.

Due to the electronic fund transfer is a kind of electronic payment service business in the annex C of the Royal Decree about the control in electronic payment service business which shall be subject to prior licence, so the service provider has to follow the criteria, methods and condition of this proclamation. In clause 9 of this proclamation, it is regulated that the service provider which need to operate the electronic payment service business according to the annex of the Royal Decree has to have the method of authentication to indicate the authorized person to

access to the information and along with the system to protect the unauthorized access and protect the integrity of information.

Therefore, the financial institution or service provider which want to have electronic fund transfer service has to create the criteria, methods and conditions about the authentication of access.

3. The Proclamation of the Bank of Thailand at SorRorKhor. 3/2552 about the policy and measure about the information security for service provider in the electronic payment business

This proclamation of the Bank of Thailand is regulated about the policy and measure about the information security needed for the financial service providers which want to do the electronic payment service business to follow. Which some content is related to the measure of authentication of electronic fund transfer because, in this proclamation, it specifies that the service provider has to have the method of authentication to identify and authorize the user before the user access to the account and make the electronic transaction. Moreover, the service provider has to use the proper technology which considered to the risk of the type of business such as Password, Personal Identification Number, Token or Smart Card, Biometric, or Public Key Infrastructure to prevent the non-repudiation.

However, the guideline in this proclamation is a widely framework because there are several kinds of electronic payment service and each payment has different risk. Which the electronic fund transfer is a kind of electronic payment but in this proclamation is not prescribe specially about the requirement of measure on authentication for the electronic fund transfer services.

4. The Royal Decree about Secured Procedure in Electronic Transaction B.E. 2553

The Royal Decree about secure procedure in electronic transaction and the measure on authentication of electronic fund transfer. The Royal Decree about secure procedure in electronic transaction is regulated about the standard of the information security which brought to use to control the information system has to be secured. This standard has to cover the confidentiality , integrity and availability of information system. In this Royal Decree, it provide three levels of standard of the

information security which are strict, average and basic. And which requirements of each standard have indicated in the annex of this Royal Decree.

Due to the Royal Decree is regulated that the electronic payment service which including the electronic fund transfer has to use the strict secure procedure. Therefore the service provider has to follow the requirements of the strict standard in the annex. Which there are some clause of the annex is related to the authentication which are clause 6.2 and 6.3. In these both clauses, it is specified that the service provider has to have the at least requirements for authentication and also has to policy about the technical use to encrypt the information.

In conclusion, the service provider which want to have the electronic fund transfer has to have the at least requirements for authentication.

Chapter 3
Foreign Regulations related to Measures on Authentication In Electronic Financial Transaction

3.1 The Revised Payment Service Directive and the European Banking Authority's Guideline

The new European measures on authentication are contained in the draft for Revised Payment Services Directive (PSD2) and in the European Banking Authority's Guidelines on the security of internet payments (EBA Guidelines).

The PSD2 and the EBA Guidelines contain similar authentication requirements. The EBA Guidelines were issued in December 2014 and will apply to customers in most EU countries on Aug. 1, 2015. We are waiting for the issuance of the final version of the PSD2, which will apply to customers in 2018, with an exact date of compliance yet to be issued.

The Revised Payment Service Directive or PSD2

The Directive on Payment Services (PSD) provides the legal foundation for the creation of an EU-wide single market for payments. The PSD aims at establishing a modern and comprehensive set of rules applicable to all payment services in the European Union. The target is to make cross-border payments as easy, efficient and secure as 'national' payments within a Member State. The PSD also seeks to improve competition by opening up payment markets to new entrants, thus fostering greater efficiency and cost-reduction. At the same time the Directive provides the necessary legal platform for the Single Euro Payments Area (SEPA).

In this Directive, it gave the definition of Authentication that means a procedure which allows the payment service provider to verify the identification of a payment service user or the validity of the use of a specific payment instrument, including the use of the user's personalized security credentials. Other than the authentication, this Directive creates a special authentication for an electronic payment which is more risked called Strong Customer Authentication.

The strong customer authentication is provided by the European Commission and the forthcoming European Banking Authority Regulatory Technical Standard on strong customer authentication and secure communication. It means an authentication based on the use of two or more elements categorized as knowledge (something only the user knows), possession (something only the user possesses) and inherence (something the user is) that are independent, in that the breach of one does not compromise the reliability of the others, and is designed in such a way as to protect the confidentiality of the authentication data. Then in the article 97, it specifies that the payment service provider has to apply the strong customer authentication when the payee:

1. to accesse its payment account online;
2. to initiate an electronic payment transaction;
3. to carry out any action through a remote channel which may imply a risk of payment fraud or other abuses.

And for the electronic remote payment transactions, the payment service providers shall apply the strong customer authentication that includes elements which dynamically link the transaction to a specific amount and a specific payee. The remote payment means the payment is made when the payment service user is not physically present at the point of sale: the interaction between the merchant and the client is ensured via internet through an electronic communication device such as computers, tablets and mobile phone. Because of the high risk of electronic remote payment transaction, it will have more complexity of authentication than usual.

However, it is not obey the service provider to apply the strong customer authentication in every case. In the article 98 of the Directive, it regulated the exemptions of application of the strong customer authentication that the exemptions shall be based on:

1. the level of risk involved in the service provided;
2. the amount, the recurrence of the transaction, or both;
3. the payment channel used for the execution of the transaction.

Finally, this Directive is issued to make the new standard of authentication for the financial payment transaction and to certain that the electronic payment transaction has more risk than normal transaction therefore why it should has the special method of authentication of itself. After having the PSD2 which regulated specially about the

authentication method for the electronic payment transaction, the European Banking Authority or EBA also issued the Guideline on internet payment to support the Directive.

The European Banking Authority's Guideline on the Security of Internet Payment

The Guidelines on the security of internet payments are based on the recommendations of the European Forum on the Security of Retail Payments (Secure Pay), a voluntary cooperative initiative set up by the ECB and comprising relevant authorities from the European Economic Area (EEA) with the aim of facilitating understanding of issues related to the security of electronic retail payment services.

They have scope to establish a set of minimum requirements in the field of the security of internet payments. The guidelines build on the rules of Directive 2007/64/EC3 (`Payment Services Directive', PSD) concerning information requirements for payment services and obligations of payment services providers (PSPs) in relation to the provision of payment services. Furthermore, Article 10(4) of the Directive requires payment institutions to have in place robust governance arrangements and adequate internal control mechanisms.

So, the EBA's guideline and PSD2 have some same contents especially for the strong customer authentication.

What is defined as strong customer authentication?

The PSD2 and the EBA Guidelines define strong authentication as authentication through at least two out of the following three factors:

1. Something only the user knows like pass code or PIN;
2. Something only the user possesses; like mobile phone or token; or
3. Something the user is; like a fingerprint.

The PSD2 and the EBA Guidelines require that the selected factors must be mutually independent in that the breach of one does not compromise the reliability of the other. Although the legal definition of strong authentication is largely the same, there are two differences between the PSD2 and the EBA Guidelines in relation to the authentication factors.

1. First, the EBA Guidelines dictate that at least one of the factors used should be:

"Non-reusable";

"Non-replicable (except for inherence)";

"Not capable of being surreptitiously stolen via the internet".

These conditions, which are not required under the PSD2, are difficult to meet in a world where information lives on the internet and can easily be replicated like in an e-commerce transactions.

2. Second, the PSD2 sets forth an even more stringent requirement: strong customer authentication for electronic remote payment transactions must include elements linking the authentication to a specific amount and a specific merchant in the form of a dynamic code.

When will strong authentication apply?

Under the EBA Guidelines, strong authentication will apply to the initiation of internet and mobile browser-based payments, virtual card payments, the registration of card payment data for use in digital wallets, and access to sensitive payment data.

Under the PSD2, strong authentication will apply to access to payment accounts online, to the initiation of any electronic payment transaction, and to any action through a remote channel which may imply a risk of payment fraud or other abuses, including online or mobile payments.

Which transactions will escape strong authentication?

While strong authentication will be the rule for e-commerce transactions, the use of alternative authentication measures will be permitted only as a way of exception. The PSD2 and the EBA Guidelines allow customers to use alternative authentication measures for specific categories of transactions.

In particular, the EBA Guidelines allows alternative authentication measures for low-risk or low-value payments. The PSD2 allows alternative authentication measures also on the basis of the recurrence of the transaction and the payment channel used for the execution of the transaction.

