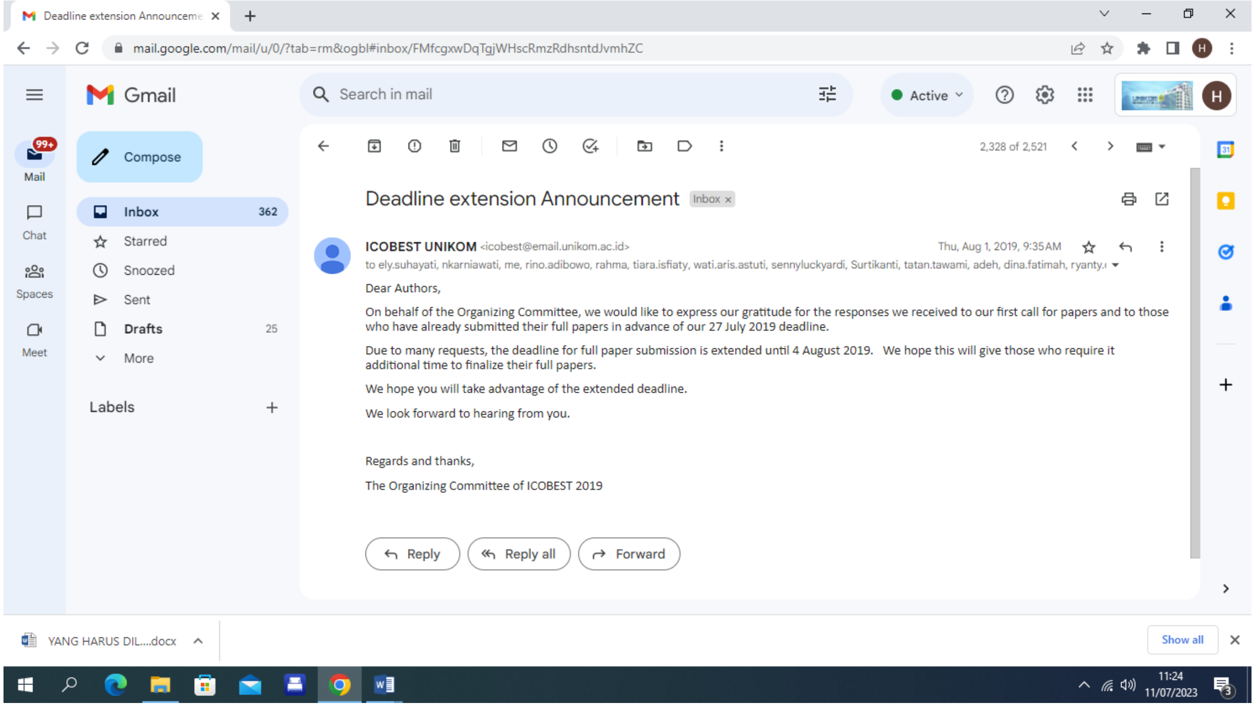
ICOBEST 2019



Deadline extension Announcement Inbox

ICOBEST UNIKOM <icobest@email.unikom.ac.id> Thu, Aug 1, 2019, 9:35 AM

to ely.suhayati, nkarniawati, me, rino.adibowo, rahma, tiara.isfiaty, wati.aris.astuti, sennyluckyardi, Surtikanti, tatan.tawami, adeh, dina.fatimah, ryanty.

Dear Authors,

On behalf of the Organizing Committee, we would like to express our gratitude for the responses we received to our first call for papers and to those who have already submitted their full papers in advance of our 27 July 2019 deadline.

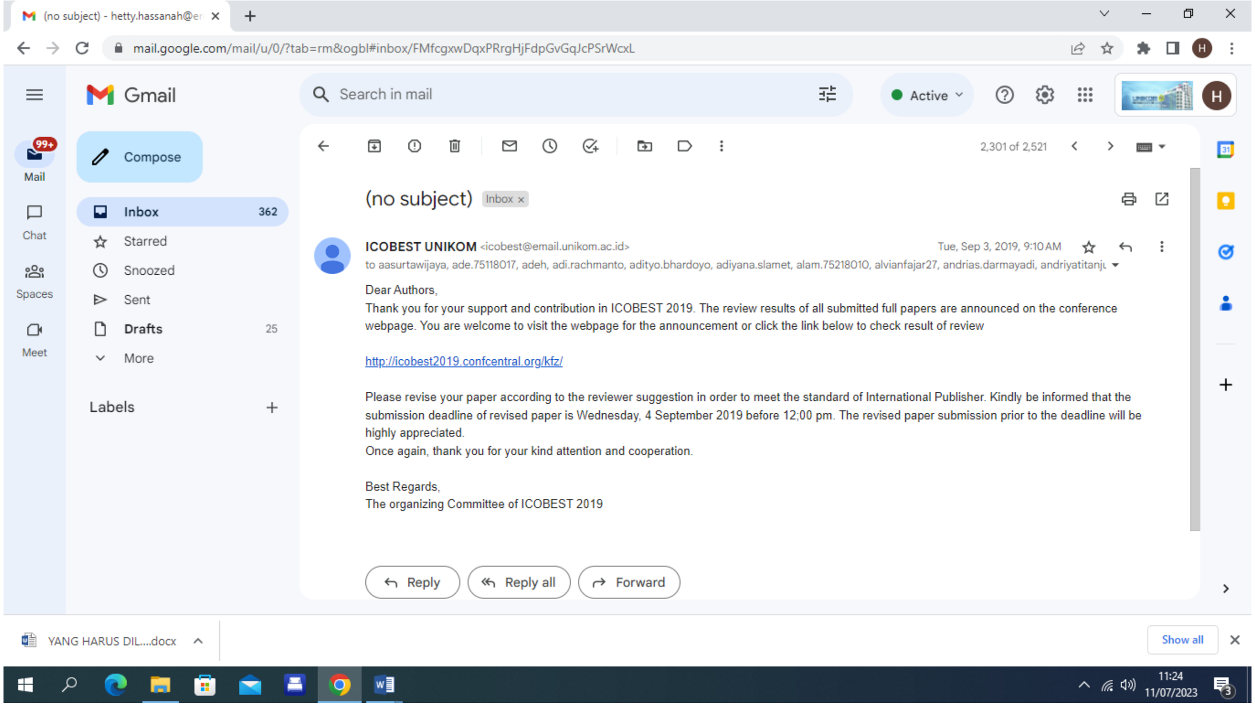
Due to many requests, the deadline for full paper submission is extended until 4 August 2019. We hope this will give those who require it additional time to finalize their full papers.

