TOWARDS COMMUNITY FRAMEWORK ON ELECTRONIC SIGNATURES AND INDONESIA LEGAL FRAMEWORK

(Final Version)

A Thesis of Master Program in Law and Technology

Universiteit van Tilburg

By

Della Utami Rahmany

515713

Thesis supervisor:

Prof. J.E.J.Corien Prins

TILBURG

JANUARY 2011

Table Of Contents

List of Abbreviations

CA	: CA
CFES	: Community Framework on E-signatures
CSP	: CSP
DNA	: Deoxyribonucleic Acid
EU	: European Union
ICT	: Information and Communication Technology
IT	: Information Technology
PIN	: Personal Identification Number
PKI	: Public Key Infrastructure

CHAPTER 1

INTRODUCTION

1.1 Background Study

The rapid development in Information Technology has brought us to a new level of trade. Nowadays, people conduct their trade through the internet from any part of the world. A significant amount of business is conducted through e-mails and the 'click through' websites usually do not require any signature in the conventional sense of the word before a transaction can be completed.[1] Without electronic signatures (hereinafter referred to as "e-signatures), companies are hardpressed to engage in electronic commerce. Bussinesses require assurance that an electronically signed document can be enforced against the sender.[2] Businesses are uncomfortable working in an environment where they cannot be sure of the identity of the other party and that an agreement they make can be enforced.[3] The legislation gives legal recognition to e-signatures and online contracts. The use of e-signatures shall make it much easier for businesses and consumers to transact business over the Internet and benefit from the efficiencies resulting from advances in technology. [4] It shall bolster e-commerce by eliminating companies' fears about the enforceability of online transactions.[5] Because the digital signature is generated as a function of the key and a unique message, the signature serves two purposes, it authenticates the signer, since only the individual owner has (in theory, anyway) access to the private key and it also indicates the reliability and integrity of the message, since any alteration to the text would invalidate the

[1] Ter Kah Leng, Have You Signed Your Electronic Contract, 2011, available at available at www.sciencedirect.com
[2] Jim Carroll, Electronic Commerce and The Paperless Economy, available at http://www.cyberlaw.com/images/getting_to_digital_signatures.pdf
[3] Jonathan Rosenoer, Getting to Digital Signatures and Electronic Commerce, June 1998, available at http://www.cyberlaw.com/images/getting_to_digital_signatures.pdf
[4] E-Sign Legislation - The milestone in the e-signature history, available at http://www.elock.com/resources-e-sign.html
[5] Ibid

signature.[6] Therefore the existence and the validity of e-signature shall give confidence for online transaction.

The Internet, in its current state, is considered by some organisation as a wild lawless frontier to which is problematic given they are afraid of liability risks. It, however, has proved to be a successful breeding ground for start-up companies willing to face these risks in search of big rewards.[7] Governments all over the world have recognised that their economies need to be ready for the internet technologies being adopted in their industries.[8] To remain competitive and to survive the dramatic changes, efforts to quickly remove the barriers to electronic commerce have been made.[9] The new legislation had been enacted to provide for an effective legal infrastructure for electronic commerce.[10] In Europe, the European Commission passed an e-signature Directive that also adopts a framework for e-signatures for their member countries.[11] In the past only hand-written signatures were legally valid. The Directive 1999/93/EC on a Community framework for e-signatures extends that recognition to e-signatures, a reliable system of e-signatures that work across EU countries is vital for safe electronic commerce and efficient electronic delivery of public services to businesses and citizens.[12] The first European country to adopt such a law has been Germany, in

[6] State Archives Department, Minnesota Historical Society , March 2004, Version 4 , Page 5, Available at http://www.mnhs.org/preserve/records/electronicrecords/docs_pdfs/ersigs.pdf

[7] Martin Wilcock BEng, MSc(Eng), MSc, DIC, AMIChemE, Open Governance: The Case for Unregulated E-Commerce, available at http://www.arraydev.com/commerce/jibc/0001-05.htm

[8] Harry SK Tan, Electronics Transaction Regulations-Singapore, Computer law and Security Report, Volume 18 Issue 4, 31 July 2002, page 272-277Issue 4, 31 July 2002, page 272-277See *Directive 1999/93/EC of 13 December 1999 on community framework for e-signatures*, available at: http://www.sciencedirect.com/science?_ob=RedirectURL&_method=externObjLink&_locator=url&_issn=02673649&_origin=article&_zone=art_page&_plusSign=%2B&_targetURL=http%253A%252F%252Feuropa.eu.int%252Fcomm%252Finternal_market%252Fen%252Fmedia%252Fsign%252Findex.htm.v

[9] Ibid

[10] Ibid

[11] Ibid

[12] Europe's Information Society, Thematic Portal, esignature, available at http://ec.europa.eu/information_society/policy/esignature/index_en.htm

1999 the European Parliament and the Council has adopted directive 1999/93/EC on a Community framework for e-signatures.[13]

Recently, in Indonesia, electronic and information technology has become an expensive issue to be developed. In general the development of ICT in Indonesia nowadays is less encouraging compared to the developed countries, or even compared to neighboring countries such as Singapore, Malaysia, Thailand and others.[14] The biggest obstacle faced by Indonesia regarding ICT is the economic crisis, the government has to postpone various programs that had been planned including the program to support ICT development.[15] Considering the country's condition, it is not easy for the government to give special attention on the development of electronic information.

Indonesian commercial legal system is basically influenced by Continental European civil law traditions that are the Dutch civil law for Indonesian Civil Codes (= Kitab Undang-undang Hukum Perdata) and customary (adat) law.[16] Both legal systems have been used long before the independence of the Republic of Indonesia.[17] However, legal aspects concerning contract made through electronic can be interpreted from the Indonesian Civil Code.[18] Nevertheless a specific regulation regarding e-signature has still not been set by the government. The legal effects on contracts made through the Internet, which include the effects of e-signatures and documents formulated through e-commerce, the acceptability of evidence in court, as well as issues relating to the legal protection of legal data stored in electronic systems, owned by government and private

[13] Andrzej M. Borzyszkowski, E-signature, the theory and the practice, Poland and Europe, Institute of Computer Science, Gda´nsk Branch, Polish Acad. of Sci.Abrahama 18, 81-825 Sopot, Poland http://www.ipipan.gda.pl/, available at http://www.google.nl/url?sa=t&rct=j&q=background%20of%20electronic%20signature%20in%20europe&source=web&cd=9&ved=0CG0QFjAI&url=http%3A%2F%2Fciteseerx.ist.psu.edu%2Fviewdoc%2Fdownload%3Fdoi%3D10.1.1.62.4975%26rep%3Drep1%26type%3Dpdf&ei=5yL5TpeZLsma-wa2nYTMAQ&usg=AFQjCNGO52bNJ6IO-Js2BbTGuIcmWz8nLw&cad=rja

[14] Harina Yuhetty, ICT and Education in Indonesia, available at http://gauge.u-gakugei.ac.jp/apeid/apeid02/papers/Indonesia.htm

[15] Ibid

[16] Sunu Purbanti A. Rini, Indonesian APEC Study Center, COUNTRY REPORT LEGAL FRAMEWORKS AND E-COMMERCE TRAINING PROGRAM (INDONESIA), page 7, available at http://www.apec.org.au/docs/rini.pdf

[17] Ibid.

[18] Ibid.

bodies/companies, have caught the attention of the users of Internet, internet providers, telecommunication society, legal scholars and government of Indonesia.[19]

Law Number 11 of 2008 on Information and Electronic Transaction which was enacted on April 21 2008, regulates all matters pertaining to information and transactions in all electronic forms, it is the first law that regulates cyber activity in Indonesia, it provides a general outline, and requires further elaboration through government regulations.[20] Law Number 11, Year 2008, on Information and Electronic Transactions, has technology neutral approach such as freedom of choice or technology. This includes choosing the type of e-signature used to sign electronic information and/or electronic documents.[21], on the basis of Law Number 11, Year 2008, and Design Regulation, the E-signature is a signature consisting of electronic information that it's attached to, associated with or related to other electronic information that is used as a means of verification and authentication.[22] The question that arises is, whether the signature in handwritten, converted into electronic data has any legal force and effect of law.

According to internet expert, Onno W. Purbo, electronic transactions depend on the concept of e-signature and certificate authority.[23] Around 99% of electronic transactions in Indonesia, especially the ones conducted through the internet, do not use e-signatures, let alone the use a certificate authority.[24] Do the laws established by government of Indonesia have fulifilled the needs of their citizen for legal certainty in making online transactions which binds through e-signature? Facing those conditions a legislation specifically regulating e-signatures and CA or CSP and its liability should be enacted as soon as possible.

---

[19] Prof Mieke Komar Kantaatmadja, Electronic Commerce and Electronic Legal Issues in Indonesia, page 2, available at http://www.aseanlawassociation.org/docs/w5_indo2.pdf

[20] Harun Reksodiputro, The Law and Electronic Transactions and information – a general outlin, July 2008, available at http://www.asialaw.com/Article/2004303/Channel/17441/The-law-on-electronic-transactions-and-information-a-general-outline.html

[21] See Law Number 11 Year 2008 on Information and Electronic Transactions

[22] See *id.*

[23] See www.detikinet.com/read/2008/03/31/130700/915866/399/pasal-transaksi-elektronik-bakal-persulit-perbankan.

[24] Ibid

1.2 Research Questions

The conditions described above lead to the following legal questions:

How can the approach of Directive 1999/93EC of the European Parliament and of the Council of December 13, 1999, on a Community Framework for E-signatures (CFES) provide guidelines for the regulation of electronic signature in Indonesia?

To guide this study, the author divides the research question above into following sub-questions:

1. How do the CFES regulate e-signature?
2. What are in legal literature seen as the positive and negative sides of the CFES?
3. To what extent should the Indonesian Law follow the CFES in order to establish regulation on e-signatures and what does it mean in the necessity to amend the current proposed provisions in Indonesia?

1.3 Aim and Trigger

The goal behind this thesis is to provide an analysis of the law on e-signatures within different legal systems. The intention is to provide the Ministry of Information and Communication Technology of the Republic of Indonesia, where the author works and which plays a role of the regulator in the field of Information and Communication Technology due to the fact that Indonesian laws have not yet set forth a specific rule regarding e-signatures in the field of electronic commerce, an elaboration of the issues that will benefit the Ministry of Information and Communication Technology of the Republic of Indonesia.

1.4 Methodology

To answer the research question described above, a literature review approach will be adopted to, by reviewing the regulatory framework in the EU, several Asian countries and Indonesia. Each of these places have different legal systems and distinct regulations for e-signatures. The EU has issued Directive 1999/93/EC of the European Parliament and of the Council of December 13,

1999, on a Community Framework for E-signatures. The Design of Government Regulations Republic of Indonesia on the Organization of Information and Electronic Transactions. Law Number 11, Year 2008, on Information and Electronic Transactions, Official Journal of the European Union, and Indonesian regulations and their explanatory notes. Secondary sources include scholarly (journal) and case law literature.

1.5 Structure

For the structure, this study will firstly give an overview on e-signatures, a regulatory framework of CFES, which parties are involved and what are the advantages and the shortcomings of CFES. Chapter 3 of the study will analyse legal frameworks and legislative approaches in several countries in Asia and whether they are adequate or not to be a model for Indonesian Law. After having an understanding on regulatory frameworks of e-signatures in the EU and several countries in Asia and as an elaboration to answer the research questions, the study will be confirmed by a comparative analysis among two regulatory frameworks of Indonesia and EU in Chapter 4, and it will end with concluding remarks and recommendations in Chapter 5.

CHAPTER 2

AN OVERVIEW OF E-SIGNATURES AS REGULATED IN DIRECTIVE 1999/93/EC

The author aims in this chapter to provide a clear foundation for the underlying issue on the topic. First it will give a brief overview of the basic notion of e-signatures as set out in Directive 1999/93 (hereinafter referred to as "the Directive"), which parties are involved and their role in this topic. This will be followed by an explanation about the aim of the Directive itself. Thus, since privacy and data protection also take part in this topic, there will be a brief overview of this followed by some analysis regarding the strengths and shortcomings of the Directive.

2.1 E-signatures: An Overview

In accordance with Art 2(1) of the Directive, an e-signature is defined as "data in electronic form which are attached to or logically associated with other electronic data and which serves as a method of authentication".[25] This definition has a technology-neutral approach, which leaves room for wider interpretation. By this definition, the Directive is trying to embrace possibilities of legal differences between EU member states regarding recognition of e-signatures.

The purpose of the Directive is to facilitate the use of e-signatures in the EU countries and contribute to their legal recognition.[26]Additionally, a main objective of the Directive is to create a community framework for the use of e-signatures, allowing the free flow of e-signature products and services cross border, and ensuring a basic legal recognition of e-signatures.[27] Thus the Directive aims to harmonize the regulatory framework within member states and to avoid divergence of regulation or conflict with respect to e-signatures.

[25] See Ralf Cimander, Meik Hansen, Prof. Dr. Herbert Kubicek, E-signatures as Obstacle for Cross-Border E-Procurement in Europe, Lessons from the PROCURE-project, Institut für Informations management Bremen GmbH (IFIB) Am Fallturm 1 28359, Bremen, June, 2009, p.9.

[26]Internet Law – The EU Law on E-signatures and its Recent Report, Martha L. Arias, IBLS Director, December 2007, http://www.ibls.com/internet_law_news_portal_view.aspx?id=1920&s=latestnews

[27]See report on the operation of Directive 1999/93/EC on a Community framework for e-signatures.

Human identification is a practical matter; in a variety of contexts, each of us needs to identify other individuals in order to conduct a conversation or transact business. Organizations also seek to identify the individuals with whom they deal, both to provide better service to them and to protect their own interests.[28]

In the context of information systems, the purpose of authentication is more concrete: it is used to link a stream of data with a person, and thus the purposes of the interchange of identification include developing mutual confidence, reducing the scope for dishonesty and enabling a person or a system to associate transactions and information with an identity.[29]

The purpose of E-signatures is to serve as a method of authentication.[30] There are three types of approaches toward electronic authentication:[31]

1) The digital signature approach is characterised by its focus on the digital signature techniques. Legislation based on this approach is a technology-specific legislation by definition.