Conclusion, both directive and guidelines have the same aim for establishing the standard of authentication of electronic payment transaction because they are realized about the risk which could be happened when the consumer make the transaction in electronic devices and internet network. Especially for the EBA's guideline which show the interesting in security of electronic transaction because they expand the application of strong customer authentication for all internet transaction

which is wider than the Directive which restrict the application only for the electronic payment transactions.

3.2 The Law and Regulations about Measure on Authentication of Electronic Fund Transfer in the United States of America

From our detection, the United State of America has laws and regulations about measure on authentication of electronic fund transfer which are Uniform Commercial Code Article 4A, Electronic Fund Transfer Act 1978 and Regulation E.

In Uniform Commercial Code (UCC) Article 4A is about the fund transfer which has the payment order to transfer credit from one account to another account with have the relevant parties which are Sender, Originator's Bank , Receiving Bank , Beneficiary's Bank and Beneficiary.

The legal relationship is presumed that bank is a collecting agent and a paying agent of sender, in the other hand, the relationship between bank and customer is creditor and debtor in the contract of commercial bank business service.

In the UCC is definition the meaning of fund transfer is an Article 4A-103(a)(1), "Payment order" means an instruction of a sender to a receiving bank, transmitted orally, electronically, or in writing, to pay, or to cause another bank to pay, a fixed or determinable amount of money to a beneficiary if all of the following apply:

(i) The instruction does not state a condition to payment to the beneficiary other than time of payment.

(ii) The receiving bank is to be reimbursed by debiting an account of, or otherwise receiving payment from, the sender.

(iii) The instruction is transmitted by the sender directly to the receiving bank or to an agent, funds-transfer system, or communication system for transmittal to the receiving bank.

The sufficiency of fund transfer by the UCC Article 4A-40 is the time that beneficary's bank accept the payment order for the benefit of beneficiary.

Therefore, the bank should have the security procedure for the trustworthiness of the payment order and it the UCC Article 4A-202(b) said that the customer will bears the loss if the bank proves that:

1. it properly verified the payment order with a security procedure agreed to by the customer (A security procedure is the use of devices such as passwords and cryptographic codes to show the authenticity of a message.);

2. the security procedure is "commercially reasonable";

3. it acted in compliance with any written instructions from the customer restricting the acceptance of payment orders that purport to come from the customer; and

4. it acted in good faith.

While, the security procedure is the process established by the agreement between customer and bank (Receiving Bank) for the purpose of confirmation of payment order on any communication, changing or exhaustion of payment order. So it need to have to use many of forms including processes to solve the problems which have to have evidences in written, number, regulations or any types of securities.

Secondly, the Electronic Fund Transfer Act 1978 and Regulation's E, they are regulated to enforce for any transaction which the customer use the electronic procedure to transfer the credit out from his account. In this act, it's special written about the unauthorized electronic fund transfer that means the electronic fund transfer from the user's account which the process has not done by the customer and the customer does not receive the beneficiary from that transfer.

In these regulations, it written about the liability of financial institution in electronic fund transfer which can explain as follow.

1. The liability of bank in section 1693h, the financial institution's shall be liable to a customer for all damages proximately caused by-

1) The financial institution's failure to make an electronic fund transfer, in accordance with the terms and conditions of account, in the correct amount or in a timely manner when properly instructed to do so by the customer, except where-

a) The customer's account has insufficient funds;

b) The funds are subject to legal process or other encumbrance restricting such transfer

c) Such transfer would exceed an established credit limit;

c) An electronic terminal has insufficient cash to complete the transaction; or

e) As otherwise provided in regulations of the Bureau;'

2) The financial institution's failure to make an electronic fund transfer due to insufficient fund when the financial institution failed to credit, in accordance with the terms and conditions of an account, a deposit of funds to the customer's account which would have provided sufficient funds to make the transfer, and

3) The financial institution's failure to stop payment of a preauthorized transfer from a customer's account when instructed to do so in accordance with the terms and conditions of the account.

2. Act of God and Technical Malfunctions. A financial institution shall not be liable if the financial institution show by a preponderance of the evidence that its action or failure to act resulted from-

An act of God or other circumstance beyond its control, that it exercised reasonable care to prevent such an occurrence, and that it exercised such diligence as the circumstances required; or

A technical malfunction which was known to the customer at the time he attempted to initiate an electronic fund transfer or, in the case of a preauthorized transfer, at the time such transfer should have occurred.

3. In the case of a failure described in 1. which was not intentional and which resulted from a bona fide error, notwithstanding the maintenance of procedures reasonably adapted to avoid any such error, the financial institution shall be liable for actual damages proved. (Electronic Fund Transfer Act 1978 Section 1693h)

4. the liability of financial institution and customer in unauthorized electronic fund transfer

In Electronic Fund Transfer Act 1978 Section 1693g, a customer shall be liable for any unauthorized electronic fund transfer involving the account of such customer only if the card or other means of access utilized for such transfer was an accepted card or other means of access and if the issuer of such card, code, or other means of access has provided a means whereby the user of such card, code, or other means of access can be identified as the person authorized to use it, such as by signature, photograph, or fingerprint or by electronic or mechanical confirmation. In no event, however, shall a customer's liability for an unauthorized transfer exceed the lesser of

(1) $50; or

(2) the amount of money or value of property or services obtained in such unauthorized electronic fund transfer prior to the time the financial institution is notified of, or otherwise becomes aware of, circumstances which lead to the reasonable belief that an unauthorized electronic fund transfer involving the customer's account has been or may be effected. Notice under this paragraph is sufficient when such steps have been taken as may be reasonably required in the ordinary course of business to provide the financial institution with the pertinent information, whether or not any particular officer, employee, or agent of the financial institution does in fact receive such information.

Notwithstanding the foregoing, reimbursement need not be made to the customer for losses the financial institution establishes would not have occurred but for the failure of the customer to report within sixty days of transmittal of the statement (or in extenuating circumstances such as extended travel or hospitalization, within a reasonable time under the circumstances) any unauthorized electronic fund transfer or account error which appears on the periodic statement provided to the customer under section 1693d of this title. In addition, reimbursement need not be made to the customer for losses which the financial institution establishes would not have occurred but for the failure of the customer to report any loss or theft of a card or other means of access within two business days after the customer learns of the loss or theft (or in extenuating circumstances such as extended travel or hospitalization, within a longer period which is reasonable under the circumstances), but the customer's liability under this subsection in any such case may not exceed a total of $500, or the amount of unauthorized electronic fund transfers which occur following the close of two business days (or such longer period) after the customer learns of the loss or theft but prior to notice to the financial institution under this subsection, whichever is less. (Electronic Fund Transfer Act 1978 Section 1693g)

The liability of financial institution in unauthorized electronic fund transfer

In the Electronic Fund Transfer Act 1978 (EFTA), it determine that the financial institution shall be liable in the case of the electronic device do not work as the order of customer and the liability as limited as they can prove for the real damage.

However, there is the judgment ([21] the judgement in case between Ognibene V. City bank) to extent the interpretation of unauthorized electronic fund transfer. The EFT Act places various limits on a customer's liability for electronic fund transfers from his account if they are "unauthorized". Insofar as is relevant here, a transfer is "unauthorized" if —

(1) it is initiated by a person other than the customer and without actual authority to initiate such transfer,

(2) the customer receives no benefit from it, and

(3) the customer did not furnish such person "with the card, code, or other means of access" to his account.

3.3 The Electronic Financial Transaction Act 2013 and Enforcement Decree of the Electronic Financial Transaction Act 2014 of the Republic of Korea

This Act has a purpose to contribute ensuring the security and reliability of electronic financial transactions by clarifying their legal relations and to promoting financial conveniences for people and develop the national economy by creating a foundation for the sound development of electronic financial industry.

The Electronic Financial Transaction Act and the Authentication of Electronic Fund Transfer

In this Act, it gives the definition of the electronic fund transfer that means any transfer of funds made by a payer which has an account with a financial company made a payment request through an electronic device for transferring the funds to a payee. The transfer is deemed to be completed when the information on the amount transfer on a request is recorded on the payee's account and also the payee's account is open.

---

[21] Judgement between Ognibene V. City Bank, Civil Court of the City of New York, New York Country, December 9, 1981, Judge Mara T T. Thorpe. at http://vvww leagle.com/decision/1981331112Misc2d219 1285/OGNIBEN E%20v.%20CITIBANK, (last visited 27 December 2016).

Before the payer made a payment request, the financial company has to have a process to confirm the identity and authority of user, but it is not called authentication, it is called means of access.