We hope you will take advantage of the extended deadline.

We look forward to hearing from you.

Regards and thanks,

The Organizing Committee of ICOBEST 2019



(no subject) Inbox

ICOBEST UNIKOM <icobest@email.unikom.ac.id> Tue, Sep 3, 2019, 9:10 AM

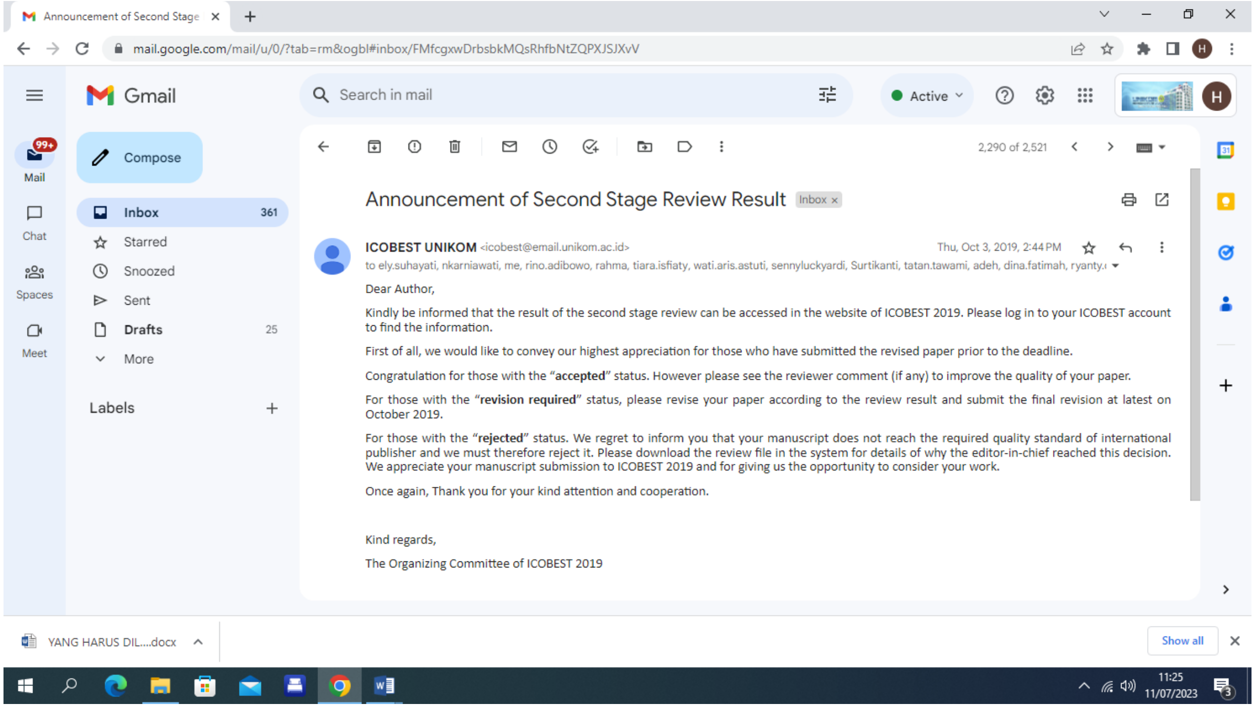
to aasurtawijaya, ade.75118017, adeh, adi.rachmanto, adityo.bhardoyo, adiyana.slamet, alam.75218010, alvianfajar27, andrias.darmayadi, andriyatitanju

Dear Authors,
Thank you for your support and contribution in ICOBEST 2019. The review results of all submitted full papers are announced on the conference webpage. You are welcome to visit the webpage for the announcement or click the link below to check result of review

http://icobest2019.confcentral.org/kfz/

Please revise your paper according to the reviewer suggestion in order to meet the standard of International Publisher. Kindly be informed that the submission deadline of revised paper is Wednesday, 4 September 2019 before 12:00 pm. The revised paper submission prior to the deadline will be highly appreciated.
Once again, thank you for your kind attention and cooperation.

