August 2021

Validity of Digital Signature as Evidence in Electronic Commerce

Patricia Audrey Ruslijanto

Follow this and additional works at: <https://scholarhub.ui.ac.id/ijil>

Part of the [International Law Commons](#)

Recommended Citation

Ruslijanto, Patricia Audrey (2021) "Validity of Digital Signature as Evidence in Electronic Commerce," *Indonesian Journal of International Law*: Vol. 8 : No. 4 , Article 4.

DOI: 10.17304/ijil.vol8.4.314

Available at: <https://scholarhub.ui.ac.id/ijil/vol8/iss4/4>

This Article is brought to you for free and open access by the Faculty of Law at UI Scholars Hub. It has been accepted for inclusion in Indonesian Journal of International Law by an authorized editor of UI Scholars Hub.

Validity of Digital Signature as Evidence in Electronic Commerce

Patricia Audrey Ruslijanto¹

Trade is a way to promote economy, recognized that trade is important, urge the emergence of new trading concept. Electronic Commerce is the succumbed attendance of faceless trading. Alongside the development of technology, crimes also develop rapidly. Cyber crime is the type of crime in the virtual world. Recognized this problem, the appearance of security system in cryptography is well developed. Digital Signature is the manifestation of cryptography in asymmetric cryptosystem. Ironically well problem solving of this condition is not entails with its position as evidence in electronic contract. In evidence law, the presence of digital signature is approved as evidence in electronic commerce. It based on the equality of hash function. The validity of digital signature also approved as evidence in electronic commerce based on the approval of art. 11 Law No 11/2008 on Information and Electronic Transaction, which emphasize the legal position of digital signature as valid evidence in electronic commerce. Considering the constraints that arise in digital signature verification divided into Non juridical consist of technology and cultural obstacle. In case a dispute occurs either in transnational area, the jurisdiction that used in cyberspace area need precise principles rooted from the principle of international law. These principles are: subjective, objective territoriality, passive nationality, protective principle and universality interest jurisdiction, theory of the law of the server and theory of international space.

Keywords: *electronic commerce, digital signature, electronic contract, evidence, Law No. 11 Year 2008*

I. Introduction

The existence of trade and its development in the era of globalization is an important issue in people's life nowadays. In its essential way, globalization as a process of social transformation has brought the condition of humans' life in different countries and region into one borderless condition². The awareness that trade as a way to promote economic development

¹ Lecturer at the Faculty of Law, Brawijaya University.

² A.F. Elly Erawaty. *Globalisasi Ekonomi dan Perdagangan Bebas: Suatu Pengantar dalam Ida Susanti & Bayu Seto. Aspek Hukum dari Perdagangan Bebas (2003). Citra Aditya Bakti. Bandung. p 3.*

has encouraged countries in performs both regional yet international trade in increasing prosperity of their countries³.

The globalization of the market place and the means of equality in accessing through superhighways national and global information have given a new dimension to the concept of information. The development of information age has brought significant and extensive use of global communication networks. The invention of interconnected network (internet) which is the development of computer technology has ignited the imagination of people. The seamless merging of data, information and entertainment has opened up new vistas for businesses⁴. The development of information technology has brought great impact that changes the conduction of trade from face to face into faceless trading. The new type of trading via internet called as electronic commerce or e-commerce.

Electronic commerce represents a broad range of technologies, processes and practices which automate the transacting of business through largely paperless mechanisms, involves information communicated via electronic mail, Electronic Data Interchange (EDI), or the World Wide Web. It also encompasses transactions in and between private and public sectors in both domestic and international communities⁵. By the conduction of electronic commerce, sellers could advertise their wares and services globally meanwhile buyers, businesses and consumers alike had access to products at competitive prices. Sellers could provide product information, prices, delivery terms, and interested parties could negotiate terms and conclude contracts electronically. Direct access to a potentially large customer base meant that sellers did not have to opt for the traditional methods for selling their products. Equally, buyers get a fast paced, easier and practical service in choosing particular product and services in various qualities and quantities without go through agents to find suitable manufacturers of products they required⁶.

However, along with the development of technology itself the possibilities of crime development also grow widespread. The existence of cyber crime as a form of new dimensions crime has attracted world attention. In general, it defined as "an effort to enter or use of computer facilities or computer networks without permissions and against the law with or

3 E.D. Maharani. *Perdagangan Elektronik*. www.hukumonline.com. Diakses 22 Maret 2008.

4 Kamlesh K Bajaj & Debjani Nag. *E-Commerce: The Cutting Edge of Business* (2000). Tata McGraw Hill Publishing Company. New Delhi, India. p 6.

