Nowadays, the development of science and technology, which can be attributed to the intelligence and creative thinking of human beings, has greatly facilitate the interaction in trade area, and electronic signature is a case in point. The existence of electronic commerce that combines technology and trade practice has emerged faceless trading. Ironically the emergence of cyber crime also develops rapidly. The existence of digital signature that reflects the practice of cryptography system still brings problems related to its validity as evidence especially in Indonesia’s evidence law perspective. The aims of this paper are to analyze the presence of digital signature in electronic commerce and the burden of proof that applied over digital signature from Indonesia’s evidence law perspective. The methods used in this paper are conceptual and case approach. The result in this paper show that: (1) the legal position of digital signature in Indonesia’s evidence law may recognized as a new type of evidence as regulate in Law No.11 of 2008 on Information and Electronic Transaction and the nature of electronic commerce that in accordance with article 1320 Indonesia’s civil code; (2) judge in applying digital signature burden of proof may use affidavit evidence and electronic testimony methods based on the practice of international space theory and the absence between parties in contract theory.

INTRODUCTION

In its essential way, globalization as a process of social transformation has brought the condition of humans’ life in different countries and regions into one borderless condition. The development of information age has brought significant and extensive use of global communication networks. Existence of interconnected network as a result of information technology...
development with its distinct facility and program, makes the possibility of global society network interact with each other in borderless area\(^2\), meanwhile in trading area with the help of internet, it boosts individual to conduct acculturation process and trans-border trading area\(^3\). The invention of interconnected network (internet) brings seamless merging of data, information and entertainment and has opened up new vistas for businesses\(^4\). The development of information technology has brought a great impact that changes the conduction of trade from face-to-face into faceless trading with the help of interconnected network as known as electronic commerce\(^5\). Electronic commerce defines trading system that conducts with the assistance of electronic transmission, furthermore it also conducts as all kinds of trading system and trade of goods and services with internet media\(^6\).

The happening of electronic commerce exists due to vast development of information technology, supported with high society demand that asks for fast, efficient service and with the existence of this electronic commerce resulted on the vast yet broad society scope in choosing product and services with many quality and quantity as the society ask. In further result, the happening of electronic commerce brings customer to have ability to gather product information, as they need in borderless area\(^7\). Electronic commerce has been considered to represent a broad range of technologies, processes and practices which automate the transacting of business through largely paperless mechanisms, involve 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 communities\(^8\).

The happening of investigation conduct in conventional trade service, related with the practice of evidence law is a simple issue, as it helps with the presence of physical proof of evidence, but it will not be the same for the sale and purchase transaction in paperless trading that requires a more complicated way about the burden of proof, however as time changes yet following with the vast growth of information technology, leak of crimes

\(^3\) Rieke, Ustadiyanto. *Ibid*. hlm 139.
\(^6\) Rieke, Ustadiyanto. *Op Cit*. hlm 139.
develops in a vast way specially with the existence of cyber crime. Cyber crime considers as a new dimension of crime, tingling international society attention with its distinct character that conducts with the help of internet media. In its general definition, cyber crime defines as “an effort to enter and or to use computer facility or computer network without permission within breach the law with or without change and or damage to the related computer facility”9. The United States Department of Justice also defines computer crime as “… any illegal act requiring knowledge of computer technology for its perpetration, investigation, or prosecution”10. Another definition of cyber crime is defined by Organization of European Community Development as “any illegal, unethical or unauthorized behavior relating to the automatic processing and/or the transmission of data”11.

Cyber crime that regards as the black side of technology development has a vast negative effect on this modern era. This problem also expressed in Cyber Crime article as delivered by ITAC (Information Technology Association of Canada) at International Information Industry Congress (IIIC) 2000 Millennium Congress that conducted in Quebec on September 19, 2000 stated that:

... Cyber crime is a real and growing threat to economic and social development around the world. Information technology touches every aspect of human life and so can electronically crime12.