In the article 2 clause 10, the means of access means any of the following means or information which is used to issue a transaction request in electronic financial transactions.or to secure the authenticity and accuracy of users and the details of such transaction:

1. An electronic card or other electronic information equivalent thereto;
2. An electronic signature creating key;
3. A user number registered with a financial company or an electronic financial business operator;
4. Biological information of users;
5. A password required to use the means or information reffered to in item 1. or 2.

According to the article 6, it is the duty of the financial company to select, use and manage the proper means of access for the users. And it has requirement for the means of access which are:

1. The means of access is capable to confirm the identity and authority of a user and;
2. The financial company shall issue the means of access only if an application is made by the user after verifying the identity of such user.

Not only the financial company has duty to issue the means of access for the user, but the user also has duty to protect and keep his means of access and do not commit any offenses which regulated in the article 6(3) which are:

1. To acquire or transfer a means of access;
2. To borrow or lend a means of access with compensation;
3. To provide a means of access subject to a right of pledge;
4. To assist such acts prescribed in 1) through 3).

So, if the user has rented a means of access or delegated the user thereof to a third person, or has offered the means of access as an object of transfer or security, it shall be deemed as the gross negligence of the user and when the user suffer any loss due to this incidents, the financial company shall not be liable for indemnifying the user for the loss.

Moreover in the regulations, the Korea is the initial country to use the biometric factor as an authentication measure in the electronic financial transaction. The KEB Hana Bank in Korea has launched fingerprint authentication-based account transfers. It is the first bank to allow customers to use fingerprint authentication (Biometric authentication) for account funds transfers for its smart phone banking system. Fingerprint authentication is a strong security measure that adds encrypted identify authentication tool to biometric authentication based on FIDO (Fast Identity Online). By merely registering their fingerprints on their smart phones, customers will be able to perform identity authentication more securely and conveniently than if they had used the existing digital certificate.

This service can be used only on smart phone that have fingerprint recognition capabilities. Later, the service will be upgraded to non-contract authentication (i.e. picture-taking), meaning that customers will not be possible to use the service on all devices, iPhone or Android phones, even those without fingerprint sensors.

Furthermore, KEB Hana Bank plans to launch the T-OTP, which operates inside the "secure zone" of smart phones. This service will be the first of its kind in Korea. T-OTP (TrustZone-One-Time Password) is an incredibly secure service, as it is based on hardware that generates one-time passwords online and operates from within the secure zone of smart phones.

With the introduction of the T-OTP service, customers no longer need to carry around one-time passwords generators to access smart phone banking. So far, customers have had to visit branch officers to have their security medium issued when they wish to be registered as an online-banking service user, but as the T-OTP is issued via smart phone, customers do not have to go a branch office.

Chapter 4
Analysis of the Problems

4.1 The Problems about Authentication of Electronic Fund Transfer

Electronic Fund Transfer means any transfer of funds from an account opened with financial institutions to another account through electronic devices for purposing of transferring funds between a payer (customer) and a payee (beneficiary). It is a kind of electronic payment. The electronic fund transfer enables financial transactions from anywhere, and its allow a non-stop working. Its process helps receiver to receive the fund immediately instead of waiting for a day like electronic cheque transfers. However, the electronic fund transfer is a remote electronic transaction which does not made in front of the bankers, while the bankers cannot exactly know who is the real one of transfer or therefore it has the risk of unauthorized access and fraudulent and the bankers have to have the authentication process to identify and verify the authenticity of user before they made the transactions.

Furthermore, authentication is a technical process to verify the authenticity of users and to confirm that the user is the real person who is authorized or be a delegation of authority to make a transaction. In practically, the authentication mechanism could be separated in three factors which are as followed:

1. The possession factor or something that the user have such as key, card, and etc.,
2. The knowledge factor or something that the user know such as password, pin, and etc. and,
3. The biometric factor or something that the user is such as retinal pattern, voice pattern, fingerprint, and etc.

Also, the authentication procedure is the way to use these factors to describe the encrypted electronic information and when the information is decrypted, it means that the user is authentic and access through the information. Then the combination of factors more than one factor will increase the difficulty of decryption and increase the strength and complexity of that authentication.

There are various types of authentication mechanisms used in electronic payment service. For examples, the electronic fund transfer via the ATM is used the combination of two factors between the possession factor which is a card and the knowledge factor which is a PIN (Personal Identification Number) or the electronic fund transfer via the application on smart phone which is also used the combination of two factors between the possession factor which is a smart phone and the knowledge factor which is the OTP (One time password). Although both transactions have used the two-factor-authentication but their procedures are different.

For the ATM transaction, it used a card which has a magnetic stripe which recorded the information of the card's holder and when it was read, it will identify who is the user. After that the user has to press a PIN code for authentication himself. Nowadays, the Bank of Thailand is concerned about the security of customer from the damages which could be occurred in the ATM transaction so it released the Press No. 22/2016: Migration of ATM and Debit Cards to Thai Standard Chip Cards on 4 May, 2016. The Payment Systems Committee formulated a policy for financial institutions to migrate magnetic stripe ATM and debit cards to chip cards. This policy is a crucial measure to increase security for cardholders, solving counterfeit card frauds whereby magnetic stripe cards are skimmed to make unauthorized payments and cash withdrawals. This measure will enhance customers' confidence in using ATM and debit cards for financial transactions via ATMs as well as paying for goods and services via point-of-sale (POS) terminals instead of using cash. In addition, this policy aligns with many other countries including ASEAN members. Chip cards are cards that come with an embedded microchip on the card itself. The chip on the card dynamically communicates with a chip-enabled card reader when you make a purchase, verifying your PIN and creating a unique code for each transaction in real time, all before approving a purchase. This new technology adds a layer of sophistication and verification to the transaction process, making your information more secure and harder to replicate because:

1) It is significantly more difficult and expensive to counterfeit.

2) It cannot be scanned a microchip remotely.

3) The chip card generates a unique one-time code that's needed for the transaction to be approved. It is a feature that is virtually impossible to replicate in a counterfeit card.

Besides, although the authentication is very important but actually it still a technical process and the laws and guidelines which related to it is wide and board. However, there is a reason why the laws cannot be legislated too much in detail of them about the authentication in electronic fund transfer which is the technical process because to take the technical process legislated in the form of laws will make that law be harsh and unyielding. So it is the source of the study that whether it should have specific legal measure on authentication of electronic fund transfer in the objective of increasing the standard of authentication and efficiency of enforcement or not and if it is possible, how its detail will be.

The problems of the authentication of electronic fund transfer:

First is the problem about laws and guidelines about the authentication of electronic fund transfer. There are some laws and guidelines which have the content about the authentication of electronic fund transfer but their content is not legislated directly about the legal measures or requirements for the proper authentication used for the electronic payment services.

According to the Section 9 and 25 of the Electronic Transaction Act, they have described about the reliable authentication for the electronic transactions. Regarding to the Section 9, the reliable authentication is the method used to capable of identifying the signatory and indicating that the signatory has approved the information contained in such data message as being his own and that method is a reliable one and appropriate for the purpose for which the data message is generated or sent, having regard to the surrounding circumstances or an agreement between the parties.

Furthermore, the Section 9 has been expanded the definition of a reliable method that it has to consider about: 1) the stability and security of methods or instruments for identification. It means that these methods or instruments have to have the technologies which can protect the confidentiality (to confirm that the information will be kept secretly), integrity (to confirm that the information will not be changed or destroyed), availability (to confirm that the information will be available to use in the needed time) and non-repudiation (to prevent the denial of a communication between the sender and the receiver) of information and 2) the characteristic. types, value or risk of the transactions and 3) the security of communication system. The reliable methods of the Section 9 is strong and follow to the aim of the Act that regulations shall cover and support the electronic communications, which can be occurred in the

future. Also, the reliable method of the Section 9 is the standard of authentication for all electronic transactions.

Additionally, the Bank of Thailand released the Proclamation at Sor Ror Khor. 3/2552 about the policies and measures about the information security for service provider in the electronic payment business. The content has been considered about the normal framework of information in security for the service provider to use as the guideline but the service provider also can create their own measures, which are different from the framework if they can prevent the risk of information security efficiently and reliably. In the clause 1.3 Authentication and Non-repudiation of this Press is written about types and measures of authentication that the service providers have to have the authentication process which is suitable for the risk of the services and given the examples of authentication technologies which are Password, Personal Identification Number, Token or Smart Card, Biometric information and Public Key Infrastructure. In the part of measure, it described that the service provider has to have the authentication process before the user access the system to recognize the authority and prevent the non-repudiation and also has to record the detail of access for using as the evidence.