5 Warwick Ford & Michael S. Baum. *Secure Electronic Commerce : Building the Infrastructure Digital Signature and Encryption* (1997). Prentice Hall. New Jersey. p 1.

6 Indira Corr. *International Trade Law* (2005). Cavendish Publishing. United Kingdom. p 103.

without changes or damages over computer facilities which are accessible or used"⁷. Another definition given by the Organization of European Community Development is "any illegal, unethical or unauthorized behavior relating to the automatic processing and or the transmission of data"⁸.

In an environment where the transactions took place with the use of paper documents make an easier way to conduct investigation when the discordance in sale and purchase transactions occur, but it will not be the same for the sale and purchase transaction in paperless trading that requires more complicated way about the burden of proof. Nevertheless, trade still wants to be assured that the electronic world is safe. The electronic commerce system must offer at least the same level of reliability as that which obtains in the paper world. It is well known that frauds do take place in the traditional paper based transactions, signatures can be forged, paper documents can be tampered with while on the electronic commerce world⁹ since they are directly the outcome of creating documents electronically, transmittance over world wide computer communication network need the convincement that such documents are authentic when received over networks, and their authentication can be established in case of dispute.

Transactions may be electronic, but the key concept of admissibility of evidence and evidential value of electronic documents which important to the law remain the same. There must be a way to prove that a message existed, that it was sent and received by the authorized party, it was not changed between the sending and receiving process.

In further development, the urgency in finding security method to provide protection in dealing with electronic commerce transaction weakness can reduce with the appliance of cryptography and in this term with the use of digital signature. Digital signature itself is an alphanumeric character generated a number of mathematical operations of cryptography that produced from a computer to an electronic document¹⁰. From a legal perspective, digital signature is a secure-lock upon digital data that made with private signature key that depends on the permission of public key user that become its partner, and its existence marked with discharge of signature key certificate from certifier. From a technical perspective, digital

7 Dikdik M Arief Mansyur & Elisatris Gultom, *Cyberlaw-aspek hukum teknologi informasi* (2000). Citra Aditya Bakti. Bandung. p 8.

8 Dikdik M Arief Mansyur, Elisatris Gultom. *Ibid.* p 8.

9 Kamlesh K Bajaj & Debjani Nag. *Op Cit.* p 259.

10 B. Schneier. *Applied Cryptography* (1994). John Wiley & Sons Inc. USA. p 22.

signature is a numeric value which fitted with a data using mathematical procedure known to the owner of the cryptographic key¹¹.

The existence of processing series that must passed by receiver before validating message sender's, involving also the public key infrastructure that become the working points of digital signature, deems to be able to provide security guarantees for the existing electronic commerce transaction, ironically digital signature advantages from its security aspect is not comparable from its legal aspect, wherein this condition related to the validity of digital signature as evidence in electronic aspect yet to create enforceable digital transaction that bring equity to the parties¹².

Where in the existing Indonesia's law of evidence the existence of electronic evidence has not received in a widespread recognition, particularly from its burden of proof, data authenticity, binding forcibility of electronic contract including also electronic commerce dispute settlement.

The paper attempts to analyze the validity of digital signature as evidence in electronic commerce and the burden of proof of digital signature in electronic commerce in such ways to make electronic commerce at least as secure and legally binding as traditional commercial transaction.

II. Validity of Digital Signature as Evidence in Electronic Commerce

Legality of electronic commerce has become a new juridical phenomenon to Indonesia's law and need to consider for further assessment in evidence law aspect. The presence of evidence as stipulated in article 1865 Indonesian Civil Code stated that :

Everyone, who claims to have a right, or, in order to confirm his own right or to deny someone else' right referring to an event, is obliged to prove the existence of such event.

In further explanation, there are four type of evidence (considered as conventional evidence) that is stipulated in article 1866 Indonesian Civil Code, namely: "Written evidence, presumptions, confession and oath."

11 D. Budhijanto. Aspek Hukum Digital Signature & Certification Authorities dalam Transaksi E-Commerce dalam M.K.Kantaatnaja. Cyberlaw: Suatu Pengantar (2000). ELIPS. Bandung. p 67.