In handling the issue of cyber crime and its vast growth, the electronic commerce system must offer at least the same level of reliability as that obtains in the paper world. It is well known that frauds do take place in the traditional paper based on transactions, signatures can be forged, paper documents can be tampered with, while on the electronic commerce world since they are directly the outcome of creating documents electronically, transmittance over worldwide computer communication network need the convincement that such documents are authentic when received over networks, and their authentication can be established in case of dispute13.

Various problems that arise from security leakage upon transaction that

10 http:// www.gipi.or.Id.
conducts in internet may minimize with the existence of cryptography\textsuperscript{14}. Cryptography derives from Greek words “krypto and logos” meaning as hidden world, considered as subject of science that learns application techniques whose existence depend on the existence of complicated issue\textsuperscript{15}, specifically in electronic contract the most well known cryptography application is digital signature\textsuperscript{16}. Digital signature itself is an amount of mathematic operation derived from cryptography and resulted from a computer in an electronic document\textsuperscript{17}. From the legal perspective, digital signature is a security system in a digital data made with private signature key which existence depends on public key that become its linkage, yet the existence of digital signature shows with the establishment of signature key certificate from a certifier\textsuperscript{18}. From the technical perspective, digital signature is a numeric point in coherence with data with a series of mathematical procedure that is privately known by the owner of cryptography key\textsuperscript{19}.

Related with the grant of security guarantee, digital signature functions to guarantee all electronic messages that exist has been sent correctly to the objective receiver, yet it may recognize as a strong proof of evidence from the legal aspect that the message has been sent and agreed with its receiver\textsuperscript{20}.

The invention of digital signature as a part of asymmetric cryptography system that requires processing series and must be passed by receiver before validating message senders deems to be able to provide security guarantees for the existing electronic commerce transaction\textsuperscript{21}, and in such a way it makes electronic commerce at least as secure and legally binding as traditional commercial transaction. Ironically from the perspective of Indonesia’s evidence law, digital signature position has not had its strong position as other evidence objects and may be questionable in contract that was conducted in electronic world. The aims of this paper are shown as: Part I summarizes the impact of globalization toward the practice of electronic commerce and what problems may happen related with the law of evidence based on Indonesia’s evidence law perspective; Part II explains the

\textsuperscript{16} M. S. Tuharea, Kajian Kerangka Hukum Digital Signature, ITB. Bandung. hlm 2, 2003.
\textsuperscript{17} B. Schneier, Applied Cryptography, John Wiley & Sons Inc, USA. hlm 22, 1994.
\textsuperscript{18} German Draft Digital Signature Law, Reporter’s Draft, Version of September 19, 1996.
\textsuperscript{19} D. Budhijanto, Op.Cit, hlm 68.
presence of digital signature in electronic commerce in Indonesia’s evidence law and digital signature’s burden of proof in Indonesia’s evidence law; Part III concludes the result of research and submits further notices for the future development of electronic commerce especially in the practice and perspective of Indonesia’s evidence law study.

I. LEGAL POSITION OF DIGITAL SIGNATURE IN INDONESIA’S EVIDENCE LAW

In its development, it realizes that globalization and global trade that were supported by the development of information technology has widen the scope of goods and services transaction flow in trans-border area, yet the development of information and technology also affect business development. With the existence of electronic commerce transaction, the relation between seller and buyer depends on the agreement and this agreement considered as a type of standard contract, and in coherence with common contract, electronic transaction bind the parties as it is in coherence with the freedom of contract principle, apart from the fulfillment of subjective and objective requirement, another issue that cannot be missed is the existence of signature itself. Signature defines as written composition from signer, which the person may individualize in his/her statement. In the study of signatures, in a conventional contract, it shows with the affixing of the signature of an agreement. It will indicate the presence of identified parties involved, as well as it will provide opportunities for other parties to verify the agreement when needed. Additionally, with the presence of a signature statement it will show the will of the parties to agree upon the agreement that has been made.