From the studying of the Directive (EU) on payment services in the internal market 2015 and the European Banking Authority's Guideline on the security of internet payment, they established a set of minimum requirements of authentication in the electronic payment services. According to the Directive, it created the Strong Customer Authentication which means that an authentication based on the using of two or more elements categorized as Knowledge (Something only the user knows such as Password and PIN Code), Possession (Something only the user possesses such as Card and Smartphone), and Inherence (Something the user is such as Biometric information) that are independent, in that the breach of one does not compromise the reliability of the others, and it is designed in such a way as to protect the confidentiality of the authentication data. Then in the Article 97 of this Directive, it is regulated that the payment service providers or bankers shall be applied strong customer authentication where the payer: 1) accesses its payment account online, 2) initiates an electronic payment transaction or 3) carries out any action through a remote channel which may imply a risk of payment fraud or other abuses. This Directive has been taken the technical processes of authentication to the form of regulations that was interested and

modern. Meanwhile, this Directive could be a good guideline labour law in the sense that the strong customer authentication will be useful for adapting and developing as the authentication measures in the electronic fund transfer.

From the analyzing, the electronic fund transfer is risk more than other electronic transactions because it is the remote electronic transactions which does not conduct in front of the bankers, it has only the technical authentication process to verify the authenticity of the user before made the transaction and it has no specific regulation written to specify the legal requirements or measures for it like the foreign laws. Although to have the regulations about legal measure on authentication will be useful and there are the foreign regulations which regulated about the specific legal measures on authentication called strong customer authentication which should be adapted as the example but:

1. In reality, our bankers have already used the strong customer authentication practically. For the ATM transaction, they used the Card and PIN as the authentication mechanism in electronic payment by ATM which same as the strong customer authentication because it is the used of two elements categorized as Knowledge (PIN Code) and Possession (Card) that are independent. So it may be unessential to have the regulation about the strong customer authentication because it has already been used practically.

2. To regulate the technical measures in the form of regulations can make that regulations be harsh and unyielding because the efficient law could cover and use for all the electronic transactions which may occur in the future. And

3. The reliable method in the Section 9 of the Electronic Transaction Act is strong, stable and safe enough to protect the confidentiality, integrity and availability of information security and to be the based for the developer to create the technical authentication process. Therefore in the opinion of writer, it is not essential to have the specific regulations about the authentication of electronic fund transfer.

However, the EU Directive could be used as the good guideline for developing our measure about authentication in the electronic payment services. So, in the future, the Bank of Thailand may have the consideration of adding more about the security measures of authentication of the electronic payments in its recent proclamation by adapting or developing from this Directive.

Secondly, it was recognized as the problem of using biometric factor as a mechanism in the authentication of electronic fund transfer. To use the biometric information as an authentication mechanism is not famous. From the studying of European Union Agency, the majority of people do not realize comfortable with granting permission on the storage of their biometric information. While, it was risk because the biometric data is compromised forever and if there are the potential attacks to a centralized data base storage, the damages will be occurred. Another important factor is the usability, since current technologies do not provide 100% of accuracy at the first try. However, the biometric factor also has advantages: 1) the responsibility of the storage is transferred to the end user, 2) the chances of a successful threat to steal large amount of biometric information is low, because the threat should be successful on many devices and stores, 3) the biometric identification vector does not have to travel over the network. After comparing its advantages and disadvantages, it is useful and interesting to bring the biometric factor as an authentication mechanism of electronic fund transfer because 1) it is compromised forever and difficult to copy or replicate, 2) the user do not need to remember hard and long password, 3) the unauthorized access is hard to occur and 4) by technical process, the biometric information does not travel over the network and hard to be stolen and 5) the recent technologies is supported to use the biometric factor as the authentication process in the electronic payment such as the fingerprint scanning on the smartphone.

Regarding to the Cause 1.3 of the Bank of Thailand Proclamation at Sor Ror Khor 3/2552, it described about the authentication system which used the proper technologies coverage for the risk of electronic payment and it given the biometric information as the example of that proper technology. From the press, it means that the Bank of Thailand has vision and expectation of taking the biometric technology used as the mechanism in the authentication process of electronic payment. Moreover, this Cause is expanded and cleared the definition of electronic signature in the Electronic Transaction Act that its definition is involved and covered the biometric information too.

Practically, there is a Korean bank launched a fingerprint authentication-based account transfers. Fingerprint authentication is a strong security measure that adds encrypted identify authentication tool to biometric authentication based on FIDO (Fast

Identity Online). But this service can be used only on smartphone that have fingerprint recognition capabilities. So, it is exciting if our bankers interest and initiate to use the biometric information as an authentication mechanism in the electronic payment services.

Third is the problem of the farness between bankers and customers. The electronic fund transfer is a remote electronic and online transaction that does not need to face with the bankers. So, the bankers may see the users only the first time that they registered to use the services. Because of the benefits of technology, the users do not need to visit the bankers therefore it is difficult for the bankers for checking the authenticity and change of the users such as their faces. In governed organizations such as the Administrative courts and the department of Consular Affairs, while the customers having the services, not only they have to identify themselves by showing the identification card or other cards which can identify as the identification card but the service providers will ask them to take a photo of themselves too. To take a photo of the customer is benefit that the service providers can check the authentic of customer by comparing between their faces on the photo and the card of the customers. Moreover, these photos are benefit to use as the evidence when the customer made the troubles.

In practically, the bankers have a process called context authentication. The context authentication is the process from the server side to check the authenticity of the user based on the behavior, location or device used and other parameters. So, it is very useful if the bankers take the process of taking photo of the customer as a part of the context authentication while the users interact with the service. For example, in the electronic payment service on smartphone, the bankers may create the process that made the customer to take their photo after using the application. This process is advantages that: 1) the service providers can check the authenticity of the customer from comparing the faces, 2) the service providers will receive and storage a recent picture of the customer and 3) the photo is a benefit evidence when the troubles were occurred.

Forth is the problem about the hearing of electronic evidence in the court. When there is a mistake in the electronic fund transfer, it has to use any related evidence to prove who has to bear the liability for that mistake. Because the electronic fund transfer is worked on electronic devices and computers so the evidence is the

electronic devices which is used to transfer the fund. The electronic evidence is a kind of material evidence so the bankers who controlled the electronic devices and computers have to prove about the kinds of devices, their generality,not about the data consisted in the devices. In this case, the bankers will invite the computer specialist to help him to explain about the functions and processes of technologies about the authentication in the court and it may be difficult for the judge to understand the technical procedures. Therefore if we havethe specific measures on authentication in writing, it will be useful that: 1) the bankerhas to prove only that his authentication process is followed the written measures or not.lf the bankers can prove that his authentication is followed the specific measures on authentication for the electronic fund transfer, he will receive the benefit of legal presumption and will push the burden of prove to the user instead. So the user will have the duty to prove his honesty and gross negligence of using the device. And 2) the judge will understand about measure on authentication and the dispute title easier because it has been described in writing, which it could be beneficial for the examination of evidence in the court.

Finally, it is not essential to take the technical process of authentication especially about the strong customer authentication to the form of regulations because it will make that law to be harsh and unyielding and the authentication methods in the Section 9 of the Electronic Transaction Act is still strong and efficient enough for prevent the information security of the user in the electronic transactions. However, the EU Directive is also the good guideline in the sense that the strong customer authentication could be considered and adapted to develop our authentication measure in the electronic payment in the future. Moreover, it will be excited and useful if our bankers interest and initiate to use the biometric information as a part of authentication mechanism and to have the process of taking photo of user while making the transactions.

4.2 The Guidelines Concerning Legal Measure on Authentication of Electronic Fund Transfer

As it is written above that to regulate the technical process in the form of regulation will make that regulation be harsh and unyielding and cannot cover all

electronic transactions efficiently. However, if it is possible to add or alter the measures on authentication of electronic payment, the Bank of Thailand may have the consideration of adding more or alteration about the security measures on the authentication of electronic payment.

So if it is possible to add more the content about security measures on authentication of electronic payment, that content shall be written in the part of security measures and prescribed as follow:

First is to determine the definition of the strong customer authentication. "Strong customer authentication" means an authentication based on the use of two or more of the following factor: Something only the user know , Something only the user possesses or Something only the user is. The selected factor must be independent in that breach of one does not compromise the reliability of the other.

Second is to describe the use of the strong customer authentication that the bankers shall ensure to apply the strong customer authentication where the payer:

(a) Accesses its account online;

(b) Initiates an electronic fund transfer or;

(c) Carries out any action through a remote channel which may imply a risk of payment fraud or other abuse.

Moreover, for electronic remote fund transfer, the strong customer authentication must include factor linking the authentication to a specific amount and a specific payee or beneficiary in the form of a dynamic cord.