12 I.B.R. Supancana. Kekuatan Akta Elektronik sebagai Alat Bukti pada Transaksi E-Commerce dalam Sistem Hukum Indonesia. www.indoregulation.com . diakses 22 Maret 2008.

The existence of Indonesia's evidence law in its presence as a part of procedural law characterized by its forcible nature, meaning that all kinds of evidence as provided in the four type of evidence must not diminished yet added.

However in its progressive development, the role of new evidence (considered as non-conventional evidence) related to the development of technology cannot be waived. Therefore, by the presence of confession evidence that divided into two types that are: confession by judge and confession by law enabling non conventional evidence to show its role in giving more accurate burden of proof rather than conventional evidence¹³.

The presence of non conventional evidence that often related to the development of technology is demonstrative evidence, by its function to make certain facts proposed to the court clearer and more understandable by its real impression of the legal facts.

There are few types of demonstrative evidence that are often used, namely :

- a. photographs or video recordings;
- b. sound recordings via tape recorder, telephone or text messages via mobile phone;
- c. maps, models or chart, diagrams, sketches and tables;
- d. X-Ray recording, CT Scans and various other medical equipment; and
- e. duplication on evidence¹⁴

On the other hand, from the perspective of legal aspect, there are few requirement that need to fulfill by demonstrative evidence for its legally binding as evidence, that are:

- a. The existence of object as evidence;
- b. Representative accuracy, meaning that the equalization of size, shape and its dimension in avoiding confusion in evidence proofing as needed;
- c. Authentication, meaning that the demonstrated evidence should describe and represent the actual evidence;
- d. Identification, meaning that the demonstrated evidence should match exactly with the actual evidence;

13 Munir Fuady I. *Teori hukum Pembuktian (Pidana dan Perdata)* (2006). Citra Aditya Bakti. Bandung, p 185.

14 Munir Fuady I. *Ibid.* p 187.

- e. Admissibility, meaning that the demonstrated evidence must be able to prove something relevant, significant and competent; and
- f. Equality, meaning that the demonstrated evidence should clarify the proven fact¹⁵

Meanwhile, when we talk about signature it's not only speak about conventional signature as we used to know in conventional contract, it will show parties will to agree upon agreement that has created yet provide parties opportunities in verifying the agreement when needed. Meanwhile, the presence of electronic signature in its function term does not have big difference in conventional signature, where as by its function in transforming electronic data message or electronic document using cryptography system obtained from certificate authorization, it will provide important function like:

- a. minimize the risk for any parties actions who attempts to breach the agreement;
- b. minimize the risk of documents forgery;
- c. provide high level security for information transmission over open networks;
- d. provide convenience for non paper agreement transaction; and
- e. provide security assurance for the reliability of data integrity by the function of cryptography key in securing any changes upon documents¹⁶

In relating digital signature as a type of electronic signature, it also has important characteristic that are:

a. Authenticity

Authenticity means that it should possible to prevent any person or object from masquerading as some other person or object. When a data message received, it should possible to verify whether it has indeed been sent by the person or object claiming to be the originator. The authenticity of electronic data obtained from digital certificate by user/applicant request to Certificate Authority. This digital certificate contains user/applicant information including identity, authority, legal position, user status. With the presence of digital certificate, it will

15 M.D.Badrulzaman. *Harmonisasi Hukum Bisnis di Lingkungan Negara-Negara ASEAN*. Jurnal Hukum Bisnis Vol 22(2) 2003.

16 David Banbridge. *Introduction to Commerce Law*. Longman Pearson. UK. p 34.

provide third party certainty that the messages comes from user/ap-
plicant.

1. Integrity

Integrity means that it should possible to generate an alert on any mod-
ification, addition or deletion to the original content. The presence of
integrity in data sending also providing assurance that the submitted
data will never be modified or changed during the sending and saving
by unauthorized party.

2. Non-Repudiability

Non Repudiability means non deniable. By the appliance of digital sig-
nature, sender cannot deny that he/she has sent the messages yet deny
the content of the messages when it come to content differences.