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. In its evidence law as stipulated in article 1866 Indonesian Civil Code, there are four types of evidence, namely: Written evidence, presumptions, confession and oath.

However, in its progressive development, the role of new evidence (considered as non-conventional evidence) related to the development of technology cannot be waived, to make sure that facts proposed to the court clearer and more understandable by its real impression of the legal facts.

From the legal perspective, there are few requirements that need to
fulfill by demonstrative evidence for its legally binding as evidence, that are 25:
- The existence of object as evidence;
- Representative accuracy, meaning that the equalization of size, shape and its dimension in avoiding confusion in evidence proofing as needed;
- Authentication, meaning that the demonstrated evidence should describe and represent the actual evidence;
- Identification, meaning that the demonstrated evidence should match exactly with the actual evidence;
- Admissibility, meaning that the demonstrated evidence must be able to prove something relevant, significant and competent;
- Equality, meaning that the demonstrated evidence should clarify the proven fact.

While in the case of the electronic contract, the type of signature used is an electronic signature. Electronic signature is part of signature that has the same function with the signature in its traditional form, which uses the transformation of electronic data messages or electronic documents with cryptographic system that managed by the agency issuing the certificate validation of electronic signatures 26. In relation with its context, electronic signatures this issue is not the same as the context of such signature or electronic form like the general of a written signature on paper. Electronic signatures are simple in this case obtained by making a message digest of a summary of the mathematical language in documents sent through the realm of cyberspace 27.

Meanwhile, the presence of electronic signature in its function term does not have big difference in conventional signature, whereas by its function in transforming electronic data message or electronic document using cryptography system obtained from certificate authorization; it will provide important function likewise 28:
- Minimize the risk for the actions of any parties who attempts to breach the agreement and forge documents;
- Provide high level security for information transmission over open networks and reliability of data integrity;

---

26 Arrelanno University School of Law Journal.
• Provide convenience for non paper agreement transaction;
• In relation to the nature of digital signature itself, it has distinct characteristics that may support his position as new types of evidence, that are\textsuperscript{29}:
  • Authenticity means when digital signature should possible to verify whether the data message 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 is request to Certificate Authority;
  • Integrity means the presence of data sending also providing assurance that the submitted data will never be modified or changed during the sending and saving by unauthorized party;
  • Non-repudiability means in the appliance of digital signature, sender cannot deny that he/she has sent the messages yet deny the content of the messages when it come to content differences;
  • Confidentiality means that digital signature may protect data from unauthorized internal users, intercepted during transmission.

In the international regulation relates to the practice of electronic commerce, the establishment of UNCITRAL 1996 Model Law on Electronic Commerce has provided legal recognition of data message transmitted via electronic or other form, yet in attempt to find technical solutions to meet the requirements of existed law and provide recognition of existing data messages\textsuperscript{30}.

In further explanation about the validity of digital signature in Indonesia’s evidence law, It may be analyzed from article 1320 Indonesian Civil Code that defines the qualifications of valid article: the presence of consent of those who bind themselves, the capability to make an agreement, the presence of particular object and lawful cause (good faith principle). Whereas by these requirements, the presence of consent by the offer and acceptance to be bound in electronic contract also includes 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. All the requirements for valid agreements finally strict to be bound as implemented in article 1338 Indonesian Civil Code ,which stipulates that all agreements made legally shall apply as the law between the parties and shall not be revocable except with the consent of both parties. Henceforth on further legislation as regulated in article 11 Law 11/2008 on

\textsuperscript{29} Kamlesh K. Bajaj & Debjani Nag. Op Cit. at 198-199.
\textsuperscript{30} INDIRA CORR, INTERNATIONAL TRADE LAW, at 111 (United Kingdom: Cavendish Publishing, 2005).
Information and Electronic Documents, it provides legal recognition on the
bounding power of electronic documents and digital signature as evidence
that is seen as security guarantor of electronic contracts which shows the
consent of will between parties in using it as a method to secure the
electronic documents.