Best Regards,
The organizing Committee of ICOBEST 2019



Announcement of Second Stage Review Result Inbox ×

ICOBEST UNIKOM <icobest@email.unikom.ac.id> Thu, Oct 3, 2019, 2:44 PM

to ely.suhayati, nkarniawati, me, rino.adibowo, rahma, tiara.isfiaty, wati.aris.astuti, sennyluckyardi, Surtikanti, tatan.tawami, adeh, dina.fatimah, ryanty.

Dear Author,

Kindly be informed that the result of the second stage review can be accessed in the website of ICOBEST 2019. Please log in to your ICOBEST account to find the information.

First of all, we would like to convey our highest appreciation for those who have submitted the revised paper prior to the deadline.

Congratulation for those with the "**accepted**" status. However please see the reviewer comment (if any) to improve the quality of your paper.

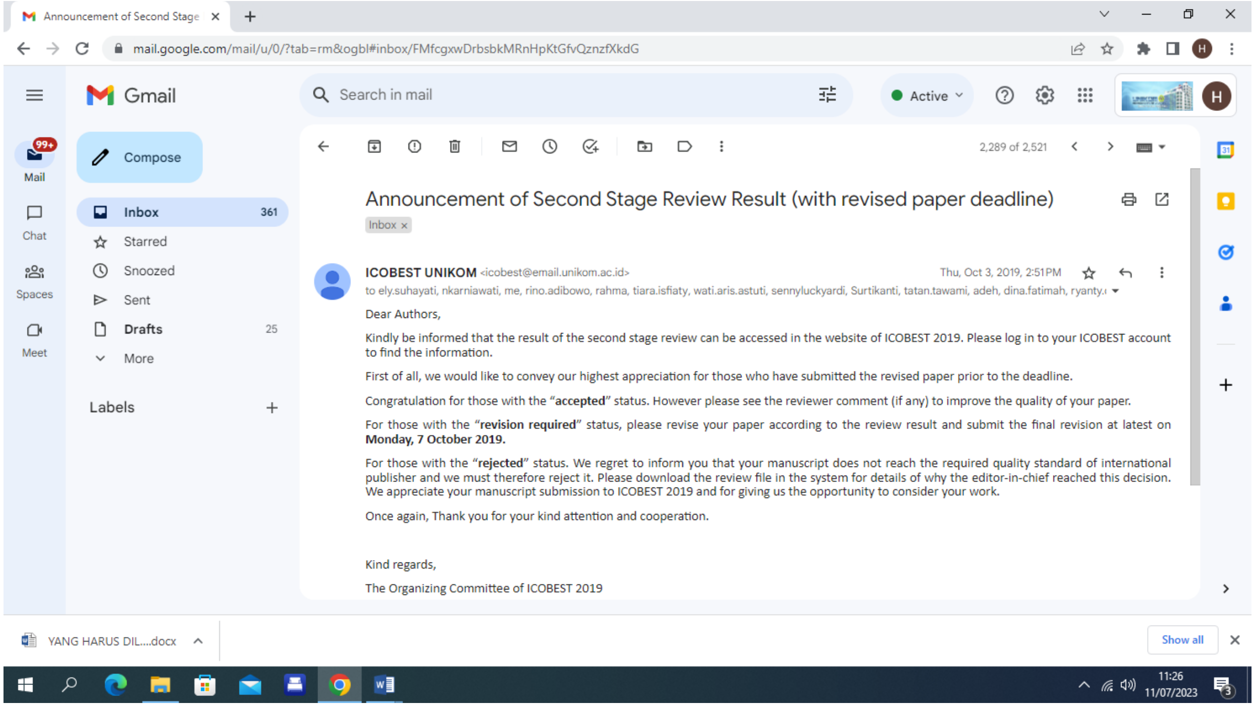
For those with the "**revision required**" status, please revise your paper according to the review result and submit the final revision at latest on October 2019.

For those with the "**rejected**" status. We regret to inform you that your manuscript does not reach the required quality standard of international publisher and we must therefore reject it. Please download the review file in the system for details of why the editor-in-chief reached this decision. We appreciate your manuscript submission to ICOBEST 2019 and for giving us the opportunity to consider your work.

Once again, Thank you for your kind attention and cooperation.

Kind regards,

The Organizing Committee of ICOBEST 2019



Announcement of Second Stage Review Result (with revised paper deadline) Inbox ×

ICOBEST UNIKOM <icobest@email.unikom.ac.id> Thu, Oct 3, 2019, 2:51 PM

to ely.suhayati, nkarniawati, me, rino.adibowo, rahma, tiara.isfiaty, wati.aris.astuti, sennyluckyardi, Surtikanti, tatan.tawami, adeh, dina.fatimah, ryanty.

Dear Authors,

Kindly be informed that the result of the second stage review can be accessed in the website of ICOBEST 2019. Please log in to your ICOBEST account to find the information.

First of all, we would like to convey our highest appreciation for those who have submitted the revised paper prior to the deadline.

Congratulation for those with the "**accepted**" status. However please see the reviewer comment (if any) to improve the quality of your paper.