2) The two-prong approach is named as such because of its hybrid way of dealing with electronic authentication. With this approach, legislation sets requirements for electronic authentication methods, which will receive a certain minimum legal status (minimum prong) and assigns greater legal effect to certain electronic authentication techniques (maximum prong).

3) The minimalist approach does not address specific techniques and therefore intends to be technology neutral.

The Directive illustrates the example of the two-prong approach; it takes this approach in order to differentiate between possible levels of reliability and provides special legal consequences with

[28] More about human identity etc. cf.; "Towards Understanding Identity – An examination of the fundamentals underlying the definitions and understanding of identity based on the assumption and experience known form the real-world in order to map them on to the requirements emerging form the digital world", produced by an EEMA Identity Technologies and Services Working Group, authors Bowden, Bramhall, Cameron, Cassassa-Mont, Colvill, Goodman, Hilton, Marhøfer, White, daft v0.35, 24 March 2004.

[29] Thomas Myhr, Regulating a European EiD a Preliminary Study on a Regulatory Framework for Entity Authentication and a pan European Electronic ID for the Porvoo e-ID Group, January 2005, p. 7, available at http://skilriki.is/media/skjol/Regulating_a_European_eID.pdf.

[30] Article 2(1) of the Directive.

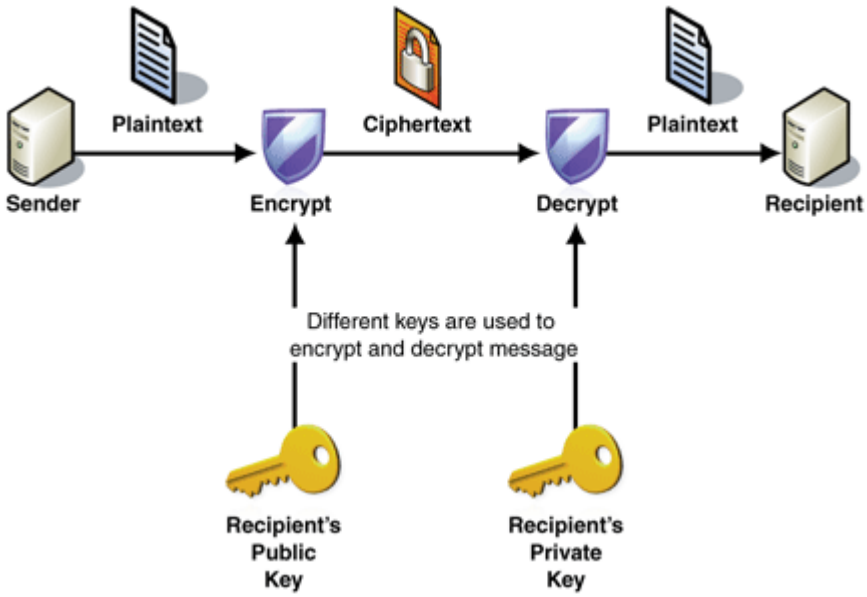
[31] Aalberts, B.P.& Van der Hof, S., Digital Signature Blindness: Analysis of Legislative Approaches to Electronic Authentication (2000). The EDI Law Review Vol. 7 No. 11.p.26.

respect to evidential issues to advanced e-signatures.[32] More about advanced e-signatures will be discussed in this chapter.

The digital signature working principle is as follows: a person creates some text, the text is encrypted by a private key using a mathematical relationship, the person sends the encrypted text, the reader who receives the text uses the person's publicly available key (connected to the private key) to open it, and they are then sure the text is original and it is written by the sender. A key does not need to be attached to any device, but often is stored on one to make it easier to use. Thus, a private key used as a digital signature generally resides on a smartcard in a smart-card reader that is installed in the signatory's personal computer.[33] This public and private key method is also known as the method used in Public Key Infrastructure (hereinafter referred to as "PKI").[34]

A PKI is a group of servers that handles the creation of public keys for digital certificates. PKI systems maintain digital certificates, creating and deleting them as needed.[35] The system allows users to swap information securely across a public network through a pair of public and private cryptographic keys, which are obtained and accessed through a certificate service provider.[36] But how does PKI really work? The mechanism of PKI can be described as shown below:[37]

[32]Ibid.
[33]Mazzeo, Mirella, Digital Signatures and European Laws, November 2010, http://www.symantec.com/connect/articles/digital-signatures-and-european-laws
[34]A PKI enables users of a basically unsecure public network such as the Internet to securely and privately exchange data and money through the use of a public and a private cryptographic key pair that is obtained and shared through a trusted authority.
[35]http://searchsecurity.techtarget.com/tip/PKI-and-digital-certificates-Security-authentication-and-implementation
[36]Ibid.
[37]Source of the picture: http://alwajbaiss.com/?p=469



The public key infrastructure assumes the use of *public key cryptography*, which is the most common method on the Internet for authenticating a message's sender or encrypting a message.[38] In public key cryptography, a public and private key are created simultaneously using the same algorithm (a popular one is known as RSA) by a certificate authority (CA) or what is known as Certificate-Service Providers (CSPs) in the Directive. The private key is given only to the requesting party and the public key is made publicly available (as part of a digital certificate) in a directory that all parties can access.[39] This type of encryption is currently the preferred approach on the internet.

2.1.1 E-signatures

The Directive works with a broad interpretation of "e-signature". It can be as simple as signing an e-mail message with a person's name or using a PIN code.[40] To be a signature, the authentication must relate to the data and not be used as a method or technology only for entity authentication.[41] In this definition, biometric authentication methods are regarded as e-signatures, as are message

[38]See Jim Brayton, Andrea Finneman, Nathan Turajski, and Scott Wiltsey, Definition PKI (Public Key Infrastructure), October 2006, available at http://searchsecurity.techtarget.com/definition/PKI
[39]Ibid.
[40]Supra note 26, page 4.
[41]Supra note 26, page 4.

authentication codes (MAC), which are based on symmetric cryptography. Public key authentication schemes, such as digital signatures, are also e-signatures.[42] Biometrics enable the automated recognition of individuals based on their unique biological and/or behavioural characteristics, such as the eye iris and the fingerprint, and thus can be considered a form of e-signature according to this definition.[43] The definition of an e-signature in the Directive does not exclude the typed name at the bottom of an email or the attachment of a scanned signature to a document.[44] Therefore, even the simple form of stating the sender's name at the bottom of an email could be considered an e-signature and could have equal legal effect as a handwritten signature.

2.1.2 Advanced E-signature

In accordance with Art 2 (2) of the Directive, "advanced e-signature" means an e-signature that meets the following requirements: [45]

(a) it is uniquely linked to the signatory;

(b) it is capable of identifying the signatory;

(c) it is created using means that the signatory can maintain under his sole control; and

(d) it is linked to the data to which it relates in such a manner that any subsequent change of the data is detectable.

Although the Directive has a technology-neutral approach, this definition refers mainly to e-signatures based on public key infrastructure (PKI).[46]PKI uses encryption technology to sign data, which requires a public and a private key.[47] In order to create an e-signature, authentication data and data to be signed or a hash of data to be signed is sent from the signatory to the provider via a

[42]Van Eecke, in Bullesbach/Poullet/Prins, Concise IT, Directive 1999/93/EC of The European Parliament and of The Council of 13 December 1999 on a Community Framework for E-signatures, p. 444.
[43]Meints and Gasson, "High-Tech ID and emerging technologies", 138
[44] Supra note 36, page 444.
[45]See Article 2(2) of the Directive.
[46]Supra note 26.
[47]Supra note 26.

secure communication channel.[48] After verification of the authentication data, the signature is created by the hardware security module, and signed data are returned to the signatory for further processing. The Directive's Article 5 states that advanced e-signatures shall be admissible evidence in legal proceedings among the EU member states, provided that some requirements are met.[49]First, the advanced e-signature should be based on a "qualified certificate"; it should be created by a "secure-signature creation device"; and it should satisfy the same legal requirements as if it were related to paper-based data.[50]This type of e-signatures also has some drawbacks, which will be discussed further in the next chapter.

An advanced e-signature has more significant value than an e-signature: it guarantees the integrity of the text, as well as the authentication.[51] The juridical value it has is for integrity: one is sure that the text received is the same that was sent, and that no hacker has changed it. The judge must consider the text unexpurgated and nobody can deny its integrity.[52]

This type of e-signature is meant to provide more security and legal certainty for businesses. Like other types of e-signatures, this type also has shortcomings. Total security of an electronic transaction using PKI is difficult, if not impossible, to achieve.[53] Although PKI is designed to make electronic transactions secure, there are still instances when the architecture can break down and a security breach can occur. Most of these instances occur because of human error or carelessness.[54] There is always a manner to hack technology, no matter how sophisticated it becomes. Another shortcoming of PKI systems is that they are complicated and expensive, require considerable

[48]See, Forum of European Supervisory Authorities for E-signatures (FESA), Public Statement on Server Based Signature Services, October 2005, it explains that The basic idea is that the signature creation data are not stored in a signature creation device located at the signatory, but in a central hardware security module located at the signature service provider. Definition of "Signatory" in accordance to Art. 2 (3) is means a person who holds a signature-creation deviceand acts either on his own behalf or on behalf of the natural or legal person or entity he represents.
[49]Supra note 25.
[50]Supra note 25.
[51]Supra note 29.
[52]Supra note 29.
[53]Philip Hlavaty, The Risks Involved With Open and Closed Public Key Infrastructure, February 2003, available at http://www.sans.org/reading_room/whitepapers/vpns/risks-involved-open-closed-public-key-infrastructure_882
[54]Ibid.

planning and can be difficult to maintain, install and deploy.[55] The implementation could be an extensive effort, requiring professional human resources to build and to maintain such infrastructure. An extensive source of funding should also be taken into account in order to provide a safeguard of the business of PKI itself; in a self-regulatory world, PKI that is provided by a reputable company would have a better chance to satisfy the needs of the consumer.

Article 5.1 states in its first paragraph that "Member States shall ensure that advanced e-signatures which are based on a qualified certificate and which are created by a secure signature-creation device "satisfy the legal requirements of a signature in relation to data in electronic form in the same manner as a hand-written signature satisfies those requirements in relation to paper-based data".[56]

There are three criteria required of e-signatures in order to be categorized as Qualified E-signatures, according to Annex I, II and III of the Directive. These signatures must be:[57]

1. advanced e-signatures;
2. based on a qualified certificate; and
3. created by a secure signature creation device.

Article 5 thus provides two levels of legal certainty for e-signatures depending on the level of technical security related to that e-signature.[58] On the first level, e-signatures in general cannot be denied legal effect. On the second level, e-signatures fulfilling some minimal technical security requirements will have the same legal effect as hand-written signatures.[59]

[55]Supra note 31.
[56]Jos Dumortier, Legal Status of Qualified E-signatures in Europe, available at https://www.law.kuleuven.be/icri/publications/611ISSE_2004_Dumortier_Text.pdf
[57]See Final Report of the EESSI Final Team, European E-signature Standardization Initiative, July 1999, available at http://cryptome.org/eessi.htm
[58]Ibid.
[59]Ibid.

To avoid misunderstandings of legal certainty among advanced e-signatures and qualified e-signatures, using such a signature implies the automatic application of existing legal rules, which still refer to the handwritten signature.[60]

Basically, qualified e-signatures could also be defined as an e-signature based on certificates issued by certification authorities, which certify public keys for a person registered by a registration authority, and can be created with a so-called secure signature creation device.[61]

2.1.3 Legal Effect of E-signature

"Legal effect" essentially means that the courts will accept that an "e-signature" is a "signature" as already defined by precedent and law.[62]In other words, an e-signature and a wet-ink signature are equivalent in most respects, and they can be brought into trial.[63] Article 5 of the Directive provides an overview in admissibility and assurance of the legal effect of e-signatures. E-signatures that do not satisfy any technical security requirements cannot be denied legal effect.[64] Moreover, e-signatures fulfilling some minimal technical security requirements will have the same legal effect as handwritten signatures.[65]Additionally, Recital (21) of the Directive specifies that "in order to contribute to the general acceptance of electronic authentication methods it has to be ensured that e-signatures can be used as evidence in legal proceedings in all Member States".[66]

Therefore the Directive approves the legal effectiveness and admissibility of e-signatures. This means that the Directive 'only' provides non-discrimination between electronic and hand-written signatures.[67] It remains at the discretion of the member states whether provisions for

[60]Supra note 51.
[61]Royer & Rosnagel, Profitability of Mobile Qualified E-signatures, page 1345, available at http://www.is-frankfurt.de/publikationenNeu/ProfitabilityofMobileQualified1320.pdf
[62]John B Harris, "This is legal, right?" – E-signatures & The Law, May 2008, available at http://blogs.adobe.com/security/2008/05/this_is_legal_right.html
[63]Ibid.
[64]Supra note 38.
[65]Supra note 38.
[66]Supra note 52.
[67]For a more restrictive opinion, see U Blaurock and J Adam, 'Elektronische Signtatur und europäisches Privatrecht' (2001) *Zeitschrift für Europäisches Privatrecht* 93 at pp 98 and 110.

technology-neutral formalities are necessary at all. Furthermore, it is possible to exclude e-signatures because of non-discriminatory reasons, that is, because the specific function of a signature requires a special form (e.g., a will).[68]

In legal terms this means that the legislation provides the same "legal effect and validity" to an e-signature and record as to the legal effect granted a handwritten signature on a paper.[69] The greatest significance of the e-signature's regulatory framework is that it provides a stable legal platform for electronic merchants and buyers so that they can use digital media in commerce with confidence.[70] Thus e-signatures serve an important role in electronic transactions as the validation and recognition of agreements, and as such provide legal certainty in electronic commerce.

2.2 Identification

As explained in the previous section, identification is one of the ways to obtain an electronic authentication. Identification plays an important role in e-signatures; it allows the parties involved in the transaction to be sure that they are dealing with who the other party claims to be. In the context of electronic commerce, for example, to help control credit card fraud, it is necessary for the merchant or the seller to authenticate the owner of a credit card to verify the validity of the transaction. In this context, smart cards might be used for a means of authentication, a method that will be discussed later in this chapter. For transactions over the internet, a more stringent authentication is needed than a name written at the end of an email. In this section we will discuss several instruments of identification that are more reliable for internet transactions when properly carried out by a secure infrastructure, such as identification through biometrics, smart cards and public keys. Among the most notable and secure technologies used for authentication are a variety

[68] Mathias M. Siems, The EU Directive on E-signatures: A Worldwide Model or A Fruitless Attempt To Regulate The Future?, p. 14.