3. Confidentiality

Confidentiality means that information should be protected from pry-
ing eyes of unauthorized internal users, external hackers and from be-
ing intercepted during transmission on communication networks by
making it unintelligible to the attacker. The confidentiality of digital
signature provided by digital envelope, that has been the integrality
part of digital signature that make the encrypted part only available by
the entitled person.¹⁷

Based on the explanation above in analyzing the validity of digital sig-
nature as evidence, as we know from the previous explanation on the posi-
tion of digital signature in electronic commerce, there are some theories
that strengthen the validity of digital signature as evidence, that are:

1. Injurious Reliance Theory

Achievement of both parties is the basis of this theory that explains also
that the agreement considered existing where it has created trust for the
parties who are bound in it¹⁸. In relating this theory with the presence
of digital signature, it shown from the agreement in giving consent by
the usage of digital signature to validate yet secure the signed agree-
ment between them.

2. Offer and Acceptance Theory

This theory is the basis consent of will, that explain the presence of
one's offer and other's acceptance create new consent of will¹⁹. In re-

¹⁷ Kamlesh K Bajaj & Debjani Nag. *Op Cit*. P 198-199.

¹⁸ Munir Fuady II. *Menata Bisnis Modern di Era Global* (2005). Citra Aditya Bakti. Bandung.
5-8.

¹⁹ Munir Fuady II. *Ibid*. p 5-8.

lating this theory with the presence of digital signature, it shown from the seller's offer in website follow by buyer in show his/her intention to buy by clicking OK/I Agree, then there has been consent of will upon the object followed by terms and manner of payment.

c. Evidence based on Law in Negative Aspect

This theory is the combination of conviction in time evidence theory and evidence based on law in positive aspect. This system of evidence use both judge belief yet law role in determining the validity of evidence²⁰. In relating this theory with the presence of digital signature, it is shown from the combination of judge interpretation by using extensive interpretation in interpreting the presence of electronic documents as a new type of evidence yet strengthen by the presence of article 11 Law 11/2008 on Information and Electronic Transaction noting that the legal standing of digital signature as evidence as far as it meet the imposing requirements.

Meanwhile, the presence of the above theory in analyzing the presence of digital signature as evidence in electronic commerce strengthen by the appliance of further international yet national regulation that applied. The presence of United Nation Commission on International Trade Law (UNCITRAL) that established Model Law on Electronic Commerce in December, 16, 1996. With the establishment on this Model Law, it give legal recognition of data message transmitted via electronic or other form, yet in attempt in finding technical solutions to meet the requirements of existing law and providing recognition of existing data messages. This Model Law aims in facilitate e-commerce among and within nations in validating transactions entered into by any means of new information technology yet promoting and encourage the implementation of new information technologies.²¹

Responding to this issue, many countries has provided regulations on electronic commerce, in the year 2000 United States of America regulates Federal Electronic Signatures in Global and National Commerce Act that abbreviated as E-Sign Act. By the regulation of E-Sign Act, it will provide that no contract, record, or signature may be denied legal effect solely because it is in an electronic form. In other words, under this law, an electronic signature is as valid as a signature on paper, and electronic documents

²⁰ Ibid.

²¹ Indira Corr. Op Cit. p 111.

can be as enforceable as a paper one. Meanwhile for the enforceability of electronic signature, the contracting parties must agreed to use electronic signatures²² In the same year Europe also regulates in The EU Directive on E-Commerce 2000 that give assurances that its countries member ensure that their legal system allows the conduction of electronic contract. The EU Directive of E-Commerce also focuses in the free movement of information society services amongst member states and the protection of the online customer.²³

Meanwhile in Asian countries, China also has its regulation by the establishment of the Contract Law of People Republic of China stated that various type of contract includes visually stored writing also classified as the type of electronic contract. Malaysia also has its regulation in Digital Signature Regulation 1998, while Singapore by the establishment of Singapore Electronic Transaction Act 1998.

Whether in Indonesia, the presence of Digital Signature as evidence in electronic commerce can be analyzed from two type of view, that related to the presence of required qualifications for the validity of an agreement as stipulated in article 1320 and 1338 Indonesian Civil Code and the regulation on the legal basis of electronic commerce as stipulated in Law 11/2008 on Information and Electronic Transaction.