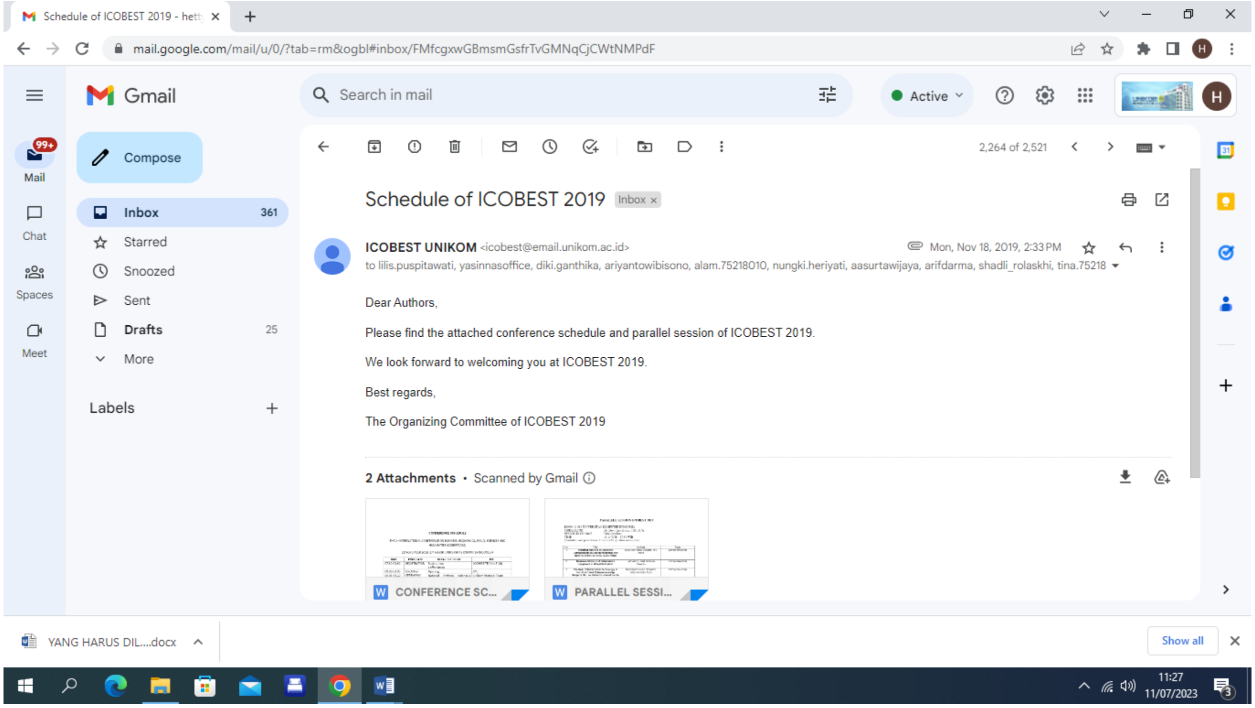
For those with the "**revision required**" status, please revise your paper according to the review result and submit the final revision at latest on **Monday, 7 October 2019.**

For those with the "**rejected**" status. We regret to inform you that your manuscript does not reach the required quality standard of international publisher and we must therefore reject it. Please download the review file in the system for details of why the editor-in-chief reached this decision. We appreciate your manuscript submission to ICOBEST 2019 and for giving us the opportunity to consider your work.

Once again, Thank you for your kind attention and cooperation.

Kind regards,

The Organizing Committee of ICOBEST 2019



Schedule of ICOBEST 2019 Inbox ×

ICOBEST UNIKOM <icobest@email.unikom.ac.id> Mon, Nov 18, 2019, 2:33 PM
to lilis.puspitawati, yasinnasoffice, diki.ganthika, ariyantowibisono, alam.75218010, nungki.heriyati, aasurtawijaya, arifdarma, shadli_rolaskhi, tina.75218

Dear Authors,

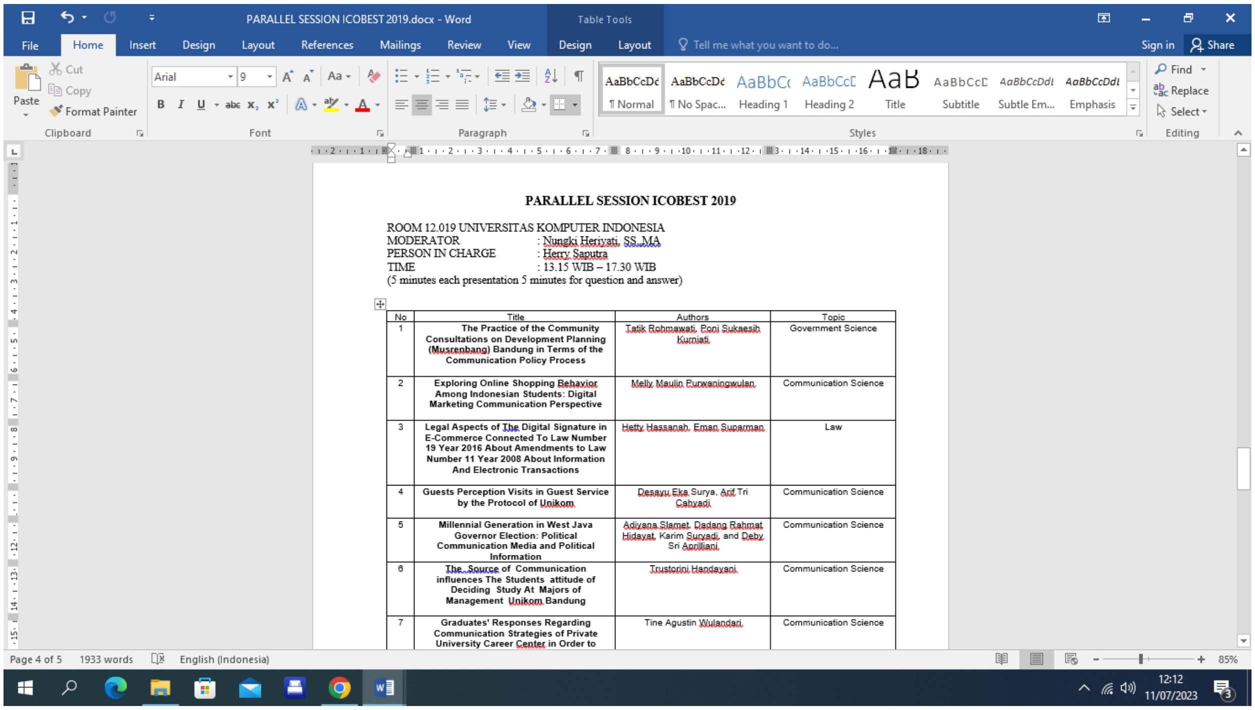
Please find the attached conference schedule and parallel session of ICOBEST 2019.