II. THE BURDEN OF PROOF OF DIGITAL SIGNATURE

The existence of cyberspace area where the electronic transaction
took place has brought other different legal consequences compared with
the real world. Though, every legal act conducted in cyberspace brings the
same consequences like in real world. In the evidence law, proof of
evidence reliability holds an important role especially for dispute
settlement in electronic evidence world\(^{31}\). On the Following figures show
the work flow of digital signature in asymmetric cryptosystem and the
comparison result of authentic decrypt data messages between sender and
receiver that show the originality and authenticity of the data that have
been sent between parties.

Figure 1 shows the flow work of digital signature as the type of
asymmetric cryptosystem that requires the use of private key and public key
to encrypt and decrypt the data messages, meanwhile Figure 2 shows the
comparison result of the decrypt data messages by using public key and
comparing the hash key function for its data messages authenticity\(^{32}\).

![Figure 1 The Work Flow of Digital Signature](image)


\(^{32}\) MARIAM D BADRULZAMAN, KOMPILASI HUKUM PERIKATAN, at 324 (Bandung: Citra Aditya Bakti. 2001).
On further explanation in analyzing the burden of proof of digital signature, there are two kinds of methods that can be used 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 and (2) Electronic testimony is an evidentiary mechanism based on transcript certification of the electronic type agreement which also includes the presence of digital signature, where the certification of the electronic type document can be classified as prima facie evidence of evidentiary mechanism\textsuperscript{33}. In coherence to strengthen the burden of proof of digital signature, the appliance of offer and acceptance theory in contract that explain the presence of one’s offer and other’s acceptance create new consent of will, due to the nature of electronic commerce as a contract shall be used, not to be missed, the use of absence between party that combines with international space theory that regard cyberspace as field of law in coherence with the regulation in international law, where there will be harmonization of law of \textit{lex electronica} in regulates civil and commercial jurisdiction instead of any countries jurisdiction\textsuperscript{34}, and regard the absence between party, physically in sending and receiving data messages in the practice of electronic commerce with the appliance of digital problem, is no more an obstacle for the validity of the electronic contract itself.

Dealing with the legal assessment of digital signature burden of proof, we cannot separate the role of computer technology itself, supported with human resources role in operating technology and the importance of morality, where morality holds an important role while technology, human

\textsuperscript{33} ANDREW CHOO, EVIDENCE TEXT AND MATERIAL, at 75 (Harlow, United Kingdom: Longman, 1996).
\textsuperscript{34} ABU BAKAR MUNIR, CYBERLAW: POLICIES AND CHALLENGES, at 270 (United Kingdom: Butterworth, 1999).
resources and legal regulation has covered the contentment of digital signature burden of proof in electronic commerce. In a further explanation, Mochtar Kusumaatmadja also said,

The existence of the law is not only as a corridor, but it also includes the role of institutions and legal institutions, which required bringing the law in reality. In Indonesia, where the laws hold the main role in community, the renewal process can conduct with updating the laws\textsuperscript{35}.

In giving further analysis in Mochtar Kusumaatmadja statement related with analyzing digital signature burden of proof, correlated institution and related legal regulation also hold an important role, what means by correlated institution are the parties who own private key and public key involved in the establishment of digital signature to authorize related data, also with the presence of certificate authorization agency as an independent agency, It bridges the legal problem issues in conduct electronic commerce and established secure key regard as digital signature in support electronic commerce practice

CONCLUSION

The existence of globalization resulted by the rapid development in information technology has brought nations in possessing all technology mostly that has brought great benefit to their economy. The presence of digital signature with its high-quality security system yet its 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, It is urgent to legislate further regulation in digital signature evidentiary method, conduct the society socialization related to the guidelines of electronic commerce practice and mostly to ensure the implementation of good faith principle among all kinds of contracts.