Third is to specify the exemption of use of the strong customer authentication. The exemptions of application shall be based on the following criteria:

(a) The level of risk;

(b) The amount,

(c) The payment channel used for the execution of the transaction.

Chapter 5
Conclusion and Recommendations

5.1 Conclusion

The Electronic fund transfer is a process to transfer of fund from one account to another account via internet network though the accounts which opened in the same or different places. So, the electronic fund transfer process is related to the computer information security because they use computer system and internet network to be parts of transferring process. The computer information security rests on the confidentiality (the concealment of information or resource), integrity (the trustworthiness of data or resources) and availability (the ability to use the information or resource). However, the internet network is a public network that can access by any computer therefore how can we reassure customers who come to the account that they are the real one, not a fake setup to steal the credit. To protect this spoofing problem, the financial institutions or banker shave created the authentication process to identify and verify the user before they access to the account and make the transactions.

The authentication is the technical process to verify the authentic of evidence or identity to prove that the user is the person who he claims to he and has authority to access to the account. Authentication factors can separate in three factors which are Possession factor (Something the user has),Knowledge factor (Something the user know) and Biometric factor (Something the user are). To protect the customer credential and prevent the attack to customer's account, the financial institutions use the authentication methods to identify and verify the user before making the financial transactions. The strength of authentication is depended on the combination of authentication factors.

However, the authentication is only the technical process which the laws and guideline could not supported efficiently because their content are wide and board.

In the section 9 of the Electronic Transaction Act, it is described about the reliable authentication of the electronic transactions. The reliable authentication shall be capable of identification of the owner and it is a reliable one which can protect the confidentiality, integrity, availability and non-repudiation of the security information.

Moreover, there is the proclamation of the Bank of Thailand which supported, expanded and described that the reliable authentication can be used in the form of Password, PIN, PKI or Biometric information but the use of them have to be proper and cover enough for the risk of the transactions. Although the security measures of Section 9 are strong and cover enough for all electronic transactions but the electronic fund transfer is actually risk more than others. And when comparing to the foreign regulations, there is a specific legal measure on authentication about the electronic payments which called the strong customer authentication.

In practically, the recent technologies used for authentication are same as the strong customer authentication so it may be unessential to have the specific regulations about the authentication of electronic fund transfer and it will made the law be harsh and unyielding when bringing the technical process to the form of regulations. However, this EU Directive will be the good guideline in the future when the law is revising or when the Bank of Thailand has a consideration of alteration or adding more about the security measure for authentication of electronic payment in its proclamations.

From researching and analyzing of law, regulation, concept and system about authentication of electronic fund transfer, we found that there are some laws about the authentication of electronic fund transfer but they are not specific and cover enough which could cause the problems in the future. So the writer has detected the important problems and written them in conclusion and implementing the recommendation as follow.

5.2 Recommendations

I. The Bank of Thailand may have the consideration of adding more content about the measures on authentication in the electronic payments in the future by using the EU Directive as the guideline. And the content may be similar to the content in Chapter 4.2.2.

2. The Bankers shall try to bring the biometric information used as the authentication mechanism for the electronic payment. The biometric factor is advantages for using as the authentication mechanism because it is difficult to copy or

replicate, the user do not need to remember the password. the unauthorized access is hard to be occurred and the biometric factor does not travel over the network. Moreover, the recent technology is supported to use the biometric information such as the smallphone which have the fingerprint scanner.

3. The Bankers shall try to have the process of taking photo as another context authentication in the electronic payment service and issue the proclamation for the bankers to have the process of taking photo while the user making the electronic payment transaction via the smart phone. The photo of user will be helped the bankers to check the authenticity of user by comparing of the user's face. Moreover, it can indicate the position of the user while making the transaction too.

Appendices

Appendix A

The Regulations about Cheques of the Civil and Commercial Code

The Civil and Commercial Code

Chapter 4

Cheques

Section 990. The holder of a cheque must present it for payment to the banker within one month one month after the date of issue if it is payable in the same town where it is issued, or within three months if it is payable elsewhere; otherwise he loses his right of recourse against the endorsers; he also loses his right aginst the drawer to the extent of any injury caused to the drawer by failure of such presentment

Section 991.A banker is bound to pay a cheque drawn on him by his customer unless:

(1) There is not enough money to the credit of the account of the customer to meet the cheque, or

(2) The cheque is presented for payment later than six months after the date of drawing, or

(3) Notice is given that the cheque has been lost or stolen.

Section 992.The duty and authority of a banker to pay a cheque drawn on him come to an end on the following cases:

(1) Countermand of payment;

(2) Knowledge of the drawer's death;

(3) Knowledge or publication of an interim receiving order or bankruptcy order against the drawer.

Section 994.If a cheque bears across its face two parallel transverse lines either with or without the words "and company" or any abbreviation thereof between such lines, it is said to be crossed generally and payment of it can only be made to a banker.

If between such lines a name of any particular banker is inserted, such cheque is said to be crossed specially and payment of it can only be made to that banker.

Section 997. Where a cheque is crossed specially to more than one banker, the banker on whom it is drawn shall refuse payment thereof ; except when it is crossed to an agent for collection being a banker.

Where a banker on whom a cheque is drawn which is so crossed nevertheless pays the same , or pays a cheque crossed generally otherwise than through a banker , or if crossed specially otherwise than to the banker to whom it is crossed or his agent for collection being a banker , he is liable to the true owner of the cheque for any loss he may sustain owing to the cheque having been so paid.

Provided that where a cheque is presented for payment which does not at the time of presentment appear to be crossed, or to have had a crossing which has been obliterated , or to have been added to or altered otherwise than as authorized by law , the banker paying the cheque in good faith and without negligence shall not be responsible or incur any liability.

Section 998.Where the banker, on whom a crossed cheque is drawn, in good faith and without negligence pays it, if crossed generally, to a banker, and if crossed specially, to the banker to whom it is crossed, or his agent for collection being a banker, the banker paying the cheque, and, if the cheque has come into the hands of the payee, the drawer, shall respectively be entitled to the same rights and be placed in the same position as if payment of the cheque had been made to the true owner thereof.

Section 1000.Where a banker in good faith and without negligence receives payment for a customer of a cheque crossed generally or specially to himself , and the customer has no title or a defective title thereto , the banker shall not incur any liability to the true owner of the cheque by reason only of having received such payment.

Section 1009.When a bill payable to order on demand is drawn on a banker , and the banker on whom it is drawn pays the bill in good faith , without negligence and in the ordinary course of business, it is not incumbent on the banker to show that the endorsement of the payee or any subsequent endorsement was made by or under the authority of the person whose endorsement it purports to be , and the banker is deemed to have paid the bill in due course, although such endorsement has been forged or made without authority.

Appendix B

The Regulations of The Computer-Related Crime Act B.E. 2550

Computer — Related Crime Act B.E. 2550

Section 5. Whoever illegally accesses to a computer system that has specific security measures and such security measures are not intended for his use, shall be liable to imprisonment for a term not exceeding six months or to a fine not exceeding ten thousand Baht or to both

Section 7. Whoever illegally accesses to a computer data that has specific security measures which are not intended for his use, shall be liable to imprisonment for a term not exceeding two years or to a fine not exceeding forty thousand Baht or to both.

Section 9. Whoever illegally acts in a manner that causes damage, impairment, deletion, alteration or addition either in whole or in part of computer data of another person , shall be liable to imprisonment for a term not exceeding five years or to a fine not exceeding one hundred thousand Baht or to both.

Section 10. Whoever illegally acts in a manner that causes suspension , deceleration , obstruction or interference of a computer system of another person so that it cannot function normally shall be liable to imprisonment for a term not exceeding five years or a fine not exceeding one hundred thousand Baht or to both.

Appendix C

The Regulations of Electronic Transaction Act B.E. 2544

ELECTRONIC TRANSACTION ACT B.E.2544

Definition

Section 4

"electronic transaction" means a transaction in which an electronic means is used in whole or in part

"electronic signature" means letter, character, number, sound or any other symbol created in electronic form and affixed to a data message in order to establish the association between a person and a data message for the purpose of identifying the signatory who involves in such data message and showing that the signatory approves the information contained in such data message

CHAPTER 1
ELECTRONIC TRANSACTIONS

Section 7. Information shall not be denied legal effect and enforceability solely on the ground that it is in the form of a data message.

Section 9. In the case where a person is to enter a signature in a writing, it shall be deemed that such data message bears a signature if:

(1) the method used is capable of identifying the signatory and indicating that the signatory has approved the information contained in such data message as being his own

(2) such method is a reliable one and appropriate for the purpose for which the data message is generated or sent, having regard to the surrounding circumstances or an agreement between the parties.