We look forward to welcoming you at ICOBEST 2019.

Best regards,

The Organizing Committee of ICOBEST 2019

2 Attachments • Scanned by Gmail



PARALLEL SESSION ICOBEST 2019

ROOM 12.019 UNIVERSITAS KOMPUTER INDONESIA
MODERATOR : Nungki Heriyati, SS.,MA
PERSON IN CHARGE : Herry Saputra
TIME : 13.15 WIB – 17.30 WIB
(5 minutes each presentation 5 minutes for question and answer)

No	Title	Authors	Topic
1	**The Practice of the Community Consultations on Development Planning (Musrenbang) Bandung in Terms of the Communication Policy Process**	Tatik Rohmawati, Poni Sukaesih Kurniati	Government Science
2	**Exploring Online Shopping Behavior Among Indonesian Students: Digital Marketing Communication Perspective**	Melly Maulin Purwaningwulan	Communication Science
3	**Legal Aspects of The Digital Signature in E-Commerce Connected To Law Number 19 Year 2016 About Amendments to Law Number 11 Year 2008 About Information And Electronic Transactions**	Hetty Hassanah, Eman Suparman	Law
4	**Guests Perception Visits in Guest Service by the Protocol of Unikom**	Desayu Eka Surya, Arif Tri Cahyadi	Communication Science
5	**Millennial Generation in West Java Governor Election: Political Communication Media and Political Information**	Adiyana Slamet, Dadang Rahmat Hidayat, Karim Suryadi, and Deby Sri Aprilliani	Communication Science
6	**The Source of Communication influences The Students attitude of Deciding Study At Majors of Management Unikom Bandung**	Trustorini Handayani	Communication Science
7	**Graduates' Responses Regarding Communication Strategies of Private University Career Center in Order to**	Tine Agustin Wulandari	Communication Science

Legal Aspects of The Digital Signature in E-Commerce Connected To Undang-Undang Number 19/2016 About Amendments to Undang-Undang Number 11/2008 About Information And Electronic Transactions

[1]Hetty Hassanah and [2]Eman Suparman
[1]hetty.hassanah@email.unikom.ac.id
[2]eman@unpad.ac.id
Faculty of Law, Universitas Komputer Indonesia, Bandung, Indonesia

Abstract

In this globalization era, research on digital signatures was conducted to find out the legal aspects relating to authentication in e-commerce. Previous studies have been conducted on e commerce and legal aspects of electronic systems, so that they can support the discussion of e-commerce authentication through this electronic system. Based on previous research, it is known that in e-commerce digital signatures are needed as a verification tool in these electronic transactions. The presence of digital signatures shows that there has been an agreement in a transaction (e commerce). This is evident from the practice that an electronic transaction can occur if an agreement has been signed with a digital signature from the parties. However, violations of laws relating to digital signatures such as occasional forgery occur, which ultimately harm the other party. Previous research has produced information about electronic transactions (e-commerce) and currently research is conducted in order to obtain legal aspects related to the digital signature in e-commerce so that it can be useful for the information society (information society).

Key words : E-commerce, Digital Signature, Legal aspect

I. INTRODUCTION

In e-commerce there is a digital signature, which is not like a signature that has been known so far, that is by using different methods to mark a document so that the document or data not only identifies the sender, but also to ensure the integrity of the document so as not to change during the transmission process.