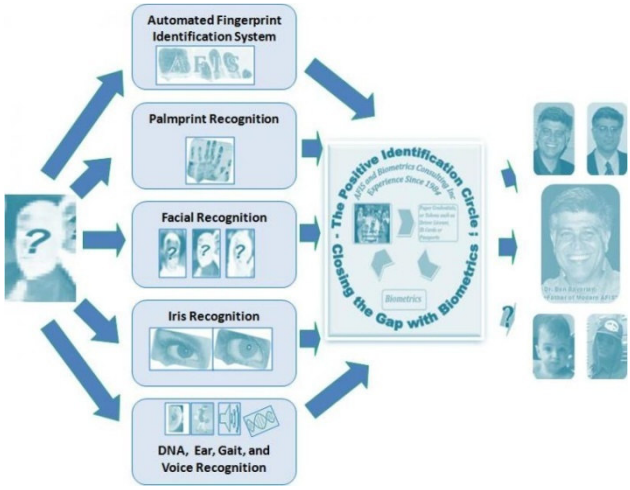
[69] Jacques R. Francoeur, B.A.Sc., M.A.Sc., MBA, E-signature Assurance & the Digital Chain-of-Evidence Executing Legally Admissible Digitally Signed Records, Proof Space White Paper, page 7, available at http://www.proofspace.com/UserFiles/File/esignature.pdf

[70] As explained in the Meeting Report of Ministry of Information and CommunicationRepublic of Korea, Electronic Transactions Act and Digital Signature Act, Background, Major Provisions and Implication, OECD Forum on Electronic Commerce, 12–13 October 1999, Paris.

of biometric and cryptographic "key-based" systems used as standalones, in combination, or as part of a larger technological solution.[71]

2.2.1 Biometrics

As one of the instruments for electronic authentication, biometrics provide a higher level of security than a traditional personal identification number (PIN).This provides the additional level of individual or personal authentication should a group of people have access to one key.[72] Biometrics enable the automated recognition of individuals based on their unique biological characteristics, such as the eye iris, DNA, the personal features of one's entire and the fingerprint. [73]The characteristic of biometrics can be shown by the following graphic:[74]



So what are biometrics, exactly? There are several definitions of biometrics. According to Robin Feldman, biometrics have been described as "the science of identifying people based on their physiological and behavioural characteristics".[75] On the other hand, Pawan and Siyal define a

[71]See Recommendation on Authentication in Electronic Commerce, May 1999, prepared by Alliance for Global Bussiness for is presented to the Joint OECD Private Sector Workshop on ElectronicAuthentication (Stanford and Menlo Park, 2-4 June 1999), as a minimum checklist ofbusiness requirements for government policies addressing authentication in electronic commerce, available at http://www.biac.org/statements/iccp/AGB_authentication_principlesI.pdf

[72]Bromby, Michael, Identification, trust and privacy:How biometrics can aid certification of digital signatures, International Review of Law, Computers & Technology ,Vol. 24, No. 1, March 2010, 133–141.

[73]Meints and Gasson, "High-Tech ID and emerging technologies", 138.

[74] http://www.afisandbiometrics.com/what_is_biometrics

[75]Robin Feldman, *Considerations on the Emerging Implementation of Biometric Technology*, 2003, 25 Hastings Comm. & Ent. L.J., p.1.

biometric signature as deriving the private key from a biometric sample; the benefits ensure security above and beyond the high encryption standards of PKI.[76] Thus, for a high level of security, it is desirable to have the biometric template stored on the particular device, to perform the match on device so that no biometric data leaves the device, and to install the required software on the device for the same reasons.[77]

In regards to privacy, which we will discuss in the next session, with biometric technology, personal information is gathered and stored easily without the subject having control or knowledge. Further, and most disconcertingly, the public has no idea who has access to the information being gathered or how it will be used.[78]It is important to acknowledge the fact that biometric technology is still developmental and evolving, and that "regardless of how much we invest in establishing standards for reliability of the technology and protections of the data from fraud or improper use, no system will be fool proof.[79] Biometric determinations will be subject to mistakes, fraud, and abuse through human and technological error, both intentional and inadvertent.[80] In conclusion, the use of biometrics can be categorized as one method of authentication for e-signatures under the regime of the Directive. Furthermore, biometrics can be regarded as e-signatures since they meet the criteria set in Article 2(1) of the Directive. This means that biometrics are converted to data in an electronic form, which are then attached to other electronic data that serves as a method of authentication.

2.2.2 Smart Card

E-signatures play an important role in electronic commerce. In the context of electronic commerce, one authentication method is the smart card, a technology that will be discussed in this section.

[76]K.J. Pawan and M.Y. Siyal, 'Novel Biometric Digital Signatures for Internet Based Applications', Information Management & Computer Security 9, no. 5 (2001): 205–12.
[77]Supra note 67.
[78] Sherman, Darcie , Biometric Technology: The Impact on Privacy (2005). CLPE Research Paper No. 5. Available at SSRN: http://ssrn.com/abstract=830049
[79]Ibid.
[80]Supra note 70, page 2.

Named for their ability to process information via an embedded computer chip, “smart cards” could become the most significant technological advancement in payment cards since the introduction of the magnetic stripe on credit cards.[81] The characteristics of the smart card enable it to not only store data but also update the data it stores, receive data, make decisions about data that it stores and receives, and detect unauthorized attempts to read its contents.[82]

With the growing use of wired and wireless networks to access information resources and the increasing occurrence of identity theft and attacks on corporate networks, password-based user authentication is increasingly acknowledged to be a significant security risk. Both enterprises and government agencies are moving to replace simple passwords with stronger, multi-factor authentication systems that strengthen information security, respond to market and regulatory conditions and lower support costs. To meet these needs, smart cards support all of the authentication technologies, storing password files, public key infrastructure certificates, one-time password seed files, and biometric image templates, as well as generating asymmetric key pairs.[83]

Smart cards deter fraudulent users and can ensure that only the person to whom the card is issued will be able to verify their identity when the card is presented. Its technology supports PINs, biometric factors, and visual identity verification; such verification links the individual cardholder and the document securely together and provides the necessary strong authentication of an individual’s identity.[84]

[81] Furletti, Mark J., An Overview of Smart Card Technology and Markets (April 2002). Federal Reserve Bank of Philla Payment Cards Center Discussion Paper No. 02-14. Available at SSRN: http://ssrn.com/abstract=927470
[82] Ibid.
[83] About Smart Cards : Applications : Enterprise ID, available at http://www.smartcardalliance.org/pages/smart-cards-applications-enterprise-id
[84] Alliance Activities : Publications : Smart Card Technology: The Right Choice for REAL ID, available at http://www.smartcardalliance.org/pages/publications-smart-cards-real-id

[85]

The e-signature is stored on a smart card and is used with the aid of a specialised card-reading device, and in this way specialised security mechanisms largely protect the actual identities of both partners in a contract.[86] In conclusion, Smart cards can bind the cardholders to their credentials and thus ensure that only those who are authorized to read the identity information are allowed to have access to the smart card for the extent of authentication. The author does not regard smart cards as advanced e-signatures, because in order for smart cards to be regarded as an advanced e-signatures, the criteria under Article 2(2) must be met. In this context, can the signatory maintain their smart card under their sole control for all time? What if the smart card is stolen? How can one find out that any subsequent change of the data is detectable? Does the company who issued the smart card will notify the owner of the smart card for every change of data or only several kinds of data changed will be notified? Under the regime of the Directive, the author regards this method of authentication as an e-signature, since the Directive leaves a very broad interpretation of the term. In this method, the data (such as PIN, name, birth date, etc.) is stored in an electronic form and associated logically with other electronic data, making it an e-signature.

[85] http://www.itblogs.in/electronics/introduction-to-smart-card/

[86] Heng, Stefan, E-Payments: Modern Complement to Traditional Payment Systems (May 6, 2004). E-Conomics Working Paper No. 44. Available at SSRN: http://ssrn.com/abstract=542523

2.3 Certification Service Provider

In accordance with Article 2(11), CSP means an entity or a legal or natural person who issues certificates or provides other services related to e-signatures. According to the Directive, member states have to ensure as a minimum standard that qualified CSPs are liable for damages in specified circumstances, unless the provider proves that it has not acted negligently.[87]CSPs issue certificates relating to e-signatures, which can be relevant to the admissibility of the signature and potentially also the reliability of that signature.[88]

In order to validate advanced e-signatures supported by qualified certificates, a receiving party would first need to check their trustworthiness.[89] This means that the receiving party has to be able to verify whether the signature is an advanced e-signature supported by a qualified certificate issued by a supervised CSP, as required by Article 3.3 of the Directive.[90] The receiving party may also need to verify whether the signature is supported by a secure signature creation device.[91]

Thus, the accreditation of the CSP does not determine whether the e-signature qualifies or not; it's the qualification of the e-signature itself that it is decisive.

Article 6 (1) of the Directive requires that where a CSP issues a qualified certificate to the public, or guarantees such a certificate, the CSP is liable for damage caused to any entity or legal or natural person who reasonably relies on the certificate in respect to:[92]

a. completeness and accuracy at the time of issuance of all information;

b. assurance that the designated signatory held the signature-creation data corresponding to the signature-verification data given or identified in the certificate; and,

---

[87]House of Commons Trade and Industry Committee, *Building Confidence in Electronic Commerce: The Government's Proposals* (1999).

[88]E-signatures FAQ, available at http://www.out-law.com/page-443, this article is based on UK law, it was last updated on September 2008.

[89]EU Trusted List of CSPs, available at http://ec.europa.eu/information_society/policy/esignature/eu_legislation/trusted_lists/index_en.htm

[90]Ibid.

[91]Ibid.

[92]See E-signatures and Associated Legislation, BERR Department for Business Enterprise & Regulatory Reform, available at http://www.bis.gov.uk/files/file49952.pdf

c. where the CSP generates both the signature creation data and the signature validation data, assurance that they work together, unless the CSP proves no negligence.

However, certain minimum requirements appear from Article 6 of the E-signature Directive, applicable to CSPs that issue qualified certificates: the liability is based upon negligence with a reversed burden of proof. Broadly speaking, a certification-service provider that issues qualified certificates is liable for damage caused to any party that reasonably relies on the content of such certificates as regards the accuracy of their content at the time they were issued, unless the provider proves that it has not acted negligently.[93]The CSP is not liable to the extent that the certificates have been used contrary to any limitations regarding the use of the certificates or any monetary limits, provided that such limitations are easily recognisable by third parties.[94] CSPs are subject to national rules regarding liability.[95]

Article 6 of the Directive sets out the minimum standards of liability that member states should impose on CSPs, and in Article 6(3) and 6(4) it states that CSPs may limit their liability on the use of their qualified certificates and such limitations must be recognised by third parties.[96] In regards to collection and processing of personal data, it sets out in Article 8(1) that CSPs are required to comply with Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on tile protection of individuals with regard to the processing of personal data and the free movement of such data.

2.4 Data Protection of E-signatures

Knowing that personal data is used and collected in order to authenticate a person's identity raises another issue: what about the protection of the data gathered and stored in the instrument (i.e., PKI, Biometrics, Smart card)? Here lies data protection regulation's real objective, as regulated by

[93]Rolf Riisnæs: Digital Certificates and Certification Services, page 17, available at http://www.scandinavianlaw.se/pdf/47-7.pdf
[94]Ibid.
[95]See Recital 22 of the Directive.
[96]See Article 6 (3) and 6 (4) of the Directive.

Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and the free movement of such data, with the intent to protect individual citizens against unjustified collection, storage, use and dissemination of their personal details.[97]

Data must be processed fairly, for specified purposes and on the basis of consent of the person concerned or some other legitimate basis laid down by law.[98]

In accordance with Article 8(1) of the Directive, member states shall ensure that CSPs and national bodies responsible for accreditation or supervision comply with the requirements laid down in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on tile protection of individuals with regard to the processing of personal data and the free movement of such data.

In the context of e-signatures, controllers and processors of personal data include the CSPs as well as any party that stores personal data with the purpose of relying on it.[99] One immediate requirement for the processing of personal data is the consent of the subscriber to a certificate, which must be given either explicitly by means of a subscriber agreement or implicitly through the conditions included in a certification practice statement or a certificate policy that is referenced in a subscriber agreement.[100] By requiring a binding agreement between the controller and the processor and establishing the duties of each of them, the questions of responsibility for the various stages of data processing are addressed.[101]

In accordance also with Article 8(2),the role also played by the CSPs is to ensure the quality of the personal data collection and also that it is only processed for the purpose of issuing qualified certificates.

[97]P.J. Hustinx, "Data Protection in the European Union", *Privacy and Informatie*, 2005, No.2, (pp. 62-65), p.62.
[98]De Hert P. &Gutwirth S., 'Data Protection in the Case Law of Strasbourg and Luxemburg: Constitutionalisation in Action' in Gutwirth S., Y. Poullet, P. De hert, J. Nouwt & C. De Terwangne (Eds), *Reinventing data protection?*, Springer Science, Dordrecht, 2009, p. 3-44.
[99]Supra note 38, p. 472.
[100]Supra note 38, page 473.
[101]Supra note 38, page 473.

Therefore, in associated with Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and the free movement of such data, personal data collected, processed and used in terms of e-signatures shall have guaranty that such personal data should not be processed at all, except when certain requirements such as transparency, legitimate purpose and proportionality are met.

2.5 Positive sides of Community Framework of E-signatures

In this sub-chapter, we will discuss what in legal literature is seen as the positive and negative sides of Community Framework of E-signatures (herewith referred to as "the CFES").