The presence of contract that has been type of human interaction always evolving and develop from the simplest until most complexes adapted with the type of human interaction itself²⁴. In theory the regulations governing commercial activities in the business conduction not only through legal provisions that created and enforced the state, but also through personal rights to law making autonomy in binding agreement and manage the implementation business among themselves and other business actor.²⁵

Therefore in analyzing the presence of electronic contract with digital signature that provide the protection of electronic document and its legal standing can classified as valid evidence and fulfill the requirements in agreements based on article 1320 that defines the qualifications of valid article that are: the presence of consent of those who bind themselves, the capability to make an agreement, the presence of particular object and law-

²² Roger Leroy & Mille Gaylord, *Marketing & E-Commerce the Online Legal Environment* (2002). Thomson Jearny West. USA. p 164.

²³ Indira Corr. *Op Cit.* p 118.

²⁴ Ahmad Alsagoff, *Principles of The Law of Contract in Malaysia* (2003). Lexis Nexis . p 60.

²⁵ Ricardo Simanjuntak, *Asas-Asas Utama Hukum Kontrak dalam Kontrak Dagang Internasional: Sebuah Tinjauan Hukum*. Jurnal Hukum Bisnis.

ful cause (good faith principle). Whereas by this requirements the presence of consent by the offer and acceptance to be bound in electronic contract, includes also term of payment and other condition applied upon buyer and seller agreement and security method by usage of digital signature to be applied upon the electronic document, though the capability to make an agreement is not simply yet easy aspect that usually convinced by many people, but this condition can be handled with the appliance of the issuing of electronic certificate that stated the certainty status of the involving parties without excluding the presence of good faith principle in making agreements between parties. All the requirements for valid agreements finally strict to be bound as implemented in article 1338 Indonesian Civil Code stipulates that all agreements that are made legally shall apply as the law between the parties and shall not revocable except with the consent of both parties. Most of all, the presence of open system in Indonesian Civil Code also make it possible for the appliance development of current paper based agreements to the model of electronic based agreements

Henceforth the validity of digital signature as evidence in electronic commerce, also strengthen by Law no 8/1997 on Company Documents, that has been pioneer of current legislation in Indonesia, where it gives legal recognition upon electronic based company agreements. By this recognition it also make possibility for the presence of electronic commerce and electronic documents as a type of non conventional agreement that can used in front the court, yet still the need for the print out version of the electronic documents for further actions.

On further legislation as regulated in article 11 Law 11/2008 on Information and Electronic Documents²⁶, views in giving legal recognition on the bounding power of electronic documents yet digital signature as evidence that seen also security guarantor of electronic contracts yet show

²⁶ Art 11 Law 11/2008 on Information and Electronic Transaction:

(1) Electronic signature shall have legal binding and legitimate legal effect in so far as it fulfills the following terms and conditions :

- a) the data about the making of electronic signature is related only to the signatory
- b) the data about the making of electronic signature as the time of electronic signing process is only in the authority of the signatory
- c) any and all changes to the electronic signature occurred after the time of signing can be acknowledge
- d) any and all changes to the electronic information related to the electronic signature after the time of signing can be acknowledge
- e) there is a certain method used to identify the signatory.

.....

the consent of will between parties in using it as a method to secure the electronic documents.

Therefore, on the basis that regulates article 1320 and article 1338 Indonesian Civil Code and article 11 Law 11/2008 on Information and Electronic Transaction, the existence of digital signature as evidence in electronic commerce is valid.

III. Digital Signature's Burden of Proof in Electronic Commerce

The existence of cyberspace area where the electronic transaction took place has brought difference other legal consequences than the real world. Though, every legal act that conducted in cyberspace brings the same consequences like in real world. Recognizing the security issue in electronic transaction by the development of information and technology, a new way of security system in electronic communication was introduced.

Security system defines as a system use in securing data and information connection network. The security system introduces the use of cryptography. In cryptography itself, there are 2 type of system, that are:

1. symmetric system or secret key cryptosystem based on single secret key that use by both parties that involved in communication links. In symmetric system, it is important to ensure that the exchange of used secret key must assured its confidentiality
2. Asymmetric cryptosystem or public key cryptosystem based on the use pair of key. In public key cryptosystem, the system work where the encrypted message with one key cannot decrypt if it not use its pair. The pairs of key are private key and public key, and digital signature is one example that use asymmetric cryptosystem²⁷

The chronology how digital signature work can describe in following example : A wants to send a message to B, so A encrypt the message with A private key, which allowed the message transform into message digest or hash function. When B want to open A's message, B just need B public key that will decrypt A message, but the first thing to do for B is comparing the value of hash point, so that when there's occur any changes, it will give warning to B that B message has opened by unauthorized party.