CHAPTER 2
ELECTRONIC SIGNATURES

Section 26. An electronic signature is considered to be a reliable electronic signature if it meets the following requirements:

(1) the signature creation data are, within the context in which they are used, linked to the signatory and to no other person;

(2) the signature creation data were, at the time of signing, under the control of the signatory and of no other person;

(3) any alteration to the electronic signature, made after the time of signing, is detectable; and

(4) where a purpose of the legal requirement for a signature is to provide assurance as to the completeness and integrity of the information and any alteration made to that information after the time of signing is detectable.

The provision of paragraph one does not limit that there is no other way to prove the reliability of an electronic signature or the adducing of the evidence of the non-reliability of an electronic signature.

Section 27. Where signature creation data can be used to create a signature that has legal effect, each signatory shall:

(1) exercise reasonable care to avoid unauthorized use of its signature creation data;

(2) without undue delay, notify any person that may reasonably be expected by the signatory to rely on or to provide services in support of the electronic signature if:

(a) the signatory knows or should have known that the signature creation data have been lost, damaged, compromised, unduly disclosed or known in the manner inconsistent with their purpose;

(b) the signatory knows from the circumstances occurred that there is a substantial risk that the signature creation data may have been lost, damaged, compromised, unduly disclosed or known in the manner in consistent with their purpose;

(3) where a certificate is issued to support the electronic signature, exercise reasonable care to ensure the accuracy and completeness of all material representations made by the signatory which are relevant to the certificate throughout its life-cycle, or as specified in the certificate.

Section 28. Where a certification service is provided to support an electronic signature that may be used for legal effect as a signature, that certification service provider shall perform as follows:

(1) act in accordance with representations made by it with respect to its policies and practices;

(2) exercise reasonable care to ensure the accuracy and completeness of all material representations made by it that are relevant to the certificate throughout its life-cycle, or as specified in the certificate;

(3) provide reasonably accessible means which enable a relying party to ascertain in all material representations from the certificate in the following matters:

(a) the identity of the certification service provider;

(b) that the signatory that is identified in the certificate had control of the signature creation data at the time when the certificate was issued;

(c) that signature creation data were valid at or before the time when the certificate was issued;

(4) provide reasonably accessible means which enable a relying party to ascertain from the certificate or otherwise as follows:

(a) the method used to identity the signatory;

(b) any limitation on the purpose or value for which the signature creation data or the certificate may be used;

(c) that the signature creation data are valid and have not been lost, damaged, compromised, unduly disclosed or known in a manner inconsistent with their purpose;

(d) any limitation on the scope or extent of liability stipulated by the certification service provider;

(e) the availability of the means for the signatory to give notice upon the occurance of the events pursuant to Section 27 (2); and

(f) a timely revocation service is offered;

(5) where services under subparagraph (4) (e) are offered, provide a means for a signatory to give notice pursuant to Section 27 (2) and. where services under (4) (f) are offered, ensure the availability of a timely revocation service;

(6) utilize trustworthy systems, procedures and human resources in performing its services.

Section 29. In determining whether any systems, procedures and human resources under Section 28 (6) are trustworthy, regard shall be had to the following, factors:

(1) financial and human resources, including existence of assets;

(2) quality of hardware and software systems;

(3) procedures for processing of certificates and applications for certificates and retention of records in connection with the provision of such services;

(4) availability of information on the signatories identified in certificates and on the potential relying parties;

(5) regularity and extent of audit by an independent body;

(6) the certification issuing organizations or certification service provider with respect to the practice or existence of the factors specified in subparagraphs (1) to (5);

(7) any other factor prescribed by the Commission.

CHAPTER 3
SERVICE BUSINESS RELATING TO ELECTRONIC TRANSACTIONS

Section 32. Persons shall have the right to operate service business relating to electronic transaction. In the event where it is necessary to maintain financial and commercial stability, or for benefit of strengthening the credibility and acceptance of electronic transactions system, or to prevent damage to the public. a Royal Decree prescribing the service business relating to electronic transaction which shall be subject to prior notification, registration or licence shall be issued.

Appendix D

The regulations of Royal Decree about the control in electronic payment service business

Royal Decree

About the control in electronic payment service business B.E.2551

Definition

Section 3. Electronic Payments means the transfer of right of money possession or the right of withdrawal or the right to debit one's account opened with the service provider by the totally or partly in electronic methods.

Chapter 1

The electronic payment service business enterprise

Section 7. The electronic payment service business which the service provider shall be subject to prior notification, registration or licencebe in line with the annex of this Royal Decree.

Section 13. For the benefit of the service of each service provider's control, the committee has separate the servicing conditions into annex A ,or B, or C.

Annex C

The Service business which subject to prior licence before servicing

(3) The electronic payment service through either apparatuses or networks

Appendix E

Regulations of The Proclamation of the electronic committee about the criteria, methods and conditions in the electronic payment service business enterprise B.E. 2552

The Proclamation of the electronic committee
about the criteria , methods and conditions for the electronic payment service business enterprise B.E. 2552

Chapter 2
Criteria , Method and Condition for the electronic payment service business enterprise

Clause 9. The service provider according to the annex A, B or C has to have the policy about the information security of the customer, the confidentiality of information and the authentication of the person who has authorization to access the information together with the trustworthiness of storage system and could be protect the unauthorized access and the integrity of information.

Appendix F

The Regulations of The Proclamation of the Bank of Thailand at SorRorKhor. 3/2552 about the policy and measure about the information security for service provider in the electronic payment business

The Proclamation of the Bank of Thailand

At SorRorKhor. 3/2552

About the policy and measure of the information security for service provider in the electronic payment business

Clause 4. Contents

4.1 The policy about information security

(2) The policy must cover at least the following titles:

(a) The access control and the authentication of user

4.2 The measure about information security

The service provider has to have the measure about the information security which relating to the electronic payment service and conform to the policy above. Moreover, the measure has to cover about the access control and the authentication of the user, the confidentiality of information, the trustworthiness and integrity of the system, the availability of the service, the solution and notification including the frequent information service examination at least one time per year.

The Guideline of information security related to the electronic payment service

The substantial of this guideline is consisted of:

1. The access control and authentication

1.3 The authentication and non-repudiation

The service provider has to have the identification examination or authentication and authorization for the user by using the proper technology which considered to the risk of the type of business such as Password, Personal Identification Number, Token or Smart Card, Biometric, or Public Key Infrastructure to prevent the non-repudiation.

Guideline

(1) Both the user and the related officer have to have the methods of identification or examination or authentication before using the information system for understanding that the access is come from the authorized person and to prevent the non-repudiation.

(2) To have a record of information access as an evidence.

Appendix G

The Regulations of The Royal Decree about Secured Procedure in Electronic Transaction B.E. 2553

Royal Decree

About Secured Procedure in Electronic Transaction

B.E. 2553

Definitions

Section 3.

Secured procedure means the secured procedure in electronic transaction

Section 4. The secured procedure has three levels

(1) Strict level

(2) Average level

(3) Basic level

The Proclamation of Electronic Transaction Committee

About kinds of electronic transaction and rules for evaluation the effect of electronic transaction considered by the secured procedure

B.E. 2555

Clause 2. The following kinds of electronic transaction have to use the strict secured procedure

(1) The electronic payment issued by the Royal Decree about the control in electronic payment service business B.E. 2551

Annex of the Proclamation of Electronic Transaction Committee about the standard of information security considered by the secured procedure B.E. 2555

3. The standard of information security considered by the strict secured procedure

Clause 6.

6.2 To have the at least requirements for authenticity and integrity of information in application and to indicate and follow the proper secured procedure.