After adopting the Directive, the EU implemented new legislation that complements the Directive, creating an appropriate legal environment for e-commerce and e-transactions. For instance, Directive 2001/115/EC on electronic invoices recognises the validity of electronically sent invoices that use advanced e-signatures.[102]

Another example of EU directives that complement the one on e-signatures is the Public Procurement Directives. These directives do not explicitly state the type of e-signatures to be used in public procurement, but note that the use of e-signatures must comply with Directive 1999/93/EC. These directives call for uniformity regarding the domestic institution of e-signatures for public procurement so there are no barriers hindering e-procurement transactions among EU states.[103]

The Directive defines an e-signature as "data in electronic form which are attached to or logically associated with other electronic data and which serve as a method of authentication".[104]

---

[102] *Martha L. Arias, IBLS Director ,*INTERNET LAW - The EU Law on E-signatures and its Recent Report, December 2007, available at http://www.ibls.com/internet_law_news_portal_view.aspx?id=1920&s=latestnews

[103] Ibid.

[104] Article 2 (1) of the Directive.

This is very broad and covers, for example, a scanned manuscript signature into a word document.[105] Therefore it indicates the Directive to be technology neutral. The underlying principle, then, is that rules are technology neutral. In formulating technology-independent rules, however, it should be considered whether these guarantee sufficient legal security.[106]Another e-policy document, the G8 Okinawa Charter on Global Information Society, stated: "We should ensure that IT-related rules and practices are responsive to revolutionary changes in economic transactions, while taking into account the principles of effective public-private sector partnership, transparency and technological neutrality."[107]

It should be noted that there are also many ICT documents and laws that do not mention this underlying principle, and that many regulations and laws are actually quite technology specific.[108] Through this Article, it shows that the Directive is aiming to make e-signatures easier to use and help them become legally recognized within the member states without creating boundaries on specifying the criteria of e-signatures to avoid overlap of regulations in member states.

According to Article 3 (1) of the Directive, member states are prohibited from making the provision of CSP subject to prior authorisation.[109] In order to stimulate community-wide provision of certification services over open networks, CSPs should be free to provide their services without prior authorisation; the consequence is that any CSP will have to be allowed to provide its services without prior authorisation.[110]This is also in accordance with Recital 10 of the Directive, which states

---

[105]See I Lloyd, *Legal Aspects of the Information Society*, para 13.54, Butterworths, London, Edinburgh, Dublin, 2000; C Reed, *Internet law: text and materials*, Butterworths, London, 2000, p. 154; German E-signature Act, BT-Drucks. 14/4662 p. 18.

[106]ILIS Memorandum 2000, p. 20.

[107]Okinawa Charter On Global Information Society, *Declarations of Principles*, http://dotforce.org/reports/itl.html.

[108] Koops, Bert-Jaap, Should ICT Regulation be Technology-Neutral?. STARTING POINTS FOR ICT REGULATION. DECONSTRUCTING PREVALENT POLICY ONE-LINERS, IT & LAW SERIES, Bert-Jaap Koops, Miriam Lips, Corien Prins & Maurice Schellekens, eds., Vol. 9, pp. 77-108, The Hague: T.M.C. Asser Press, 2006. Available at SSRN: http://ssrn.com/abstract=918746.

[109]See Article 3(1) of the Directive.

[110]Jos Dumortier, The European Directive 1999/93/EC on a Community Framework for E-signatures, Published in Lodder, A.R., Kaspersen, H.W.K.,.: e Directives: Guide to European Union law on E-Commerce. Commentary on the Directives on Distance Selling, E-signatures, Electronic Commerce, Copyright in the Information Society, and Data Protection. Law and Electronic Commerce Series, Vol 14, Kluwer law International, p.33-65, ISBN 90-411-1752-0.

the following: “The internal market enables certification-service providers to develop their cross-border activities with a view to increasing their competitiveness, and thus to offer consumers and businesses new opportunities to exchange information and trade electronically in a secure way”.[111] This provision is also aimed at reducing any obstacles in a cross-border market that may arise within member states. Therefore, since prior authorisation is not needed by CSPs to meet the requirement of an accreditation scheme, EU member states show different approaches to the establishment of such accreditation schemes; while some countries plan to set up an accreditation scheme that is controlled by the state, others prefer a privately governed accreditation scheme.[112]It is, indeed, perfectly possible for a CSP established in one member state to provide certification services in another member state without having to ask the prior permission of a national authority. This was not possible everywhere in Europe before the Directive was issued and transposed.[113] It was a good decision for no permission to be necessary to become a certification-service provider under the Directive, as self-regulation can secure high standards and national permission would be contrary to free trade in the EU and would restrain the use of new technologies.[114]

In regards to the equivalence between handwritten signatures and e-signatures, the positive side is that discriminating between e-signatures and handwritten signatures is prohibited. According to Article 5 (1) of the Directive: “Member States shall ensure that advanced e-signatures which are based on a qualified certificate and which are created by a secure-signature-creation device “satisfy the legal requirements of a signature in relation to data in electronic form in the same manner as a hand-written signature satisfies those requirements in relation to paper-based data”.[115]In other words, this Article does not contain an obligation to use electronic data processing. Legal rules enforcing the use of paper documents can consequently continue to exist and they don’t have to be

[111]See recital 10 of the Directive.
[112]COLEMAN/SAPTE, *E-Commerce Bill-Ireland, the Irish Electronic Commerce Bill 2000*, Computer Law & Security Report Vol. 16 no. 4, 2000, p.249.
[113]Jos Dumortier, Stefan Kelm, The Legal and Market Aspects of E-signatures, Katholieke Universiteit Leuven, Study for the European Commission – DG Information Society.
[114]Supra note 64, page 10.
[115]See Article 5 (1) of the Directive.

abrogated, at least not according to this Directive.[116] Article 5(2) also states that e-signatures may not be denied legal effectiveness and admissibility as evidence in legal proceedings solely on the grounds that it is in electronic form or that the signature is not a qualified signature.[117] Although it seems to be a very positive indication for the acknowledgement of legal effect of e-signatures, there is still debate, and the counter argument on this issue will be elaborated in the next sub-chapter of this thesis.

2.6 Counter Argument on the Community Framework of E-signatures

Having discussed the positive sides of the Directive in the previous section, we now come to the discussion of the lacking of adequacy of the Directive based on scholars' opinions. These issues include diverging interpretations of advanced e-signatures among the member states, doubts regarding the ability of the Directive to cope with the emerging technologies, whether it is really a technology-neutral-oriented regulation, and the ambiguity of the liability of the CSPs. These issues will be briefly elaborated in the following sub-chapter to give some understanding about possibilities of shortcomings of the Directive.

2.6.1 Non-uniformity of Interpretations of Advanced E-signatures

There is a possibility that divergences will make advanced e-signatures useless. Why? The reason is that there are a large number of divergences remaining between member states about the requirements for qualified e-signatures, and the whole system adopted by European legislation is, in other words, only useful on condition that there is one common European concept of "qualified e-signature".[118] The definition seems to be technology neutral and allows the member states to interpret it accordingly, but it is also confusing if this concept is not interpreted in a similar way.

[116]Supra note 98, page 16, The progresive abrogation of such rules is, as far as electronic contracts are concerned, one of the objectives of the Electronic Commerce Directive.
[117]Supra note 52, page 10.
[118]Supra note 52, page 6.

A Belgian citizen, for example, wishing to make an electronic commercial transaction with a Greek company by using qualified e-signature should be certain that his/her signature will have, under Greek law, the same legal status as a handwritten signature. What a Belgian considers a "qualified e-signature" should therefore be equally recognized as such by Greek authorities. The whole system adopted by European legislation is, in other words, only useful on the condition that there is one common European concept of "qualified e-signature".[119]

The Directive leaves decisions regarding two critical points up to the discretion of the member states: they may introduce or maintain "voluntary accreditation schemes aiming at enhanced levels of certification service provision", and can also make the use of e-signatures in the public sector subject to possible additional requirements. Such requirements shall be objective, transparent, proportionate, and non-discriminatory, and shall only relate to the specific characteristics of the application.[120]

2.6.2 The present regulation framework might not able to cover future technology

Technology is rapidly developed nowadays, and it is almost impossible to predict what kind of new technology or devices will be innovated or invented. Therefore it is more secure to create a neutral regulation instead of a codified one in order to cover all kinds of possibilities in technology. The technology of e-signatures is developing quickly and it is practically impossible to predict what kind of e-signature will be most successful.[121] This may be either a hardware and software solution including mathematical features, as is used today, or a more secure but more expensive biometric solution, or something completely new.[122] Moreover, the use of a European Union Directive may be

[119]Supra note 52, page 6.
[120]Alexander Rossnagel, Digital Signature Regulation and European Trends, page 4, available at http://www.emr-sb.de/news/Dsregulation.pdf
[121]Supra note 64, page 7.
[122]For details see R Hopkins, 'An Introduction to Biometrics and Large Scale Civilian Identification'(1999) 13 *International Review of Law Computers & Technology* 337: Biometrics is 'the application of computional methods to biological features, especially with regard to the study of unique biological characteristics of humans"; see also Reed, *Internet Law*, p 161; see also<www.penop.com>.

even more inappropriate since the changing of European legislation is a rather difficult and slow process.[123]

With reference to the UCITA, it is said that a detailed codification is premature and unwise, and no codification at all for the next five years would be preferable.[124]It can be concluded that the Directive is seen to be more useless in the upcoming years due to the possibility of the rapid development and change in the terms of technology. In the future there might be other technology regarding e-signatures that is considered to be more secure and reliable than the technology mentioned in Article 5 of the Directive.

2.6.3 Is it Really Technology Neutral?

It is doubtful whether the Directive is really, as it is claimed, technology neutral.[125] Although it does not exclude other forms of cryptography or entirely different types of technology, it is particularly based upon public key cryptography.[126] The Directive creates the b presumption that "advanced e-signatures which are based on a *qualified certificate*… satisfy the legal requirements of a signature ... in the same manner as a handwritten signature".[127]This presumption is of limited functionally to digital signatures because qualified certificates are unique to PKI technology.[128]

It follows that signatures created through signature dynamics would not enjoy the same presumptive validity as digital signatures because they provide direct proof of signer identity rather than relying on "a complex system of trusted third parties".[129]This is not "technological neutrality"

[123]Supra note 64, page 8.
[124]See J Braucher, 'The 2BGuide: Why UCITA, like UCC Article 2b, is Premature and Unsound'<www.2bguide.com/docs/0499jb.html >.
[125]Supra note 64, page 8.
[126]See I Lloyd, *Information Technology Law* 3rd ed., Butterworths, London, 2000, para 29. 61 (in a different context).
[127]See Article 5 of the Directive.
[128]Andrew Barofsky, The European Commission's Directive on E-signatures: Technological "Favoritism" Towards Digital Signatures, Boston College International and Comparative Law Review, Volume 24 Issue 1, Article 5, 12-1-2000.
[129]Philip S. Corwin, *Digital Sigllа/lm>s and Sigllature DYllalllics: Some Issues /0 Considl'l;* 17 BANKING POL'y REp. 1. 10 no. 9 (1998). at 15.

but rather "technological favouritism."[130] The UCITA, the UNCITRAL Draft Uniform Rules and the OECD principles appear to be more neutral in the choice of method.[131]It is true that sometimes legislation refers explicitly to standards, but only insofar that this is strictly necessary and the reference to a particular standard is mostly interpreted in a restrictive manner.[132]In the review process it should be analysed which regulations should follow a technology-neutral approach (e.g. Article 5(2)) and for which regulations it would be better to make the implicit link to asymmetric cryptography explicit for better understanding.[133]

The Directive addresses how e-signatures are created and explains what type of organisational structure is needed in general terms, and it also gives legal recognition to documents that are electronically signed, but it also prioritises the growth of a complex network of PKIs providing electronic certificates for the recognition and development of e-signatures.[134]

In this case, since the Directive seeks to be technology neutral, it seems to be inconsistent if it is deliberately favouring advanced e-signatures to some extent.

2.6.4 Liability of CSP

The next issue is how a CSP can be held liable, since certification services can be freely provided in any member state without prior authorisation from a national authority.[135]Article 6 of the Directive and 17(3) of the consultation document state that a CSP that provides a qualified certificate shall be liable for "damage caused to any entity or legal or natural person who reasonably relies on that certificate" in regards to the accuracy of any information therein or as an assurance that the

[130]Supra note 116, page 14.

[131]See UCITA, ss. 102(a)(6), 107, 108; UNCITRAL Draft Uniform Rules on E-signatures, art. 3; OECD Guidelines for Cryptography Policy, principles no.2-4; see also Hogg, Secrecy andSignatures, pp 53-4; H L MacQueen, M A Hogg and P Hood, 'Muddling Through? Legal Responsesto E-Commerce from the Perspective of a Mixed Legal System', in Grosheide and BoeleWoelki (eds), *Molengrafica: Euopees Privatrecht*, Lelystad, 1998, pp 214-5.

[132]Supra note 52, page 7.

[133]Forum of European Supervisory Authorities for E-signatures (FESA) Important topics for the review of Directive 1999/93/EC from the supervisory authorities' point of view, June 30 2003., p. 4.

[134]Murray, J. Public Key Infrastructure Digital Signatures and Systematic Risk. *Journal ofInformation, Law and Technology.* 2003.