There have been some previous researches, among others, the validity of digital signatures in e commerce agreements, by Rehulina[1], the study only discussed one aspect is the validity of digital signatures in the agreement, without elaborating on other legal aspects related to digital signatures in e-commerce. according to his opinion, the digital signature must be accepted as a signature with the following reasons: A digital signature is a signature that can be affixed by someone or some person who is authorized by someone else who wishes to be legally bound; using mechanical equipment, such as traditional / conventional signatures; A digital signature is very likely to be safer or more insecure as it is possible this also occurs in traditional / conventional signatures; as in traditional / conventional signatures. In another study, about digital signature there is research about digital signature in e-commerce, but the results of this study only explain that Information technology is a sector which grows rapidly from

[1] *Rehulina, Keabsahan Digital Signature Dalam Perjanjian E-Commerce, The Journal of Law, Volume 1, 2019, P. 45.*

year to year. The current development of technology has greatly affected human's life globally. Computer and internet have experienced rapid growth so people can access, communicate, and access anything without limit. The internet is the unifier of people around the world. Due to the advancement and development of information technology, many changes happen. One of them is the increased transactions, which are carried out through telecommunication media or the internet. In regards to this, digital signature system is developed. Digital signature under Article 1 paragraph (12) of the Electronic Information and Transaction Law is a signature consisting of electronic information attached, associated or related to other electronic information used as a means of verification and authentication[2]. Another study from Kalama M. Lui Kwan explained that digital signatures essentially allow parties to authenticate their document when communicating online. This is particularly useful for parties who want to know that their contract is enforceable, or for companies that want to be assured that customers with whom they are dealing inline thruthfully representing themselves[3]. The other opinion such as form Charles R. Merrill say that digital signature using cryptographic software and the signer of a digital signature will use the sender's private key to transform the message into a digital signature[4].Paul R. Katz and Aron Schwartz say that digital signature is a sequence of bits created when a person, intending to sign an electronic document, runs his or her message, through a one way function to create a unique identifier used for sender verification purpose[5]. The *current conditions have been new laws governing the internet and cyberspace, namely the promulgation of Undang-Undang Number 19/2016 About Amendments to Undang-Undang Number 11/2008 About Information And Electronic Transaction (Then written UU ITE) concerning Information and Electronic Transactions, but have not explicitly regulated criminal acts of digital signature forgery.*

My previous research related to digital signatures has analyzed the validity aspects in commerece. The research method used is the normative juridical approach and the resulting data is analyzed qualitatively juridically. One of the legal requirements of the agreement is the agreement of the parties or the conformity of the wishes of the parties which must be proven by the existence of a signature, thus in e commerce any agreement between the parties must be proven by the presence of digital signatures.

II. METHOD

The specification of the research is descriptive analytical, ie giving the facts systematically. Approach method to be used is normative juridical approach method, in this case test and review secondary data about legal aspect of digital signature on e commerce. All the data obtained are analyzed by qualitative juridical, in this case the analysis is done by considering the hierarchy of legislation so that the one legislation does not contradict other laws and legal certainty.

[2] Meina Diniari Basani, Perkembangan Tandatangan Elektronik di Indonesia, Jurnal Hukum UNPAD, Volume 1, 2017., P. 45.

[3]Kalama M. Lui Kwan, Recent Developments in Digital Signature Legislation Electronic Commerce, Barkeley Technology Law Journal, Vol 14 No. 1, Annual Review of Law and Technology, 1999, P. 463-481.

[4]Charles R. Merrill, Science & Technology Digital : Signature Guidline For Electronic Commerce, Best ABA Sections Journal, Solo & Smal Firm Section, Vol. 1, No. 2, 1997, P.50-51.

[5] Paul R. Katz & Aron Schwartz, Electronic Documents and Digital Signaturing : Changing The Way Business is Conducted and Contracts are Formed, Best of ABA Section Journal, Solo & Smal Firm Section, Vol. 1 No. 1, 1997, P. 36-37.

III. RESULT AND DISCUSSION

Digital signatures are not manual signatures scanned and affixed to documents or emails that we send. Digital signature is one of the uses of cryptographic methods that aims to detect unauthorized modification of data and to check identity authentication from the sender and non repudiation (refusing denial)[6]. The purpose of a digital signature in a document is to ensure the authenticity of the document. A digital signature is actually not a signature as it is known so far, digital signatures use different methods to mark a document so that digital signatures not only identify data from the sender, but digital signatures also ensure the integrity of the document, not changing during transmission process. A digital signature is based on the contents of the message itself[7].

Giving digital signatures to the electronic data sent will be able to show where the electronic data actually came from. Guaranteed integrity of the message can occur because of the existence of the Digital Certificate. Digital Certificate is obtained on the basis of application to Certification Authority by user / subscriber. Digital certificate contains information about users including:

1. *Identity*
2. *authority*
3. *legal standing*
4. *status of the user*

This digital certificate has various levels, the level of the digital certificate determines how much authority the user has. An example of this authority or qualification is if a company wants to do a legal act, then the party authorized to represent the company is the board of directors. So if a company wants to do a legal action, the Digital Certificate used is a digital certificate owned by the directors of the company.

The existence of this digital certificate, the third party associated with the digital certificate holder can feel confident that a message / message is true from that user. Integrity / integrity is related to the integrity of the data sent. A message recipient / data can be sure whether the message received is the same as the message sent. He can feel confident that the data has been modified or changed during the shipping or storage process.

The use of digital signatures that are applied to electronic messages / data sent can guarantee that these electronic messages / data do not experience a change or modification by an unauthorized party. This guarantee of authenticity can be seen from the hash function in a digital signature system, where data recipients can compare the hash value. If the hash value is the same and is appropriate, then the data is truly authentic, no action has ever taken place to modify the data during the shipping process, so the authenticity is guaranteed. Conversely, if the hash value is different, then it should be suspected and immediately it can be concluded that the recipient (recipient) receives data that has been modified.