²⁷ Mariam D Badruzaman. *Kompilasi Hukum Perikatan* (2001). Citra Aditya Bakti. Bandung. 324.

Ironically the presence development of electronic contract yet digital signature has arise the digital divide problem that affect by certain factor, that are:

a. Technology constraint

The existence of security system usage through digital signatures depends on the ability of each country in adopting the technology used. What has been the main problem is the ability of one country that may lead to the confusion to other country that has not has the ability to adopt the technology

b. Cultural constraint

For some countries the mechanism of transferring the ownership of an object to other party not always seen as the single aspect in trading, yet the influence of social values also take part in trading. This condition has been the problem of doing electronic commerce that requires face-less trading instead of face to face trading.

c. Legal constraint

The difference between many countries in regulate the existence of code in conduct electronic commerce has been a challenge in enforcing this security system in wide scope, yet the requirements of some contract in some documents still require notary role in approving the document, yet including the absence of standard in digital signature and electronic documents usage.²⁸

Based on the existence of constraints above has show us, despite security guarantee that digital signature provided and the practicality of electronic contract still bring problems that need to solved, mostly when it comes to legal burden of proof. In law of evidence, evidence reliability hold an important role, especially where a dispute happen and need for further validity proving. Relating to this issue, there are some factors that need to be consider for the validity of proof, that are:

- a. accuracy, completeness and accessibility of data sources;
- b. reliability of the method used in entering data in computer;
- c. reliability of the way computer process data; and
- d. accuracy of the process in producing the necessary data from computer.²⁹

²⁸ Baumer & Poindexter. *Cyberlaw & E-Commerce* (2001). McGraw Hill New York. p 88.

²⁹ Alan McGunther. *Electronic Evidence* (1999) Carswell Canada.

On further explanation in analyzing the burden of proof of digital signature, there are few important points to be noted, that are jurisdiction method in the burden of proof, evidence method that develop nowadays and judge capacity in interpreting the burden of proof related with the regulation that regulates human resources in maintaining security system of electronic documents.

In its development, it is undeniable that the agreements in electronic contract has the same model with the standard contract that present in the real world, more over in the world of electronic commerce it involves transnational character that leads to the regulation that regulates the practice of electronic commerce, and this condition related to the jurisdiction factor of countries authorities in judging particular cases related to electronic commerce. There are 3 type of jurisdiction posses by countries, that are: jurisdiction to prescribe, where country has authority in making legal provisions without limitation to the power of another country, second is executive jurisdiction where country has limitation in applying its jurisdiction due to other country jurisdiction, third is enforcement jurisdiction, where country cannot enforce court verdict against those who committed crime within the jurisdiction of other country.³⁰

Moreover, related to the jurisdiction with the presence of international private law is unavoidable in forming legal rules in resolve transnational matter, which there are few principle that can use, first is objective territoriality principle, stated that the applicable law is the law that the main result of the action took place and resulted on adverse impact for the victim country, second is protective principle, stated that the applicable law based on state demand in protecting state interest from offences outward its territory, third is universality interest jurisdiction, stated that every country has the rights to arrest and punish piracy, humanity and even more information and technology offences³¹. In further explanation, there are few theories that applied as a guidelines in United States of America in regulating the jurisdiction of cyberspace, first is theory of the uploader and the downloader, stated that state can prohibit uploading and downloading activity in its territory that bring harm to the interest of the country, second is the theory of the law of the server that gave a legal recognition upon data server in webpage and this may lead to the recognition of electronic data as

30 Tien S. Saefullah. *Yurisdiksi sebagai Upaya Penegakan Hukum dalam Kegiatan Cyberspace dalam M.K.Kantaatmaja. Cyberlaw-Suatu Pengantar*. ELIPS. Bandung p. 97-98.

31 A.M. Ramli. *Cyberlaw dan HAKI dalam Sistem Hukum Indonesia (2004)*. PT. Refika Aditama. Bandung. p 20.

valid evidence in the court, third is the theory of international space, stated in the analogy of cyberspace with space activity and the expectation that cyberspace will be the fourth space in coherence with the regulation in international law, where there will be harmonization of law in regulates civil and commercial jurisdiction instead of any countries jurisdiction³².