[135]See Article 3 of the Directive.

signatory held the relevant private key corresponding to the public key in the certificate.[136] A CSP that generates keys has a duty to ensure that they are complementary and will be liable unless the CSP proves that it has not acted negligently.[137]

The Directive requires that the member states ensure that CSPs are liable for the damage caused to their customers who rely on a qualified certificate issued by them. It also provides that the CSPs can limit their liabilities by limiting the use of their certificates.[138] Simple e-signature providers are therefore held accountable in accordance with national liability rules, which may cause an uneven situation for e-signature providers in Europe since the national liability rules vary.[139]
Article 6 of the Directive sets out specific CSP liability limitations to be transposed by the member states into national law; these limitations concern the scope of use of the certificate and the value of transactions for which the certification can be used.[140]Therefore it is unlikely that a CSP that makes it clear on the face of a qualified certificate that such a certificate cannot be used in transactions over £50,000 will be liable to a third party suing for a debt of £70,000.[141]

The supervision systems of the individual member states cannot ensure the enforcement of this requirement either. Since there is no assurance whatsoever that a provider is solvent, it is, in fact, possible for a financially weak organization to offer certification services and simply claim bankruptcy when the first loss occurs.[142]

The author includes liability of CSPs as one of the counter arguments of the Directive since it may give rise to problems concerning protection of consumers if something went wrong with a CSP. Although Annex II of the Directive sets out the requirements for certification-service providers

[136]Adèle Murphy B.L. analyses the issues raised by attempts to regulate electroniccommerce, from a national, european and international perspective, The Regulation of E-Commerce, available at http://www.lawlibrary.ie/documents/publications/adelemurphy.pdf
[137]Ibid.
[138]G.C. Parry, M. James-Moore, A.P. Graves and O. Altinok, Legal Aspects of E-signatures, University of Bath, School of Management, Working Paper Series, 2008.02 , p. 11.
[139]Supra note 125, page 11.
[140]Supra note 101, page 83.
[141]Supra note 124, page 3.
[142]Supra note 108, page 7.

issuing qualified certificates, there is no concrete and clear system on how to check or measure the financial resources of the CSPs as one of the measurement to validate whether a CSP is trustworthy enough to run the business. In the review process of the Directive it seems that this issue should also be taken into account.

2.7 Conclusion

International trade conducted over the internet requires a careful balance between technology, process and application. Electronic commerce that is built on a sustainable and integrated foundation is a necessary component for economic development. The use of the internet as a means of international trade has a remarkable role in cross-border transactions. The European Union, as one of the leading entities in regulating current issues such as electronic commerce in international trade, plays an important role in Indonesia as an emerging power in Asia. In this chapter the author has briefly elaborated on the Directive, which lays down the minimum requirements for security in the application of e-signatures, liability of certification-service providers, the legal certainty of e-signatures and the technology-neutral approach of the Directive. In addition, there are international dimensions for co-operation with countries outside the EU; as such, the Directive has the potential to become a stimulus for Indonesia in drafting legislation regarding e-signatures. Particularly, if Indonesia desires to have a mutual recognition on the basis of bilateral or multilateral agreements in international trade with member states through a secure online transaction, several criteria for e-signatures performed by Indonesian citizens must be met, according to the Directive. However the potential benefits that can be used as a model for Indonesia will be analysed further in the next chapter.

CHAPTER 3

OVERVIEW OF E-SIGNATURE REGULATION IN ASIAN COUNTRIES

RELEVANT TO INDONESIA

In this chapter, we will give a briefly overview of how e-signatures is regulated in several Asian countries, the author will take examples from Electronic Transaction Ordinance in Hongkong, Digital Signature Bill of 1997 in Malaysia and Singapore's Electronic Transaction Act of 1998. These countries have a close relationship with Indonesia in a term of international trade and political influence.[143] By taking into account the measurement in drafting legislation of e-signature from these countries, it might enhanced economic cooperation or market access among these countries with Indonesia in removing obstacles regarding exports to enter their market thus improving relationship in economic and political terms between both countries.

3.1 Electronic Transaction Ordinance in Hongkong.

The Ordinance mainly aims to provide a clear legal framework so that electronic records and digital signatures have the same legal recognition as that of their paper based counterparts, thereby promoting and facilitating the development of e- business in Hong Kong.[144]

There is one distinct characteristic in this Ordinance, which is Hong Kong only gives legal recognition to digital signature, but not other kinds of e-signatures, and the reason is that 'digital signature is currently the only technically mature technology that provides security service of a quality that satisfies the need for user authentication, ensuring the integrity and confidentiality of

[143] http://www2.bkpm.go.id/file_uploaded/public/5%20NEGARA%20PMA.pdf

[144] See Consultation Paper on the Review of Electronic Transaction Ordinance, available at http://www.google.nl/url?sa=t&rct=j&q=consultation%20paper%20on%20the%20review%20of%20the%20electronic%20transactions%20ordinance&source=web&cd=1&ved=0CCIQFjAA&url=http%3A%2F%2Fwww.ogcio.gov.hk%2Feng%2Feto%2Fdownload%2FETOreview-Consultation%28E%29.doc&ei=8ozaTq_MOMOVOou-4M8O&usg=AFQjCNHvAukcAfcTTIbAwfhC7tVzk2UA9g&cad=rja.

data and protecting non-repudiation of transactions.[145] Digital signature here is referred to as adoption of asymmetric cryptosystem, establishment of a voluntary recognition system of certification authorities and creation of recognized certification authorities, establishment of Public Key Infrastructure, and obligation of secrecy.[146]

Having regard with the CSP or CA (CAs), Hong Kong adopts a voluntary recognition system. As one Hong Kong government official explained, CAs are free to apply for recognition on a voluntary basis but only those CAs which have achieved certain objective standards will be 'recognized'. In other words, 'unrecognized' CAs may operate in Hong Kong side by side with RCA. Their activities and their relationship with their clients will, however, are governed by common law.[147]

As with other digital signature legislation, the Ordinance suffers from two fundamental problems. First, the changing nature of the digital signature technology has the potential of rendering the Ordinance obsolete within a short span of time, secondly, the Ordinance, being a local law in nature, is inadequate to cope with the regulation of e-commerce which is basically a global issue.[148]

One of the most common criticisms of the ETO was that although it was declared to be technologically neutral, in fact, it was not. It only gave legislative backing to one type of digital signature - the public key-private key signature based on public key infrastructure, and it has been proposed to also accomodate the use of personal identification numbers ("PIN") as a form of "digital signature" which will then have the same status as the public key-private key type "digital signature" currently backed by the Ordinance. [149] This change will mean that there are two types of "digital signatures" which have the same status as paper-based signatures.[150]

---

[145] Wu R, 'Electronic Transactions Ordinance – Building a Legal Framework for E-commerce in Hong Kong', 2000 (1) *The Journal of Information, Law and Technology (JILT)*. http://elj.warwick.ac.uk/jilt/00-1/wu.html

[146] Ibid

[147] See Hong Kong Government's Response to Comments made by the Hong Kong Computer Society , LC Paper No.CB(1)297/99-00(04)

[148] Swindell C and Henderson K **(**1998) ' Legal Regulation of Electronic Commerce', Journal of Information, Law and Technology 1998(3)

[149] David.A.Ellis, Proposed changes to the Hong Kong Electronic Transactions Ordinance, 2002, available at http://www.mayerbrown.com/publications/article.asp?id=7010&nid=6

Approach taken by the Ordinance also declared itself to be technology neutral as other technology related regulation, but in practice it also has preferences of the use of Public Key Infrastructure. It can not be denied that at the moment the Ordinance was enacted in 2002, Public Key Infrastucture was deemed to be one of the most sophisticated way in digital signature.[151]

As a Special Administrative Region in People's Republic of China and one of the world's leading international financial centres, Hongkong is known as a big player in asian trade.[152] It is also a leading supplier in Indonesian industries.

Based on these consideration, if Indonesia desire to deepen the economic cooperation and to improve market access, it might be more easily achieved if Indonesia taking into account some principles of ETO in drafting e-signature legislation. Under the regime of the Directive it has several similar characteristic, such as it's tendency of using Public Key Infrastructure although it declared to be technology neutral, and the voluntary scheme of CSP's recognition. This could be a good example for Indonesia, the voluntary recognition system might be applied in Indonesia since it allows the market to have self-recognition thus it might stimulate CSP to proRevide their utmost service for consumer.

3.2 Malaysia's Digital Signature Act of 1998

The Digital Signature Act 1997 and Digital Signature Regulation 1998 provide the licensing framework for the provision of digital signatures in Malaysia including the type of services, the qualification requirements, how to apply and the respected fees.[153] The Digital Signature Act used

---

[150] Ibid
[151] Ip I, 2000 'E-signature Recognition Bill Opens Door for e-commerce' Hong Kong Standard 6 January
[152] Official website Indonesia – China cooperation,
http://www.cic.mofcom.gov.cn/ciweb/cci/info/Article.jsp?a_no=257621&col_no=521
[153] Official Portal Of Malaysia Communications and Multimedia Commission
http://www.skmm.gov.my/index.php?c=public&v=art_view&art_id=88

the Utah Digital Signature Act as the model.[154] The Act regulates the legal recognition and authentication of the originator of electronic document. This Act enables businesses and the community to use e-signatures instead of their hand-written counterparts in legal and business transactions.[155] Similar with Hong Kong's Electronic Transaction Ordinance, this Bill is also provides regulation for Public Key Infrastructure.[156] The potential benefits of the public key infrastructure (PKI) implemented by the Utah Act are considerable, as a well-functioning public key infrastructure would allow private individuals, businesses and governments to routinely and securely conduct personal, financial and legal affairs over open networks like the Internet.[157]

For a digital signature to be recognised, it is necessary to obtain a certificate from a CA licensed by the Controller of Certification Authorities, and on the salient elements of this law are that Certification Authorities authorised by a foreign government entity may be recognised and that the liability of a CA is limited, a document created in accordance with this Act or signed digitally is legally binding as a document.[158]

The Act provides for penalties consisting of fines and jail terms for those who purport to hold CA licenses or operate as such without licenses. Those operating illegally can be fined a maximum of 500,000 ringgit (about US$125,000) or jailed for 10 years, or both.[159]

A valid license are required for CA to perform their function which is to to issue a certificate to a subscriber upon application and upon satisfaction of the licensed CA's requirements as to the identity of the subscriber to be listed in the certificate and upon payment of the prescribed fees and

---

[154] Lim Kit Siang, Instead of having the world's best Digital Signature Law, Malaysia has been landed with Utah II which is worse than Utah I, making our cyberlaw on digital signature the worst in the world, available at http://www.limkitsiang.com/archive/1997/May97/sg390.htm

[155] Mingfa Chen, Adequacy of Malaysia's Cyberlaws to Address Cybercrimes and Cybertorts, 2008, available at http://amrjournal.blogspot.com/2008/09/adequacy-of-malaysia-cyberlaws-to.html

[156] Ferrelica. Anne. M, Impact of ICT on Society: Malaysian Cyber Law, Electronic Governement Law, available at http://www.scribd.com/doc/33853666/Malaysian-Cyber-Law-Electronic-Government-Law

[157] Supra note 140, para 1

[158] See Chapter 5, Legal Matters, page 2 ,available at http://www.mampu.gov.my/pdf/MyMIS/chapter5.PDF

[159] Julian Matthews, Malaysia's Digital Signature Laws To Take Effect in October, 1998, available at http://www.trinetizen.com/archive/?p=69

charges .[160] One of the legislation in Malaysia Digital Signature Framework is Certificate of Recognition for a Repository. This legislation sets up requirement of how an entity could carried out an operation as a repository.[161] The repository contains certificates published by certification authorities that are required to conform to rules of practice that are similar to or more stringent that the requirement of the Act and its Regulations, it keeps and maintains an archive of certificates that have been suspended or revoked, or that have been expired at least he preceding ten years.[162] This regime on their legislation of Certificate of Recognition of Repository could be a good example for indonesia in setting up detailed legislation and to ensure secured connection between the transactional parties.

This regime is chosen to be discussed in this theses as Indonesia and Malaysia has agreed t o increase the countries cooperation and to strengthen their bilateral agreement. Having considered the regime of Malaysian legislation in e-signature may help to overcome number of issues in the future relating to any transaction made through internet by parties from both countries. One interesting fact to be compared with the Directive is that in this Act, government of Malaysia which done by the Commission (Malaysian Communications and Multimedia Commission established under the Malaysian Communications and Multimedia Commission Act 1998) requires CA to hold a valid license in order to perform their function, this mandatory licensing scheme is on the contrary with the regime in Article 3 of the Directive that forbids Member States to create an obligatory licensing scheme for CSPs to enter the market.

[160] See Article 4 and Article 6 of Digital Signature Act,
available at http://www.agc.gov.my/Akta/Vol.%2012/Act%20562.pdf
[161] Repository commonly refers to a location for storage, often for safety or preservation, based on definition by http://en.wikipedia.org/wiki/Repository
[162] Official Portal of Malaysian Communications and Multimedia Commission, available at http://www.skmm.gov.my/index.php?c=public&v=art_view&art_id=104

3.3 Singapore's Electronic Transaction Act of 1998

The law of contract is a common law development that has taken many years to reach its current matured state.[163] Although many of the rules seem archaic by comparison to the current technologies, many principles remain true in the electronic environment.[164] The Singapore Electronic Transactions Act 1998 (No. 25 of 1998) (the "ETA"), passed on 10 July 1998, was specifically adopted with the intent of resolving the legal concerns arising from new technologies that affect online business.[165]

While the Act has liberalised the boundaries of electronic records, it does not mean that electronic records may be substitutes for all cases where the law requires the matter to be in writing or have a written signature. The Act is clear as to what some of these matters that are not substituted by electronic records are. These include:[166]

(i) creation or execution of a will;

(ii) negotiable instruments;

(iii) declarations of trusts or power of attorney;

(iv) contracts for sale or other disposition of immovable property;

(v) conveyance or transfer of any immovable property; and

(vi) any document of title

The Electronic Transaction Act has a wide ambit that includes provisions relating to the Liability of Network Service Providers, Digital Signatures, Duties of Digital Signature Subscribers and Certification Authorities. [167]

---

[163] Harry SK Tan, The Impact of the Singapore Electronic Transactions Act on the Formation of E-contracts, 2002 *Kluwer Law International, Electronic Communication Law Review* **9**: 85–112, 2002, available at http://unpan1.un.org/intradoc/groups/public/documents/apcity/unpan026245.pdf

[164] Ibid

[165] Ibid

[166] E-commerce and Electronic Transactions Act 1998, available at http://www.google.co.id/url?sa=t&rct=j&q=singapore%27s%20electronic%20transaction%20act%20of%201998&source=web&cd=4&ved=0CDoQFjAD&url=http%3A%2F%2Fwww.drewnapier.com%2Fpublications%2FDnpub-6.pdf&ei=gMPaTvPWBsyfOqu94ccC&usg=AFQjCNGeaisznoGH6ACZ3YRGXp1k8PuUvQ&cad=rja

[167] The Model Law is available to the public by Internet access at *http://www.uncitral.org*. Other sources for the ETA included the Illinois Electronic Commerce Security Act; and Utah Digital Signature Act.