6.3 To have the policy about the technical use related to the encryption

Appendix H The Regulations of Revised Payment Directive or PSD2

DIRECTIVE (EU) 2015/2366 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 25 November 2015

on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC

(Text with EEA relevance)

Article 4

Definitions

For the purposes of this Directive, the following definitions apply:

(5) 'payment transaction' means an act, initiated by the payer or on his behalf or by the payee, of placing, transferring or withdrawing funds, irrespective of any underlying obligations between the payer and the payee;

(6) 'remote payment transaction' means a payment transaction initiated via internet or through a device that can be used for distance communication;(7) 'payment system' means a funds transfer system with formal and standardised arrangements and common rules for the processing, clearing and/or settlement of payment transactions(8) 'payer' means a natural or legal person who holds a payment account and allows a payment order from that payment account, or, where there is no payment account, a natural or legal person who gives a payment order;(9) 'payee' means a natural or legal person who is the intended recipient of funds which have been the subject of a payment transaction;(10) 'payment service user' means a natural or legal person making use of a payment service in the capacity of payer, payee, or both;(11) `payment service provider' means a body referred to in Article 1(1) or a natural or legal person benefiting from an exemption pursuant to Article 32 or 33;(12) 'payment account' means an account held in the name of one or more payment service users which is used for the execution of payment transactions;

(29) 'authentication' means a procedure which allows the payment service provider to verify the identity of a payment service user or the validity of the use of a specific payment instrument, including the use of the user's personalised security credentials;(30) 'strong customer authentication' means an authentication based on the use of two or more elements categorised as knowledge (something only the user knows), possession (something only the user possesses) and inherence (something the

user is) that are independent, in that the breach of one does not compromise the reliability of the others, and is designed in such a way as to protect the confidentiality of the authentication *data;Article 97*

Authentication

1. Member States shall ensure that a payment service provider applies strong customer authentication where the payer:

(a) accesses its payment account online;

(b) initiates an electronic payment transaction;(c) carries out any action through a remote channel which may imply a risk of payment fraud or other abuses.

2. With regard to the initiation of electronic payment transactions as referred to in point (b) of paragraph 1, Member States shall ensure that, for electronic remote payment transactions, payment service providers apply strong customer authentication that includes elements which dynamically link the transaction to a specific amount and a specific payee.

3. With regard to paragraph 1, Member States shall ensure that payment service providers have in place adequate security measures to protect the confidentiality and integrity of payment service users' personalised security credentials.

4. Paragraphs 2 and 3 shall also apply where payments are initiated through a payment initiation service provider. Paragraphs 1 and 3 shall also apply when the information is requested through an account information service provider.

5. Member States shall ensure that the account servicing payment service provider allows the payment initiation service provider and the account information service provider to rely on the authentication procedures provided by the account servicing payment service provider to the payment service user in accordance with paragraphs 1 and 3 and, where the payment initiation service provider is involved, in accordance with paragraphs 1, 2 and 3.

Article 98

Regulatory technical standards on authentication and communication

1. EBA shall, in close cooperation with the ECB and after consulting all relevant stakeholders, including those in the payment services market, reflecting all interests involved, develop draft regulatory technical standards addressed to payment service providers as set out in Article 1(1) of this Directive in accordance with Article 10 of Regulation (EU) No 1093/2010 specifying:

(a) the requirements of the strong customer authentication referred to in Article 97(1) and (2);

(b) the exemptions from the application of Article 97(1). (2) and (3), based on the criteria established in paragraph 3 of this Article;

(c) the requirements with which security measures have to comply, in accordance with Article 97(3) in order to protect the confidentiality and the integrity of the payment service users' personalised security credentials; and

(d) the requirements for common and secure open standards of communication for the purpose of identification, authentication, notification, and information, as well as for the implementation of security measures, between account servicing payment service providers, payment initiation service providers, account information service providers, payers, payees and other payment service providers.2. The draft regulatory technical standards referred to in paragraph 1 shall be developed by EBA in order to:

(a) ensure an appropriate level of security for payment service users and payment service providers, through the adoption of effective and risk-based requirements;

(b) ensure the safety of payment service users' funds and personal data; (c) secure and maintain fair competition among all payment service providers;(d) ensure technology and business-model neutrality; (e) allow for the development of user-friendly, accessible and innovative means of payment. 3.The exemptions referred to in point (b) of paragraph 1 shall be based on the following criteria:

(a) the level of risk involved in the service provided;

(b) the amount, the recurrence of the transaction, or both: (c) the payment channel used for the execution of the transaction.4. EBA shall submit the draft regulatory technical standards referred to in paragraph 1 to the Commission by 13

January 2017.Power is delegated to the Commission to adopt those regulatory technical standards in accordance with Articles 10 to 14 of Regulation (EU) No 1093/2010.

5. In accordance with Article 10 of Regulation (EU) No 1093/2010, EBA shall review and, if appropriate, update the regulatory technical standards on a regular basis in order, inter alia, to take account of innovation and technological developments.

Appendix H

The European Banking Authority's Guidelines on the security of internet payment

Title I — Scope and definitions

Scope

1. These guidelines establish a set of minimum requirements in the field of the security of internet payments. The guidelines build on the rules of Directive 2007/64/EC3 (Tayment Services Directive', PSD) concerning information requirements for payment services and obligations of payment services providers (PSPs) in relation to the provision of payment services. Furthermore, Article 10(4) of the Directive requires payment institutions to have in place robust governance arrangements and adequate internal control mechanisms.

Definitions

12. For the purpose of these guidelines, and in addition to the definitions provided in the PSD, the following definitions apply:

- Authentication means a procedure that allows the PSP to verify a customer's identity.

- Strong customer authentication is, for the purpose of these guidelines, a procedure based on the use of two or more of the following elements - categorised as knowledge, ownership and inherence:

i) something only the user knows, e.g. static password, code, personal identification number;

ii) something only the user possesses, e.g. token, smart card, mobile phone;

iii) something the user is, e.g. biometric characteristic, such as a fingerprint. In addition, the elements selected must be mutually independent, i.e. the breach of one does not compromise the other(s).

At least one of the elements should be non-reusable and non-replicable (except for inherence), and not capable of being surreptitiously stolen via the internet. The strong authentication procedure should be designed in such a way as to protect the confidentiality of the authentication data.

Strong customer authentication

7. The initiation of internet payments, as well as access to sensitive payment data, should be protected by strong customer authentication. PSPs should have a strong customer authentication procedure in line with the definition provided in these guidelines

7.1 [CT/e-mandate/e-money] PSPs should perform strong customer authentication for the customer's authorisation of internet payment transactions (including bundled CTs) and the issuance or amendment of electronic direct debit mandates. However, PSPs could consider adopting alternative customer authentication measures for: - outgoing payments to trusted beneficiaries included in previously established white lists for that customer; - transactions between two accounts of the same customer held at the same PSP; - transfers within the same PSP justified by a transaction risk analysis; - low-value payments, as referred to in the PSD.

Appendix I

The Regulations of The Electronic Financial Transaction Act 2013 and Enforcement Decree of The Electronic Financial Transaction Act 2014 of the Republic of Korea

This Act has a purpose to contribute ensuring the security and reliability of electronic financial transactions by clarifying their legal relations and to promoting financial conveniences for people and develop the national economy by creating a foundation for the sound development of electronic financial industry.

Definition

Article Reference

Article 2

10. Means of access means any of the following means or information which is used to issue a transaction request in electronic financial tansactions or to secure the authenticity and accuracy of users and the details of such transaction:

(a) An electronic card or other electronic information equivalent thereto;

(b) An electronic signature creating key

(c) A user number registered with a financial company or an electronic financial business operator;

(d) Biological information of users;

(e) A password required to use the means or information referred to in item (a) or (b)

12. Electronic funds transfer means any transfer of funds made by any of the following methods from an account opened with a financial company or electronic financial business operator (limited to any account linked to a financial company ; hereinafter the same shall apply) to another account through an electronic apparatus for the purpose of transferring funds between a payer and a payee:

(a) A payment request made by a payer to a financial company or electronic financial business operator;

(b) A collection request made by a payee (hereinafter referred to as the "collection transfer")to a financial company or electronic financial business operator

The effectiveness of electronic fund transfer

Article Reference

Article 13

1. For electronic funds transfer: When the information on the amount transferred on a transaction request is completely recorded on the ledger of the account of a financial company or electronic financial business operator with which the payee's account is opened.

Duty of Selection , Use and Management of measures on authentication (Means of Access)

Article Reference

Article 6

(1) A financial company or electronic financial business operator shall select, use and manage the means of access necessary for electronic financial transactions and confirm the identity and authority of a user, the details of a transaction request, etc.

(2) A financial company or an electronic financial business operator shall issue the means of access only if an application is made by the user after verifying the identity of such user:

Provide, that it may be also issued without the user's application nor the verification of the user's identity in any of the following cases:

1. In case of an electronic prepayment means
2. Where user consent is obtained for renewal, replacement. etc. of the means of access, as prescribe by Presidential Decree.

Related to Article 6 of Presidential Decree, it may renew or replace a means of access even without the user's application or verification of the user's identity:

1. Where the user's written consent is obtained with respect to the renewal or replacement of a means of access that has not been used within six months before the expected date of renewal or replacement;
2. Where the user is informed at least one month before the expected date of the purposed replacement of a means of access that has been used within six months of the expected date of renewal or replacement and no objection is raised by the user within 20 days therefrom.