Referring to the explanation above, in international practice relating of verification mechanism of digital signature in electronic commerce, there are two kinds of methods that can use, namely 1) Affidavit Evidence, is an evidentiary mechanism based on knowledge experience made by self-own party and has the competence from the party in proving the validity of the electronically signed document. The testimony of the involving party can proved for its truth on open court and sub cross examination can perform over it. 2) Electronic Testimony, is an evidentiary mechanism based on transcript certification of the electronic type agreement include also the presence of digital signature, where the certification of the electronic type document can be classified as *prima facie* evidence of evidentiary mechanism.³³

In coherence with the legal practice in Indonesia, regarding burden of proof of electronic document has not develop in more complex mechanism, though the presence of electronic documents and digital signature has regarded as legal evidence. Therefore, in fulfilling presence in certainty of justice resulted on particular method that bind to develop by judge in finding suitable law and known as *rechtvinding* (discovery of law), that has few major reason to follow to be develop, which are : the existing legal rules do not cover a legal event, the absence of physically existing legal role upon a legal event and the failure of existing legal rules in fulfilling sense of justice or public order.

More over relating the burden of proof authority with the above reason in *rechtvinding* (discovery of law) there are two type of interpretation method that can use. First, is analogical interpretation method, by giving such as proverb upon words that has accordance with legal principles, resulted to the possibility of existing regulation can applied upon certain event³⁴. In relating to the presence of digital signature, judge can use the interpretation of *Bewijs en Verjaring naar Het Nederlands Burgerlijk Wetboek*, which stated:

32 Abu Bakar Munir. *Cyberlaw : policies and challenges* (1999) Butterworth. UK. p 270.

33 Andrew Choo. *Evidence text and material* (1996). Longman. Harlow UK. p 75.

34 Yuyun Yuliana, *Pembuktian Tindak Pidana Cybercrime*. Diakses dari *hukumonline* 22 Januari 2009.

Letter as the bearer of signature, reading which mean interpreting content of mind, and what materials including it in the reading sign is not important.

And the interpretation of France Civil Code art 1316, stated that:

The meaning of evidence with letters or written evidence is the sequence of letters, signs, numbers or symbol that can understood, in whatever its media and transmission.

Second. is extensive interpretation method, by expanding the meaning of provisions as regulated in law and the expansion of meaning should completed with sociological interpretation in fulfilling society reality³⁵. The presence of judge presumption can applied in relating with digital signature requirements to be binding as valid evidence as stipulates in article 11 Law 11/2008 on Information and Electronic Transaction.³⁶

Meanwhile, while there are conflict of norm in the existing rules that used, judge can use 2 type of dispute settlement principle, which are:

a. Lex specialis derogate legi generalis

Noting that special legal rule expel common legal rule, which relates to the position of Indonesian Civil Code as common legal rule and Law No 11/2008 on Information and Electronic Transaction regarded as special legal rule in coherence with the development of social and information technology, the presence of electronic contract agreement and digital signature as new type of evidence. On legal basis of lex specialis derogate legi generalis, the presence of Law 11/2008 on Information and Electronic Transaction expel the appliances of Indonesian Civil Code relating to the presence of new type evidence.

b. Lex posteriori derogate lex priori

Noting that a new law will expel old law, which relates to the position of Indonesian Civil Code as old law and Law No 11/2008 on Information and Electronic Transaction regarded as a new law. In coherence with the presence of new type of evidence, it is clear that Law 11/2008 on Information and Electronic Transaction has regulates legal recognizing upon electronic document and digital signature and it will resulted in the expel

³⁵ Danan Mursito. Pendekatan Keamanan untuk Dunia Cyber. Diakses dari internet 22 Januari 2009.

³⁶ Refer to art 11 Law 11/2008 on Information and Electronic Transaction above.

of Indonesian Civil Code relating to the presence of conventional evidence by Law 11/2008 on Information and Electronic Transaction in assuring security transaction in electronic commerce. Therefore, the presence of Certification Authentication (CA) as independent third party that certified and authorized by government in its authority in auditing and issuing assurance certificate in electronic transaction is an important issue.

In comparison with the regulation in the Netherlands concerning the equality between electronic signatures and conventional signature as regulated in *richtlijnen elektronische handtekeningen* (1999) in ensuring identification and originality of the electronic signatures by providing trusted third party as an independent organization in storing electronic signature, ensuring data exchange with cryptography method.³⁷

In other Asian country, the presence of Certification Authorization also available in Singapore by Case Trust organization that provide assurance over consumer rights in conducting electronic commerce business, and help customer in assisting their rights for dispute settlement, also by providing penal and non penal punishment over seller failure in fulfilling their obligation to customer, yet vice versa.