The Electronic Transaction**s** Act 2010 came into operation on 1 July 2010**.**[168] It repealed the previous edition of the Electronic Transaction**s** Act 1998 and brought Singapore's laws on electronic transaction**s** in line with the United Nations Convention on the Use of Electronic Communications in International Contracts which was adopted by the United Nations on 23 November 2005. [169] It also moves beyond PKI/tokens/digital certificates approved by the government approach of the past and now recognizes that parties that use mutually-agreed third-party solutions, which properly identify the parties, link to immutable/protected records, and that are properly secure, are afforded maximum legal protection and full equivalency to paper contracts.[170]

The Electronic Transactions Act essentially provides the legal foundation for the recognition of e-signatures, and Singapore is one of the first countries in the world to enact legislation which addresses the issues that arise in the context of electronic contracts and digital signatures. [171] Broadly, the Electronic Transaction Act seeks to:[172]

a. enact a commercial code to support e-commerce transactions;
b. set the legislative framework for specified security procedure providers like Certification Authorities;
c. enable electronic applications and licences for the public sector; and
d. clarify network service providers' liability for third party content.

---

[168] Rodyk & Davidson LLP. Woon C.Yew and Jeremy Tan, The Electronic Transactions Act 2010 a boost to the e-marketplace, 2010, available at http://www.lexology.com/library/detail.aspx?g=5e20c761-4ccd-4de3-8c0d-5c6eb6a9f2e1

[169] Ibid

[170] See Singapore Updates its E-signatures Laws, Moves Beyond PKI into the Web-Centric World, July 2010, available at http://blog.echosign.com/2010/07/singapore-replaces-its-electronic-signatures-laws-moves-beyond-pki-into-the-webcentric-world.html

[171] See The Impact of Regulatory Framework on E-Commerce in Singapore, Symposium Technology Development Group Singapore Academy of Law, 2002, available at http://www.lawnet.com.sg/legal/ln2/comm/PDF/The_impact_of_the_regulatory_framework_on_e_commerce_in_SG.pdf

[172] Official Portal of Singapore Government, available at http://www.ida.gov.sg/Policies%20and%20Regulation/20060920100740.aspx

How e-signatures is enacted in this country, the awareness of Singaporean Government in removing barriers in electronic commerce can be learned by Indonesia and also can be used as a comparative model. Under the regime of the Directive, the Electronic Transaction Act is also intended to be technology neutral although it qualifies digital signature as a form of e-signature that have equal legal recognition with handwritten signature.[173]

3.4 Conclusion

There are many obstacles in the admissibility of documents, contracts, or transactions signed by e-signature as valid evidence in court, it cannot be denied that legal recognition holds an important role in the position of e-signature, as for e-signature to have equal legal recognition with handwritten signature, it should meet certain requirements as set up in legislation. How to make such e-signature to be as secure as possible also becomes a challenge which needs to be overcome simultaneously due to the development of technology. Hong Kong, Malaysia and Singapore has attempted to provide legal certainty for e-signature to stimulates a positive growth in the term of electronic commerce and to facilitate in improving cross-border transaction.

Having discussed several above regime, it can be learned by Indonesia to consider some of the basic principle of their legislation. Hong Kong has a tendency in using Public Key Cryptography although it declared to be technology neutral, and similar with the regime of the Directive that it also applied a voluntary recognition system for CSP. Malaysia in the other hand seems to be more strict in regulating e-signature, it requires CSP to hold a valid license in order to carry out their services, as it also recognized the use Public Key Cryptography method of e-signature to be legally valid and enforceable as handwritten signature. Singapore as the first among these countries which recognized other method aside from Public Key Cryptography, although the definition of the third party solution used by the transactional parties remain unclear.

[173] Ibid

CHAPTER 4

HOW A COMMUNITY FRAMEWORK GOVERNING E-SIGNATURES CAN BE A MODEL FOR INDONESIAN LAW IN ESTABLISHING THEIR OWN REGULATIONS

This chapter consists of an overview of how legislation in Indonesia regulates e-signatures (e-signatures), to what extent Indonesian law should follow the European Union (EU) Directive in establishing their own regulations concerning e-signatures and what is necessity to amend the current draft in Indonesia. This chapter also contains a brief explanation of how inadequate Indonesian laws related to e-signatures may be overcome using some ideas from the EU Directive.

4.1 E-signatures in Indonesia

Indonesia has entered a new stage in the world of information and communication, namely the use of the Internet. Indonesia is a developing country where communication, data exchange and online transactions via the Internet have increased greatly. The rapid development of electronic transactions made by society is sometimes considered to be unforeseeable. In today's modern world, transactions can be accomplished electronically without face-to-face interaction or having to physically sign a document. In addition, print-outs may be used as legal evidence. What if a document comes in a soft copy format and is signed electronically using public key infrastructure (PKI)? Is the document considered proper evidence? Does it have the same legal weight a document with a handwritten signature has? To facilitate giving electronic documents the same legal weight as hard copy documents, evidence that comes in a soft copy format may be cited as the expansion of valid evidence.

Article 184 in Kitab Undang Undang Hukum Pidana (Book of Laws of Criminal Procedure of Indonesia) does not explicitly recognise electronic data as valid evidence in court. It only recognises the following as valid evidence in court: [174]

a. Statements of witnesses,
b. Statements of experts,
c. letters,
d. instructions and
e. information given by defendants.

Regarding the term "letters", it can be concluded that the Book of Laws does not explicitly recognise letters with an e-signature as valid evidence. The Book of Laws was enacted in 1981, at which time electronic commerce (e-commerce), cybercrime and other Internet-related issues were uncommon compared to today.[175]

However, just because it is not stated specifically, does it mean that electronic documents bearing e-signatures cannot be accepted as valid evidence in court? By law, as long as there is no denial of the contents of such documents, electronic documents should be accepted as having the same legal weight as conventional documents bearing handwritten signatures.[176]

Indonesian law has never provided a definition of the word "signature", which actually has two basic legal functions, namely: (1) the identification of the signatory and (2) as a sign the signatory has approved or agreed to the contents of a document. A "signature is an identity that serves as a sign of approval of the obligations attached to the deed". [177]Therefore the basic notion of signature needs to be meet by e-signature, which using electronic means to have the deed/document signed.

[174] Translated by the author.
[175] Dedy Suwasono, SH, KUHAP History: Sejarah Lahirnya KUHAP, February 2009, available at http://dediwongcilik.blogspot.com/2009/02/sejarah-lahirnya-kuhap-setelah-lahirnya.html
[176]http://hukumonline.com/berita/baca/hol5954/data-elektronik-sebagai-alat-bukti-masih-dipertanyakan.
[177]Julius Indra Dwipayono Singara, S.H., D.E.A, Pengakuan tanda Tangan Elektronik dalam Hukum Pembuktian di Indonesia, available at http://julian.unsri.ac.id/userfiles/file/Materi%20Pertemuan%206%20Bagian%201.pdf

Technological advances can then be anticipated by the law. Information settings, documents, and e-signatures, as stated in Article 5 through Article 12 of Law Number 11 Year 2008 of Information and Electronic Transaction. In general, electronic information and/or electronic documents and/or prints-outs are valid legal evidence according to Indonesian law. The same is true of e-signatures.

4.2 How Legislation in Indonesia Regulates E-signatures

Based on a general explanation of Indonesian Law Number 11 Year 2008 regarding Information and Electronic Transactions (hereinafter referred to as "the Law"), information technology is the combination of communication and technology provided by the Internet. As a result, borders between countries virtually no longer exist. It increases the speed and efficiency of e-commerce and electronic governance (hereinafter referred to as "e-governance"). This benefits society in that it makes various information-related activities easier. However, the phenomenon has also triggered various forms of societal conflict as a result of unauthorised usage.[178]

Article 11 of the Law states that "E-signatures has the force of law legitimate and legal consequences by fulfilling the provisions of this Law", as long as it can be guaranteed there is a link between the e-signature with the concerned signing, and e-signatures are created and stored in conditions that guarantee the integrity with the document, deed or transaction concerned, then such e-signatures has the same legal value with handwritten signature.[179]

The Law was enacted in April, 2008 but has yet to be implemented. A government regulation and the formation of two new institutions, the Certification Body Electronics Reliability and Operator

---

[178] Translated by the author. See Law Number 11 Year 2008 http://www.batan.go.id/prod_hukum/extern/uu-ite-11-2008.pdf.
[179] See Article 11 of the Law.

Certification, are still forthcoming. These two institutions are expected to function as follows.[180]

1. The Reliability Certification Body will perform an administrative function that includes registration, authentication against the perpetrators of physical effort, the creation and management of certificates reliability, and maintaining a list of certificates that are frozen. Any business wanting to use electronic transactions can have a certificate issued by the Institute for Reliability Certification by registering themselves. The Reliability Certification Agency will collect data and make assessments regarding the identity of the business, the terms under which they provide products, and the type of products provided. If the business passes the certification test, a logo can be placed on the business' homepage indicating it has been officially certified to conduct business online.

2. Certification of Electronic Organisers deals with the registration and authentication of applicants' public and private keys, electronic certificate management, and certificate list is frozen. Each party will conduct the electronic transactions needed to meet the minimum requirements of the Law; in short, e-signatures are required for electronic transactions. E-signatures will be more secure if there is a third party involved in the transaction. The third party is the Operator Certification Electronics and its main function is to issue electronic certificates containing e-signature creation data known as the 'public key' and the 'private key'. Business people who want to obtain a Certificate of Electronics to support the use of e-signatures on electronic transactions may apply to the Operator Certification Electronics. The Operator Certification Electronic data collection and assessment process will include verifying the applicant's identity, physical authentication of the applicant, and other requirements. If there are no problems, then a public key, a private key, and a certificate will be issued. This will give society a sense of security and increase the confidence of transacting parties.

---

[180] Dr. Ronny, M.Kom, M.H, Sembilan Peraturan Pemerintah dan Dua Lembaga yang baru untuk UU ITE, 2008, available at http://saepudinonline.wordpress.com/2010/11/09/sembilan-peraturan-pemerintah-dan-dua-lembaga-yang-baru-untuk-uu-ite/

These two institutions seem to be expected to deal with any loopholes that may have been created by the Law, yet the government regulation governing the establishment of these two institutions is still being drafted.

In the draft of Article 1 (21),the Draft of Information and Electronic Transactions, e-signatures are defined as electronic information that is attached to, associated with or related to other electronic information that is used as a means of verification and authentication. [181]

In comparison with a previous definition In the Draft of government regulation on E-signatures (hereinafter referred to as "Draft of the regulation on e-signatures"), e-signatures are defined in more detail as electronic information that is attached, has a direct connection to or is associated with other electronic information created by the signatories to demonstrate their legal identity, including but not limited to the use of PKI (digital signature), biometrics and symmetric cryptography, including the original signature that is converted into electronic data.[182]

As legislation governing the use of e-signatures is still in draft form, it might be quite a while before the government actually implements the Law.

4.3 Examples of Possible Frameworks and Rules for Indonesia

As discussed, Indonesia has no law specifically regulating the use of e-signatures. Yet, innumerable transactions are being made throughout the country via the Internet. If Indonesia wants to participate in bilateral or multilateral agreements, the government needs to establish a solid regulatory framework that deals with e-commerce and with e-signatures in particular. This is necessary to ensure legality for all transactional parties.

---

[181] See Article 1 (21) of the draft on the Organisation of Information and Electronic Transactions at http://www.google.co.id/url?sa=t&rct=j&q=rpp%20pite&source=web&cd=2&sqi=2&ved=0CB8QFjAB&url=http%3A%2F%2Fwww.postel.go.id%2Fcontent%2FID%2Fregulasi%2Ftelekomunikasi%2Fpp%2Frpp%2520pite%2520hasil%2520rapat%252030%2520juli.sent.publikasi.doc&ei=iqrwTs7kIIfqOYD9nKIB&usg=AFQjCNFXzakMreJBaQxoUowRwTEqj-uvNg&cad=rja

[182] See Article 1 (3), the draft of the government regulation governing the use of e-signatures, available at http://dc105.4shared.com/doc/xuMMdSX_/preview.html

The Indonesian framework legislation separates the regulation of e-signatures and the regulation of CSPs (CSPs) (electronic certification). So far, the drafting process of the Draft of the regulation on e-signatures is at the stage of assesment and public testing, since it still needs to be scrutinized with various improvements and optimally by various parties, either directly or indirectly interested. [183] As mentioned in the previous chapter, the Directive is set up to be a technology-neutral regulation, therefore the Draft of the regulation on e-signatures may also be considered to be technology-neutral as it allows choice in terms of the type of e-signature used to sign electronic documents.[184] That neutrality is documented in Article 2(3) of Draft of Government Regulation of E-sign, as follows. "There is no provision in this government regulation that restricting the use any technique of making and use of e-signatures". I believe this provision allows for any form of e-signature that may occur with advancing technology.

Article 3 of the Draft states that e-signatures have legal force if the following requirements are met:[185]

a) e-signature data relates only to the signatory;
b) e-signature data at the time of electronic signing is only available under the signatory sole control;
c) any changes made to the e-signature after the data was originally created must be detectable; and
d) there must be proof that the signatory approves the content of the electronic document.

One of the requirements of the Directive is that e-signatures are created using a "secure" signature-creation device. This criterion is not included in the Draft of the regulation on e-signatures. I believe this criterion should be mandatory in order for e-signatures to have legal weight. This will

[183] See Official Website of Ministry of Communication and Information Technology, Directorate General of Post and Informatics
available at http://www.postel.go.id/artikel_c_1_p_1.htm
[184] See Article 2 (2) of the Draft of the regulation on e-signatures.
[185] See Article 3 of the Draft of the regulation on e-signatures

ensure the validity and security of e-signatures Such devices can be in the form of a smart card, random reader, or physical tokens solely controlled by the signatory. The capability of such devices to function together with signatory-verification devices must be assessed and guaranteed.

The “no prior authorisation” principle in Article 3 of the Directive should also be applied in Indonesia as it opens the market and deliver the competition to the market to decide. The “no prior authorisation” here means that member states may not make the provision of CSPs subject to prior authorisation. Prior authorisation here does not only mean that CSPs need permission to obtain a decision/license/approval from national authorities/government bodies before being allowed to provide services, but also refers to any other requirements having the same effect.