[6] *Rahmat Sobari, Penggunaan Tanda Tangan Digital untuk Pengamanan Pertukaran Informasi, Tugas Akhir Proteksi dan Teknik Keamanan Sistem Informasi Bab IV: Cryptography, Program Magister Teknolgi Informasi Fakultas Teknik Komputer Universitas Indonesia 2005, Hlm. 15.*

[7] *Edmon Makarim, Kerangka Hukum digital Signature Dalam Electronic Commerce, Makalah Dipresentrasikan Di Hadapan Masyarakat Telekomunikasi Indonesia Pada Bulan Juni 1999 Di Pusat Ilmu Komputer Universitas Indonesia, Depok Jawa Barat.*

Non repudiation or cannot be denied the existence of a message related to the person who sent the message. The message sender cannot deny that he sent a message when he sent a message. He also cannot deny the contents of a message different from what he sent when he sent the message. Non repudiation is very important for e-commerce if a transaction is done through an internet network, electronic contracts (electronic contracts), or payment transactions[8]*. This non repudiation arises from the presence of digital signatures that use asymmetric encryption (asymmetric encryption). This asymmetric encryption involves the existence of the private key and public key. A message that has been encrypted using a private key can only be opened / description using the sender's public key. So if there is a message that has been encrypted by the sender using his private key, he cannot deny the existence of the message because it is proven that the message can be encrypted with the sender's public key. The integrity of the message can be seen from the existence of the hash function of the message, noting that the signature data will be entered into the digital envelope. The messages in the form of electronic data sent are confidential / confidential, so not everyone can find out the contents of electronic data that has been signed and entered in the digital envelope. The existence of a digital envelope that includes an integral part of a digital signature causes an encrypted message to be opened only by the rightful person. The level of confidentiality of a message that has been encrypted depends on the length of the key / key used to encrypt. At this time the standard key length used was 128 bites. Safeguarding data in e-commerce with cryptographic methods through the digital signature scheme is technically acceptable and applied, but if discussed from the point of view of law, it still lacks attention. The lack of attention from legal science is understandable because especially in Indonesia, the use of computers as a means of communication through the internet has only been known since 1994. Thus, safeguarding internet networks with digital signature methods in Indonesia is certainly still new to computer users.*

Some properties that exist in digital signatures, namely[9]*:*

1. *It is authentic, a message containing a digital signature can also be evidence, so that the party making the ratification (who signed) cannot deny that he never signed it.*
2. *It is exclusive, only valid for the document (message) or the exact copy. The signature cannot be transferred to another document. This also means that if the document is changed, the digital signature of the message is no longer valid.*
3. *It is global verification, checks can be done easily, even by people who are not related or have never met with the party who did the ratification (who signed) though.*

UU ITE stipulates that electronic signatures have legal force and legal consequences as long as they comply with the provisions of this law, meaning that as long as it can be ascertained the relationship between the electronic signature and the signatory concerned and the electronic signature is made and stored in conditions guarantee integrity with the deed attached to it, then an

[8] *Ilja Ponka, Legal Aspects of Digital Signatures and Non Repudiation, The Journal of Information Law and Technology, Vol. 2, 1999, P.5.*

[9] *Julius Indra Dwipayono Singara***,** *Pengakuan Tanda Tangan Elektronik Dalam Hukum Pembuktian Indonesia, sumber data dari situs www.legalitas.org pada tanggal 1 Juni 2019.*

electronic signature has the same legal value as an ordinary signature.

The rise of cases of electronic crime (cyber crime) has become one of the backgrounds for the use of digital signatures. Now, the Ministry of Communication and Information is actively implementing digital signatures for online transactions. Hopefully, with this technology, the community can carry out various online activities.

In addition to reducing the case of cyber crime, digital signatures also aim to facilitate business activities. The signature can be used to authorize documents. For example, you want to sign a business agreement with someone face to face. Digital signatures can be substituted for wet signatures. The Ministry of Communication and Information is collaborating with the Financial Services Authority to launch the program. Signature validation questions, submitted to Root CA (Certification Authority). This institution is tasked with determining the identity of the digital signature user and continuing the process[10]*.*

Electronic signatures are said to be valid if they meet certain requirements stipulated in the law. In the UU ITE , the legal requirements for digital signatures include the following. Manufacturing data is privacy and only known by the owner of the signature. When creating a signature, only the original owner has the power to use it. If there is a change after making an electronic signature, it can be known with certainty.

All changes to electronic information relating to signatures; can be known. Have a special way to know for sure the owner of his signature. Have a special way to prove that the signature owner has given legal approval regarding certain electronic information. Signing *a document has four main objectives, namely as evidence, a sign of agreement, fulfillment of formality, and efficiency. For this purpose to be achieved, there are two attributes of electronic signatures that must be met. Signature owner authentication. That is, the electronic signature is not easy to imitate and is able to show the owner's identity. Document authentication. This gives meaning, under an electronic signature must be able to characterize the authenticity of the signed document. Thus, the document is not easily faked or changed without being known by the author.*

In essence, the authentication of the signing and the document must be able to prevent someone from the case of cyber crime, such as forgery. Therefore, electronic signatures must adhere to the concept of nonrepudation. This is one form of guaranteeing the authenticity of the file to prevent denial from the owner of the signature.