Meanwhile concerning its practice in Indonesia, the presence of Certificate Authorization in Indonesia (CA) has been regulated in Law 11/2008 on Information and Electronic Transaction article 13, explaining that every person has the right to use electronic certification organizer services to make electronic signature, and the electronic certificate organizer open the possibility both for Indonesian and foreign electronic certification organizer that must domiciled in Indonesia or shall register in Indonesia, and on article 14 explaining that, the requirements that must provided by electronic certification organizer with accurate, clear and certain information to user covering the method being applied to identify signatory, items that can use to know personal data of electronic signature make and item that may used to show the enforceable condition and security of the electronic signature. Though the regulation concerning Certificate Authorization seems to be clear, however there are not further regulation on evidentiary method in electronic commerce yet further regulation in Certificate Authorization (CA).

³⁷ Herlien Budiono. *Kumpulan Tulisan Hukum Perdata di Bidang Kenotariatan* (2007). Citra Aditya Bakti. Bandung. p 221.

Not to be missed, judge capacity and authority in conducting dispute settlement relating to electronic commerce matter are methods of determinants approach in international civil law that need to be consider, that are:

a. Choice of Law Approach

Basically is the basic policies that has to be enforced by countries contract law aiming in :a) protect legitimate expectation of the parties, b) ensuring stability and continuity of transnational contract, c) predictability in international civil law decision that has great importance in transnational contract, as such there are freedom of contract in implementing choice of law between them. In implementing choice of law approach in transnational trade contract, this approach assumes that despite the freedom of contract implement by the parties, there are still few limitation in conducting freedom of contract principle, which are: a) bona fide, legitimate yet not violating public order, b) the restriction toward a legal system that does not has any relevance to the contract, c) the restriction of meaningless choice of law, d) the restriction toward contract that has been made by the parties, d) the restriction toward forcible forum of law that has relevance to the contract³⁸.

Yet, when the parties can not strictly determine choice of law to applied, there are few points to be noted : a) considering the choice of forum as agreed in contract, b) considering few factors as agreed in contract that concluding parties will, c) considering the nearest legal system with the related factors as agreed in contract³⁹

b. Traditional approach

Basically lies in the principle, that the existence of simple yet practical rules of international private law will encourage the emergence of decision uniformity, improve the predictability of dispute settlement.

In determining method of determinant, traditional approach requires four main steps : a) implement basic qualification and involving related problem in the categorized problem of judges b) determine rules of international civil law c) determine legal rules that applied in accordance with rules of international civil law d) find rule of internal law in *Lex Causae*

38 Roslina. Pengaruh Kontrak Baku Online terhadap Hubungan Hukum dan Tanggung Jawan Pelaku Usaha Online kepada konsumen E-Commerce. Thesis. Program Pasca Sarjana Universitas Parahyangan, Bandung.

39 Sukarmi. Kontrak Elektronik dalam Bayang-Bayang Pelaku Usaha (2008). Pustaka Sutra. Bandung. p 145- 146.

and decide the related case base on *Lex Causae* internal law rules based on the traditional approach, state selected law considered as the only country that has legal jurisdiction to determine the existence of right that define the case and law from the country that must imposed on all substantial issues in a problem⁴⁰.

In implementing traditional approach in transnational trade contract includes electronic commerce, this approach assumes that all international private law issue related to the validity of contract shall be governed by the legal rules where the contract took place, this condition is in coherence with its doctrine known as *The Last Act Test* determine that the place where the contract begin and ends it final act resulted on the bound of the parties.

III. Concluding Remarks

The existence of globalization resulted by the rapid development in information technology has brought nations in possessing all technology mostly that has bring great benefit to their economy aspect. The presence of digital signature with its high-quality security system yet it legal status as valid evidence in electronic commerce, and related its burden of proof need equal combination between legislators in legislate regulation, international practice of international civil law and judge competency in conducted dispute settlement related to the electronic commerce burden of proof. Last but not least, the urgency in legislate further regulation in digital signature evidentiary method, conduction of society socialization related to the guidelines of electronic commerce practice and mostly ensuring the implementation of good faith principle among all kinds of contracts.

40 Sukarni. *Ibid.* p 145-146.