It is a good idea to apply this principle not only to open the market to ensure the reliability and trustworthiness of CSPs, but also to minimise the administrative procedures CSPs must follow to provide their services. Procedures created by government bodies or national authorities to obtain a license might take a long time and even after CSPs obtain a license, there is no absolute guarantee CSPs will fulfil their obligations as stated in the license requirements. It would seem more reasonable to let the market decide which CSPs are trustworthy. However, supervision of CSPs by a national authority or government body would still be necessary to provide legal certainty for society. Such regulatory supervision is proposed in Article 22 of the Draft of Government Regulation of Organisation of Information and Electronic Transaction.[186]

Based on Article 5 (3) of the Directive, which deals with the legality of e-signatures, I believe this type of assurance should be considered in the Draft of the regulation on e-signatures. It provides more of a legal basis for e-signatures to be evidence in court proceedings.

[186] See Draft of Government Regulation of Organisation of Information and Electronic Transaction http://www.google.co.id/url?sa=t&rct=j&q=rpp%20pite&source=web&cd=2&sqi=2&ved=0CB8QFjAB&url=http%3A%2F%2Fwww.postel.go.id%2Fcontent%2FID%2Fregulasi%2Ftelekomunikasi%2Fpp%2Frpp%2520pite%2520hasil%2520rapat%252030%2520juli.sent.publikasi.doc&ei=terwTpO0MYOVOsi5yZ4B&usg=AFQjCNFXzakMreJBaQxoUowRwTEqj-uvNg&cad=rja

4.4 What needs to be Amended or Proposed in the Current Draft of Provisions in Indonesia

The first issue concerns the retention of data stored in e-signatures. The devices used to create e-signatures store the personal data of signatories. Issues include how to manage the availability, integrity, authenticity, confidentiality and accessibility of that data. Since Indonesia has no unified law that covers data protection, there are different regulations for each sector. Concern about protecting personal data can be seen as progress in terms of the development of information technology and communication in Indonesia. The term data protection can be found in Article 26 of the Law:[187]

(1) Unless otherwise provided by Laws and Regulations, the use of any information obtained via electronic media that involves personal data must be with the consent of the person concerned.

(2) Any person whose rights are infringed upon as intended by section (1) may lodge a claim for damages under this Law.

Nevertheless, based on the article above, the protection of personal data by the Law is considered to be too general and may not be adequate. In regards with the fact that Indonesia has no codified regulation of protection of personal data, therefore this lack needs to be addressed in the Draft of Government Regulation of e-signature to overcome the loopholes.

The second issue concerns compliance with international standards. Nowhere is it stated that e-signatures have to meet international standards. For example, according to Article 7 of the Directive, cooperation between member states and non-member states is based on the principle of mutual recognition of certificates and is effected through bilateral or multilateral agreements. With the expansion of e-commerce, there will be more potential for Indonesian citizens to conduct electronic transactions with EU citizens. To complete such transactions, e-signatures might be required. Thus to comply with international standard from the first place, which might be include to

[187] Ali Budihardjo, Nugroho, Reksodiputro translation.
http://www.pranata.lipi.go.id/wpcontent/uploads/2009/01/UUTIE.pdf

be regulated in the Draft of Government Regulation of E-sign, shall give a good atmosphere for Indonesia to enter international trade as one of the reliable and trustworthy country to have a business with and to give more opportunity for Indonesia to have bilateral or multilateral agreement in electronic commerce. In particular with Member States who has a high level of protection regarding e-commerce.

4.5 Conclusion

The rise of globalisation and electronic transactions requires the government of Indonesia to establish a decent legal framework to protect their citizens in terms of conducting e-commerce. Despite the current limitations, such as the lack of e-commerce legislation, particularly in regards e-signatures, the lack of infrastructure and other economic and socio-cultural conditions, efforts have been made by the government to protect transactional parties as technology advances.

As discussed, Indonesia has a lot of work to do to amend the current proposed draft. Considering Indonesia has no unified law regarding e-commerce, having a single comprehensive regulation governing the use of e-signatures that covers all loop holes and weaknesses in the Law is necessary.

CHAPTER 5

CONCLUDING REMARKS

This chapter consists of the conclusion and recommendations.

5.1 Conclusion

1. *How does Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for E-signatures regulate e-signatures?*

The Directive provides a legal framework for member states regarding e-signatures and CSPs. It takes a technology-neutral approach in order to adapt to ever changing technology. The Directive also introduces new terms, such as advanced e-signature and CSP. Regarding market access, the Directive also stipulates CSPs not be subject to prior authorisation in order to ensure a flow freely market. A voluntary accreditation scheme for CSPs is also provided by the Directive.

The Directive not only states that advanced e-signatures have the same legal weight as handwritten signatures, it sets out the requirements for a qualified certificate, a qualified certificate provider and secure signature creation devices in Annex I, II, and III. The Directive requires that member states ensure CSPs are liable for any damage to their clients. It also stipulates that CSPs may limit their liability by limiting the use of their certificates and that they must notify any third party involved.

2. *Based on the legal literature, what are the positive and negative sides of the Community Framework on E-signatures?*

Taking a technology-neutral approach is a good starting point. Such an approach accommodates the rapid development of technology and avoids any overlap with member states in terms of regulating e-signatures. The voluntary accreditation scheme provided by the Directive is intended to allow a freely circulated e-signature in member states. Such a scheme will increase the trust and confidence of users while also potentially helping level the competitive playing field for CSPs. The

acknowledgement that advanced e-signatures are equal to handwritten ones also provides legal certainty in the world of e-commerce.

However, the Directive does have some drawbacks, such as too broad an interpretation of various terms. For example, not all member states agree about what constitutes a qualified e-signature. It is also doubtful the Directive can deal suitably with technological innovations since it is supposed to be technology-neutral (yet it seems to emphasise the use of PKI).

3. *To what extent should the Indonesian Law follow the Community Framework on E-signatures in order to establish a regulation governing e-signatures and what does it mean in regards amending the current proposed provisions?*

International instruments such as the Directive could be a good starting point to encourage the regulating of e-commerce and e-signatures in particular. To truly be a part of the international community, Indonesia must be able to cooperate with other countries by providing an adequate legal framework to regulate international trade by their citizens.

Being a developing country, Indonesia faces complex limitations in terms of infrastructure and social issues. It cannot be denied that the government needs to provide an adequate legal framework to regulate trade and business, much of which is conducted electronically via the Internet. The Directive's main principles of being technology-neutral, making e-signatures equal to handwritten ones, and the voluntary accreditation scheme should be legally instituted in Indonesia. Other provisions such as requires the use of 'secure' signature creation device, possibility of CSP to limit their liability in the certificate, and the assurance of protection of personal data should also be legally instituted.

5.2 Recommendations

i. Having no single unified law governing e-commerce and e-signatures in particular could cause Indonesia to be left behind in terms of economic cooperation with the international community. It therefore might be useful for Indonesia to learn from another country's successful regulatory framework and laws to help in establishing their own legal framework regarding e-commerce and e-signatures.

ii. Furthermore, each legal framework in several asian countries should learn one another, in this case the author will briefly recommend Indonesia to consider, for instance, applying voluntary recognition system for CSP from the Hong Kong legal framework, which is in the contrary with the Malaysia legal framework that applying mandatory licensing scheme for CSP to enter the market. Likewise the Singapore legal framework, Indonesia should always keep the awareness of development of technology in the upcoming years in a manner of enacting legislation and not just rely on the present legal framework.

iii. Establishing a comprehensive legal framework regarding e-commerce and e-signatures will strengthen Indonesia's position in terms of participating in bilateral or multilateral agreements.

Bibliography

Legislation/Directive/Convention

Chinese

Electronic Transactions Ordinance

Consultation Paper on the Review of Electronic Transaction Ordinance

EU

Digital Signature Act

Directive 1999/93/EC on a Community framework for electronic signatures

German Electronic Signature Act

Final Report of the EESSI Final Team, European Electronic Signature Standardization Initiative, July 1999

Forum of European Supervisory Authorities for Electronic Signatures (FESA) Important topics for the review of Directive 1999/93/EC

EU Trusted List of Certification Service Providers

Report on the operation of Directive 1999/93/EC on a Community framework for electronic signatures

Indonesia

Law Number 11 Year 2008 on Information and Electronic Transactions

Draft of the government regulation governing the use of e-signatures

Draft on the Organisation of Information and Electronic Transactions

Malaysia

Digital Signature Bill of 1997

Singapore

E-commerce and Electronic Transactions Act 1998

Books, Journals, Articles & Papers

Aalberts B P & Van der Hof S, Digital Signature Blindness Analysis of Legislative Approaches to Electronic Authentication (2000) The EDI Law Review Vol. 7 No. 1 1.p.26.

Adèle Murphy B.L. analyses the issues raised by attempts to regulate electronic commerce, from a national, european and international perspective, The Regulation of E-Commerce, available at http://www.lawlibrary.ie/documents/publications/adelemurphy.pdf

Alexander Rossnagel, Digital Signature Regulation and European Trends, page 4, available at http://www.emr-sb.de/news/Dsregulation.pdf

Andrew Barofsky, The European Commission's Directive on Electronic Signatures: Technological "Favoritism" Towards Digital Signatures, Boston College International and Comparative Law Review, Volume 24 Issue 1, Article 5, 12-1-2000

Andrzej M. Borzyszkowski, Electronic signature, the theory and the practice, Poland and Europe, Institute of Computer Science, Gda´nsk Branch, Polish Acad. of Sci.Abrahama 18, 81-825 Sopot, Poland http://www.ipipan.gda.pl/, available at http://www.google.nl/url?sa=t&rct=j&q=background%20of%20electronic%20signature%20in%20europe&source=web&cd=9&ved=0CG0QFjAI&url=http%3A%2F%2Fciteseerx.ist.psu.edu%2Fviewdoc%2Fdownload%3Fdoi%3D10.1.1.62.4975%26rep%3Drep1%26type%3Dpdf&ei=5yL5TpeZLsma-wa2nYTMAQ&usg=AFQjCNGO52bNJ6IO-Js2BbTGuIcmWz8nLw&cad=rja

Bowden, Bramhall, Cameron, Cassassa-Mont, Colvill, Goodman, Hilton, Marhøfer, White, EEMA Identity Technologies and Services Working Group, authors daft v0.35, 24 March 2004

Bromby, Michael, Identification, trust and privacy:How biometrics can aid certification of digital signatures, International Review of Law, Computers & Technology ,Vol. 24, No. 1, March 2010, 133–141.

Colman/Sapte, E-Commerce Bill-Ireland, the Irish Electronic Commerce Bill 2000, Computer Law & Security Report Vol. 16 no. 4 2000, p.249.

De Hert P. &Gutwirth S., 'Data Protection in the Case Law of Strasbourg and Luxemburg: Constitutionalisation in Action' in Gutwirth S., Y. Poullet, P. De hert, J. Nouwt & C. De Terwangne (Eds), Reinventing data protection?, Springer Science, Dordrecht, 2009, 3-44

Electronic Signatures and Associated Legislation, BERR Department for Business Enterprise & Regulatory Reform, available at http://www.bis.gov.uk/files/file49952.pdf

G.C. Parry, M. James-Moore, A.P. Graves and O. Altinok, Legal Aspects of Electronic Signatures, University of Bath, School of Management, Working Paper Series, 2008.02 , page 11

Harina Yuhetty, ICT and Education in Indonesia, available at http://gauge.u-gakugei.ac.jp/apeid/apeid02/papers/Indonesia.htm

Harry SK Tan, Electronics Transaction Regulations-Singapore, Computer law and Security Report, Volume 18 Issue 4, 31 July 2002, page 272-277Issue 4, 31 July 2002, page 272-277See Directive 1999/93/EC of 13 December 1999 on community framework for electronic signatures, available at: http://www.sciencedirect.com/science?_ob=RedirectURL&_method=externObjLink&_locator=url&_issn=02673649&_origin=article&_zone=art_page&_plusSign=%2B&_targetURL=http%253A%252F%252Feuropa.eu.int%252Fcomm%252Finternal_market%252Fen%252Fmedia%252Fsign%252Findex.htm.

Harry SK Tan, The Impact of the Singapore Electronic Transactions Act on the Formation of E-contracts, 2002 Kluwer Law International, Electronic Communication Law Review 9: 85–112, 2002, available at http://unpan1.un.org/intradoc/groups/public/documents/apcity/unpan026245.pdf

Heng, Stefan, E-Payments: Modern Complement to Traditional Payment Systems (May 6, 2004). E-Conomics Working Paper No. 44. Available at SSRN: http://ssrn.com/abstract=542523

Hong Kong Government's Response to Comments made by the Hong Kong Computer Society , LC Paper No. CB(1)297/99-00(04)

House of Commons Trade and Industry Committee, Building Confidence in Electronic Commerce:The Government's Proposals (1999)

I Lloyd, Information Technology Law 3rd edn, Butterworths, London, 2000, para 29. 61

I Lloyd, Legal Aspects of the Information Society, para 13.54, Butterworths, London,

Jacques R. Francoeur, B.A.Sc., M.A.Sc., MBA, Electronic Signature Assurance & the Digital Chain-of-Evidence Executing Legally Admissible Digitally Signed Records, Proof Space White Paper, page 7, available at http://www.proofspace.com/UserFiles/File/esignature.pdf

Jos Dumortier, Legal Status of Qualified Electronic Signatures in Europe, available at https://www.law.kuleuven.be/icri/publications/611ISSE_2004_Dumortier_Text.pdf

Jos Dumortier, Stefan Kelm, The Legal and Market Aspects of Electronic Signatures, Katholieke Universiteit Leuven, Study for the European Commission – DG Information Society.

Jos Dumortier, The European Directive 1999/93/EC on a Community Framework for Electronic Signatures, Published in Lodder, A.R., Kaspersen, H.W.K.,: e Directives: Guide to European Union law on E-Commerce. Commentary on the Directives on Distance Selling, Electronic Signatures, Electronic Commerce, Copyright in the Information Society, and Data Protection. Law and Electronic Commerce Series, Vol 14, Kluwer law International, p.33-65, ISBN 90-411-1752-0

K.J. Pawan and M.Y. Siyal, 'Novel Biometric Digital Signatures for Internet Based Applications', Information Management & Computer Security 9, no. 5 (2001): 205–12.