(3) No one shall commit any of the following offences unless otherwise expressly provided for in other Acts with respect to the use and management of a mean of access: Provided, That the same shall not apply where an electronic prepayment means or electronic currencies shall be transferred or offered as security:

1. To acquire or transfer a means of access;
2. To borrow or lend a means of access with compensation;
3. To provide a means of access subject to a right of pledge;
4. To assist such acts prescribed in subparagraphs 1 through 3.

Article 7

(1) Any financial company or electronic financial business operator shall ensure that a user can confirm the transaction details through an electronic apparatus (including an electronic apparatus, if any, stipulated in advance between the financial company or electronic financial business operator and the user) used for electronic financial transactions.

The liability of Financial company or Financial business operator

Article Reference

Article 9

(1) When a user suffer any loss due to any of the following incidents , the relevant financial company or electronic financial business operator shall be liable for indemnifying him/her for the loss:

1. An incident caused by the forgery or alteration of mean of access;
2. An incident caused in the course of electronically transmitting or processing the conclusion of a contract or a transaction request;
3. An incident caused by the use of a means of access acquired by fraudulent or other illegal means by invading the electronic apparatus for electronic financial transaction or an information and communication network.

(2) Notwithstanding paragraph (1), a financial company or electronic financial business operator may require a user to fully or partially bear the liability for any loss in any of the following cases:

1. When, with respect to any incident caused by the intention or gross negligence of the user, a prior agreement is made with the user to the effect that all or part of the loss may be borne by the user;
2. Where a corperate user (excluding any small enterprise) suffers any loss although the financial company or electronic financial business operator fulfills the duty of due care reasonably required to prevent incidents, such as the establishment and strict observance of security procedures.

(3) The intention or gross negligence of the user referred to in paragraph (2)1 shall be limited to that stipulated in the term and conditions of electronic financial transactions within the limits set forth by Presidential Decree.

Scope of Intention or Gross Negligence under Article 9(3) according to Article 8 of Presidential Decree means any of the following cases:

1. Where the user has rented a means of access or delegated the use thereof to a third person, or has offered the means of access as an object of transfer or security;

2. Where a means of access is divulged or exposed or left neglected despite knowing or being able to easily access the information that a third person is able to make an electronic financial transaction by using the user's means of access without authorization;

3. Where an incident under Article 9(1) 3 of the Act occurs because the user refuses, without any good cause , to take additional security measures required for electronic financial transactions which are requested by a financial company or an electronic financial business entity to enhance security, in addition to the confirmation under Article 6(1) of the Act;

4. Where an incident under Article 9(1) 3 of the Act occurs because the user performs any of the following acts with regard to the medium, means or information used for additional security measures referred to in subparagraph 3:

(a) Divulging, exposing or leaving it neglected;

(b) Renting it or delegating the use thereof to a third person, or offering it as object of transfer or security.

(4) Every financial company or electronic financial business operator shall take measures necessary to discharge the liability provided for in paragraph (1), such as purchasing insurance, joining a mutual aid society or accumulating reserves, pursuant to the standards determined by the Financial Services Commission.

5.5 Bank of Thailand Press Release No. 22/2016: Migration of ATM and Debit Cards to Thai Standard Chip Cards, 4 May ,2016.

Bank of Thailand

Bank of Thailand Press Release No.22/2016

Migration of ATM and Debit Cards to Thai Standard Chip Cards

Mrs. Tongurai Limpiti, Deputy Governor (Financial Institutions Stability), Bank of Thailand, announced the migration of ATM and debit cards from magnetic stripe cards to chip cards complying with the Thai Bank Chip Card Standard. Starting from 16 May 2016 onwards, all newly issued ATM and debit cards will be chip-based.

Existing 60 million magnetic stripe cards currently in use will he migrated to chip cards by 31 December 2019.

In 2013, the Payment Systems Committee formulated a policy for financial institutions to migrate magnetic stripe ATM and debit cards to chip cards. This policy is a crucial measure to increase security for cardholders. solving counterfeit card frauds whereby magnetic stripe cards are skimmed to make unauthorized payments and cash withdrawals. This measure will enhance customers' confidence in using ATM and debit cards for financial transactions via ATMs as well as paying for goods and services via point-of-sale (POS) terminals instead of using cash. In addition, this policy aligns with many other countries including ASEAN members.

Cooperation from relevant stakeholders was a key success factor for this project, especially from the Thai Bankers Association (TBA). The TBA has established the Thai Bank Chip Card Standard for locally-issued ATM and debit cards to enable interoperability for bank customers. The banks have also worked together to improve their internal procedures and upgrade the ATMs and POS to accept chip cards.

The implementation of this chip card standard in Thailand is a crucial step in the development of payment services by encouraging greater use of e-payment. It is also in line with the National e-Payment Master Plan's aim of moving the country to a cashless society. This beneficial development of Thailand's payment system is another successful step in enhancing the efficiency and security of payment services in Thailand.

Bibliography

Documents

European Union Agency for Network and Information Security. elD Authentication methods in e-Finance and e-Payment Services.

Bank of Thailand Press Release 31/2016, 15 June 2016. A New I. and Transfer Service — "PromptPay".

Bank of Thailand News on PromptPay : New way of Transaction and Receiving Money Service

The Future Shape of Banking : Time for Reformation of Bankirw, and Bank, July 2014, by PWC Financial Service.

Chris Skinner , Essay on A visual vision of banking's future , on 1/05/2013, At http:// http://www.thebanker.com/Transactions-Technology/Comment/A-visual-vision-of-banking-s-future.

Rangsan.Nochai and Titida.Nochai, The Impact of Internet Banking Service on Customer Satisfaction in Thailand: A Case Study in Bangkok.

Authentication in an Internet Banking Environment, Federal Financial Institutions Examination Council.

Research, Theses

Dan Zhu Department of Logistic, Operation and MIS Iowa State University , Electronic Commerce Research Vol.3 No.l. 2002_ Security Control in Inter-Bank Fund Transfer.

SkundricNikola, MilutinovicVeljko, Kovacevic Milos. Klem Nikola, Chapter 5 E-Banking, E-Business on Internet.

BoonyaratSamphanwattanachai, Internet Banking Adoption in Thailand: A Delphi Study, Department of Marketing, School of Management, Assumption University.

TaiwoDayoAjkaiyet and Karl SenanuKudzo Krause, Online Based Authentication and Secure Payment, Master of Science Thesis in the Programme Secure and Dependable computer systems, Methods for M-Commerce Applications.

Seolhwa Han, Okkyung Choi, Kangseok Kim, HongjinYeh and Taesik Shon, A Design of Electronic Payment Authentication Method based on NFC Smartphone, Dept. of Knowledge Information Security, Graduate School of Ajou University, Suwon, Korea.

Guidelines, Law and Regulation

The Bank of Ireland Notification on Phone and Digital Banking I erms and Conditions

The Bank of Thailand Notification SRK 3/2552: Policy and Measures on Information Security in Business Electronic Payment Service

The Commerce and Civil Code of Thailand B.E. 2468

The Computer — Related Crime Act B.E. 2550

The Decree of The Electronic Financial Transaction Act 2014

The Electronic Transaction Act B.E. 2544

The European Banking Authority's Guidelines on the security of internet payment The Revised Payment Services Directive

The Republic of Korea's Electronic Financial Transaction Act 2013 and Enforcement

The Republic of Singapore's Electronic Transaction Act 2010

Internet

Online Banking, At http://en.wikipedia.org/wiki/Online banking. (last visited 30 August 2016).

Thai Electronic Bank, At http://th.wikipedia.org/wikihirm al'Annoiln4, (last visited 15 May 2016).

How does online banking work, At http://www.stockmonkevs.conilhow-does-online-banking-work-NWLTEHID/. (last visited 19 October 2016).

How do ATM machines work internally, At http://www.quora.com/How-do-ATM-machines-work-internallyl. (last visited 19 October 2016).

How Payment Processing Works, at http://www.cybersource.com/developers/getting_started/how payment processing works/. (last visited 19 October 2016).

Understanding credit card, At http://www.westpac.com au/personal -banking/credit-cards/understanding-credit-cards!. (last visited 19 October 2016).

Online Banking ePayment, At http://en.wikipedia.org/wiki/Online Ranking ePayments.

Mobile Banking, At http://www.investinganswers.com/financial-dictionary/personal-financial/mobile-banking-2595. (last visited 30 August 2016).

Cash on the move, At http://www.businesstoday.in/moneytociav/smart-spending/mobile-banking-technology-transfer-money-cash-sarely/story/24247.html. (last visited 19 October 2016).