Koops, Bert-Jaap, Should ICT Regulation be Technology-Neutral?. STARTING POINTS FOR ICT REGULATION. DECONSTRUCTING PREVALENT POLICY ONE-LINERS, IT & LAW SERIES, Bert-Jaap Koops, Miriam Lips, Corien Prins& Maurice Schellekens, eds., Vol. 9, pp. 77-108, The Hague: T.M.C. Asser Press, 2006. Available at SSRN: http://ssrn.com/abstract=918746.

MacQueen, M A Hogg and P Hood, 'Muddling Through? Legal Responses to E-Commerce from the Perspective of a Mixed Legal System', in Grosheide and Boele Woelki (eds), Molengrafica: Euopees Privatrecht, Lelystad, 1998, pp 214-5.

Mathias M. Siems, The EU Directive on Electronic Signatures: A Worldwide Model or A Fruitless Attempt To Regulate The Future?, page 14.

Murray, J. Public Key Infrastructure Digital Signatures and Systematic Risk. Journal of Information, Law and Technology. 2003.

Philip S. Corwin, Digital Siglla/lm>s and Sigllature DYllalllics: Some Issues /0 Considl'l; 17 BANKING POL'y REp. 1. 10 no. 9 (1998). at 15

P.J. Hustinx, "Data Protection in the European Union", Privacy and Informatie, 2005, No.2, (pp. 62-65), p.62

Prof Mieke Komar Kantaatmadja, Electronic Commerce and Electronic Legal Issues in Indonesia, page 2, available at http://www.aseanlawassociation.org/docs/w5_indo2.pdf

Ralf Cimander, Meik Hansen, Prof. Dr. Herbert Kubicek, Electronic Signatures as Obstacle for

Cross-Border E-Procurement in Europe, Lessons from the PROCURE-project, InstitutfürInformationsmanagement Bremen GmbH (ifib) AmFallturm 1 28359, Bremen, June, 2009, p.9.

Recommendation on Authentication in Electronic Commerce, May 1999, prepared by Alliance for Global Bussiness for is presented to the Joint OECD Private Sector Workshop on Electronic Authentication (Stanford and Menlo Park, 2-4 June 1999), as a minimum checklist of business requirements for government policies addressing authentication in electronic commerce, available at http://www.biac.org/statements/iccp/AGB_authentication_principlesI.pdf

Report Meeting of Ministry of Information and CommunicationRepublic of Korea, Electronic Transactions Act and Digital Signature Act, Background, Major Provisions and Implication, OECD Forum on Electronic Commerce, 12~13 October 1999, Paris

R Hopkins, 'An Introduction to Biometrics and Large Scale Civilian Identification' (1999) 13 International Review of Law Computers & Technology 337: Biometrics is 'the application of computional methods to biological features, especially with regard to the study of unique biological characteristics of humans"; see also Reed, Internet Law, p 161; see also <www.penop.com>.

Robin Feldman, 'Considerations on the Emerging Implementation of Biometric Technology,' 2003, 25 Hastings Comm. & Ent. L.J., p.1

Rolf Riisnæs: Digital Certificates and Certification Services, page 17, available at http://www.scandinavianlaw.se/pdf/47-7.pdf

Royer & Rosnagel, Profitability of Mobile Qualified Electronic Signatures, page 1345, available at

http://www.is-frankfurt.de/publikationenNeu/ProfitabilityofMobileQualified1320.pdf

Sherman, Darcie , Biometric Technology: The Impact on Privacy (2005). CLPE Research Paper No. 5. Available at SSRN: http://ssrn.com/abstract=830049

State Archives Department, Minnesota Historical Society ,March 2004, Version 4 , Page 5, Available at http://www.mnhs.org/preserve/records/electronicrecords/docs_pdfs/ersigs.pdf

Sunu Purbanti A. Rini, Indonesian APEC Study Center, COUNTRY REPORT LEGAL FRAMEWORKS AND E-COMMERCE TRAINING PROGRAM (INDONESIA), page 7, available at http://www.apec.org.au/docs/rini.pdf

Swindell C and Henderson K (1998) ' Legal Regulation of Electronic Commerce', Journal of Information, Law and Technology 1998(3)

Thomas Myhr, Regulating a European EiD a Preliminary Study on a Regulatory Framework for Entity Authentication and a pan European Electronic ID for the Porvoo e-ID Group, Januari 2005, Page 7, available at http://skilriki.is/media/skjol/Regulating_a_European_eID.pdf

The Impact of Regulatory Framework on E-Commerce in Singapore, Symposium Technology Development Group Singapore Academy of Law, 2002, available at http://www.lawnet.com.sg/legal/ln2/comm/PDF/The_impact_of_the_regulatory_framework_on_e_commerce_in_SG.pdf

U Blaurock and J Adam, 'Elektronische Signatur und europäisches

Privatrecht' (2001) Zeitschrift für Europäisches Privatrecht 93 at pp 98 and 110.

Van Eecke, in Bullesbach/Poullet/Prins, Concise IT, Directive 1999/93/EC of The European Parliament and of The Council of 13 December 1999 on a Community Framework for Electronic Signatures, page 444.

Wu R, 'Electronic Transactions Ordinance – Building a Legal Framework for E-commerce in Hong Kong', 2000 (1)*The Journal of Information, Law and Technology (JILT)*.http://elj.warwick.ac.uk/jilt/00-1/wu.html

Websites, Online Contents and Other Sources of Information

About Smart Cards : Applications : Enterprise ID, available at http://www.smartcardalliance.org/pages/smart-cards-applications-enterprise-id

Ali Budihardjo, Nugroho, Reksodiputro translation. http://www.pranata.lipi.go.id/wpcontent/uploads/2009/01/UUTIE.pdf

Alliance Activities : Publications : Smart Card Technology: The Right Choice for REAL ID, available at http://www.smartcardalliance.org/pages/publications-smart-cards-real-id

A PKI enables users of a basically unsecure public network such as the Internet to securely and privately exchange data and money through the use of a public and a private cryptographic key pair that is obtained and shared through a trusted authority.http://searchsecurity.techtarget.com/tip/PKI-and-digital-certificates-Security-authentication-and-implementation

David.A.Ellis, Proposed changes to the Hong Kong Electronic Transactions Ordinance, 2002, available at
http://www.mayerbrown.com/publications/article.asp?id=7010&nid=6

DedySuwasono, SH, KUHAP History: SejarahLahirnya KUHAP, February 2009, available at http://dediwongcilik.blogspot.com/2009/02/sejarah-lahirnya-kuhap-setelah-lahirnya.html

Dr. Ronny, M.Kom, M.H, Sembilan PeraturanPemerintahdanDuaLembaga yang baruuntuk UU ITE, 2008, available at
http://saepudinonline.wordpress.com/2010/11/09/sembilan-peraturan-pemerintah-dan-dua-lembaga-yang-baru-untuk-uu-ite/

Electronic Signatures FAQ, available at http://www.out-law.com/page-443, this article is based on UK law, it was last updated on September 2008.

E-Sign Legislation - The milestone in the e-signature history, available at
http://www.elock.com/resources-e-sign.html

Europe's Information Society, Thematic Portal, esignature, available at
http://ec.europa.eu/information_society/policy/esignature/index_en.htm

Ferrelica. Anne. M, Impact of ICT on Society: Malaysian Cyber Law, Electronic Governement Law, available at http://www.scribd.com/doc/33853666/Malaysian-Cyber-Law-Electronic-Government-Law

Furletti, Mark J., An Overview of Smart Card Technology and Markets (April 2002).
Federal Reserve Bank of Philla Payment Cards Center Discussion Paper No. 02-14. Available at SSRN: http://ssrn.com/abstract=927470

Harun Reksodiputro, The Law and Electronic Transactions and information – a general outlin, July 2008, available at
http://www.asialaw.com/Article/2004303/Channel/17441/The-law-on-electronic-transactions-and-information-a-general-outline.html

http://hukumonline.com/berita/baca/hol5954/data-elektronik-sebagai-alat-bukti-masih-dipertanyakan.

http://www.afisandbiometrics.com/what_is_biometrics

http://www2.bkpm.go.id/file_uploaded/public/5%20NEGARA%20PMA.pdf

http://www.itblogs.in/electronics/introduction-to-smart-card/

Internet Law – The EU Law on Electronic Signatures and its Recent Report, Martha L. Arias, IBLS Director, December 2007,
http://www.ibls.com/internet_law_news_portal_view.aspx?id=1920&s=latestnews
ILIS Memorandum 2000, p. 20

Edinburgh, Dublin, 2000; C Reed, Internet law: text and materials, Butterworths, London, 2000,

Ip I, 2000 'Electronic Signature Recognition Bill Opens Door for e-commerce' Hong Kong Standard 6 January

J Braucher, 'The 2BGuide: Why UCITA, like UCC Article 2b, is Premature and Unsound' www.2bguide.com/docs/0499jb.html

Jim Brayton, Andrea Finneman, Nathan Turajski, and Scott Wiltsey, Definition PKI (Public Key Infrastructure), October 2006, available at
http://searchsecurity.techtarget.com/definition/PKI

Jim Carroll, Electronic Commerce and The Paperless Economy, available at http://www.cyberlaw.com/images/getting_to_digital_signatures.pdf
John B Harris, "This is legal, right?" – Electronic Signatures & The Law, May 2008, available at http://blogs.adobe.com/security/2008/05/this_is_legal_right.html

Jonathan Rosenoer, Getting to Digital Signatures and Electronic Commerce, June 1998, available at http://www.cyberlaw.com/images/getting_to_digital_signatures.pdf

Julius Indra Dwipayono Singara, S.H., D.E.A, Pengakuan tanda Tangan Elektronik dalam Hukum Pembuktian di Indonesia, available at
http://julian.unsri.ac.id/userfiles/file/Materi%20Pertemuan%206%20Bagian%201.pdf

Julian Matthews, Malaysia's Digital Signature Laws To Take Effect in October, 1998, available at http://www.trinetizen.com/archive/?p=69

Law Number 11 Year 2008 http://www.batan.go.id/prod_hukum/extern/uu-ite-11-2008.pdf.Translated by the author.

Law Number 11 Year 2008 on Information and Electronic Transactions
www.detikinet.com/read/2008/03/31/130700/915866/399/pasal-transaksi-elektronik-bakal-persulit-perbankan.

Legal Matters, chapter 5, page 2 ,available at
http://www.mampu.gov.my/pdf/MyMIS/chapter5.PDF

Lim Kit Siang, Instead of having the world's best Digital Signature Law, Malaysia has been landed with Utah II which is worse than Utah I, making our cyberlaw on digital signature the worst in the world, available at
http://www.limkitsiang.com/archive/1997/May97/sg390.htm

Martha L. Arias, IBLS Director, INTERNET LAW - The EU Law on Electronic Signatures and its Recent Report, December 2007, available at
http://www.ibls.com/internet_law_news_portal_view.aspx?id=1920&s=latestnews

Martin WilcockBEng, MSc(Eng), MSc, DIC, AMIChemE, Open Governance: The Case for Unregulated E-Commerce, available at

http://www.arraydev.com/commerce/jibc/0001-05.htm

Mazzeo, Mirella, Digital Signatures and European Laws, November 2010, http://www.symantec.com/connect/articles/digital-signatures-and-european-laws

Meints and Gasson, “High-Tech ID and emerging technologies”, 138

Mingfa Chen, Adequacy of Malaysia's Cyberlaws to Address Cybercrimes and Cybertorts, 2008, available at http://amrjournal.blogspot.com/2008/09/adequacy-of-malaysia-cyberlaws-to.html

Official Portal Of Malaysia Communications and Multimedia Commission
http://www.skmm.gov.my/index.php?c=public&v=art_view&art_id=88

Official Portal of Malaysian Communications and Multimedia Commission, available athttp://www.skmm.gov.my/index.php?c=public&v=art_view&art_id=104

Official Portal of Singapore Government, available at
http://www.ida.gov.sg/Policies%20and%20Regulation/20060920100740.aspx

Official website Indonesia – China cooperation,
http://www.cic.mofcom.gov.cn/ciweb/cci/info/Article.jsp?a_no=257621&col_no=521

Official Website of Ministry of Communication and Information Technology, Directorate General of Post and Informatics
available at http://www.postel.go.id/artikel_c_1_p_1.htm

Okinawa Charter On Global Information Society, Declarations of Principles, http://dotforce.org/reports/itl.html.

Philip Hlavaty, The Risks Involved With Open and Closed Public Key Infrastructure, February 2003, available at
http://www.sans.org/reading_room/whitepapers/vpns/risks-involved-open-closed-public-key-infrastructure_882

Repository commonly refers to a location for storage, often for safety or preservation, based on definition by http://en.wikipedia.org/wiki/Repository

Rodyk & Davidson LLP. Woon C.Yew and Jeremy Tan, The Electronic Transactions Act 2010 a boost to the e-marketplace, 2010, available at http://www.lexology.com/library/detail.aspx?g=5e20c761-4ccd-4de3-8c0d-5c6eb6a9f2e1

Singapore Updates its Electronic Signatures Laws, Moves Beyond PKI into the Web-Centric World, July 2010, available at http://blog.echosign.com/2010/07/singapore-replaces-its-electronic-signatures-laws-moves-beyond-pki-into-the-webcentric-world.html

Source of the picture: http://alwajbaiss.com/?p=469

Ter Kah Leng, Have You Signed Your Electronic Contract, 2011, available at available at www.sciencedirect.com

The Model Law is available to the public by Internet access at http://www.uncitral.org. Other sources for the ETA included the Illinois Electronic Commerce Security Act; and Utah Digital Signature Act.

UCITA, ss. 102(a)(6), 107, 108; UNCITRAL Draft Uniform Rules on Electronic Signatures, art. 3; OECD Guidelines for Cryptography Policy, principles no.2-4; see also Hogg, Secrecy and Signatures, pp 53-4; H L