In verification of digital signatures, the hash function needs to be considered. Hash is an algorithm used to make a fingerprint type. One hash can usually only be used in one document. The value is smaller than the original file.

There are two elements associated with the hash function, namely:

1. *Making an electronic signature uses a hash value that comes from the file and the privacy key (must have been defined). Electronic signatures are applied to the same two documents, but have different private keys.*
2. *When verifying digital signatures, the process must be referenced to the original file and public key. Thus, the signature can be accessed by the recipient.*

Regarding the validity of electronic signatures, the government has issued several official regulations. Guided by these rules, digital signatures have legal powers. So, as if there were frauds or cases of disputes, we can follow up on legal channels.

[10] *Anthony J. Diana & David G. Krone, Electronic Signatures : Legal & Practical Considerations for E-Signing On The Virtual Dotted Line, New York Law Journal, Vol. 1 No. 1, 2019, P. 2.*

IV. CONCLUSION

Based on the above legal analysis, Electronic signatures certified as valid status are almost the same as authentic certificates, whereas if not certified in the process of proof requires digital forensic testing. Both are recognized by law, but their position is much stronger which is certified. Electronic signatures have legal force and legal consequences with the following conditions: Data on the manufacture of Electronic Signatures related only to Signatories; Data on the manufacture of Electronic Signatures during the electronic signing process is only in the power of the Signatory; All changes to the Electronic Signature that occur after the signing time can be known; All changes to Electronic information related to the Electronic Signature after the signatory can be known; There are certain ways that are used to identify who is the signatory; There are certain ways to indicate that the signatory has given approval of related electronic information.

V. ACKNOWLEDGMENTS

This project is support by The Rector of Universitas Komputer Indonesia.

REFERENCE

[1] Rehulina, Keabsahan Digital Signature Dalam Perjanjian E-Commerce, The Journal of Law, Volume 1, 2019.

[2] Meina Diniari Basani, Perkembangan Tandatangan Elektronik di Indonesia, Jurnal Hukum UNPAD, Volume 1, 2017.

[3] Kalama M. Lui Kwan, Recent Developments in Digital Signature Legislation Electronic Commerce, Barkeley Technology Law Journal, Vol 14 No. 1, Annual Review of Law and Technology, 1999.

[4] Charles R. Merrill, Science & Technology Digital : Signature Guidline For Electronic Commerce, Best ABA Sections Journal, Solo & Smal Firm Section, Vol. 1, No. 2, 1997.

[5] Paul R. Katz & Aron Schwartz, Electronic Documents and Digital Signaturing : Changing The Way Business is Conducted and Contracts are Formed, Best of ABA Section Journal, Solo & Smal Firm Section, Vol. 1 No. 1, 1997.

[6] Rahmat Sobari, Penggunaan Tanda Tangan Digital untuk Pengamanan Pertukaran Informasi, Tugas Akhir Proteksi dan Teknik Keamanan Sistem Informasi Bab IV: Cryptography, Program Magister Teknolgi Informasi Fakultas Teknik Komputer Universitas Indonesia 2005.

[7] Edmon Makarim, Kerangka Hukum digital Signature Dalam Electronic Commerce, Makalah Dipresentrasikan Di Hadapan Masyarakat Telekomunikasi Indonesia Pada Bulan Juni 1999 Di Pusat Ilmu Komputer Universitas Indonesia, Depok Jawa Barat

[8] Ilja Ponka, Legal Aspects of Digital Signatures and Non Repudiation, The Journal of Information Law and Technology, Vol. 2, 1999.

[9] Julius Indra Dwipayono Singara, Pengakuan Tanda Tangan Elektronik Dalam Hukum Pembuktian Indonesia, sumber data dari situs www.legalitas.org pada tanggal 1 Juni 2019.

[10] Anthony J. Diana & David G. Krone, Electronic Signatures : Legal & Practical Considerations for E-Signing On The Virtual Dotted Line, New York Law Journal, Vol. 1 No. 1, 2019.

Legal Aspects of The Digital Signature in E-Commerce Connected To Law Number 19 Year 2016 About Amendments to Law Number 11 Year 2008 About Information And Electronic Transactions

***Hetty Hassanah*[1] *and Eman Suparman*[2]**
hetty.hassanah@email.unikom.ac.id[1]
eman@unpad.ac.id[2]
Departmen of Law, Faculty of Law, Universitas Komputer Indonesia,
Dipatiukur Street Number 112-116 Bandung, Indonesia

Abstract

This research aims to find out the legal aspects related to digital signature authentication in e-commerce. The research method used is the normative juridical approach method and the resulting data were analyzed qualitatively juridical. The results obtained are that digital signatures have an important role in the validity of contracts in e-commerce. Based on the legal analysis conducted, the conclusion of this research is that digital signatures that are certified or not certified are recognized by law and have legal force, provided that the identity of the signatory and all processes of signing are known, however the use of digital signatures can also lead to legal problems. The impact of the research that has been done can provide an understanding related to the use of digital signatures, especially in e-commerce, so that people can be more careful in using these digital signatures.

Key words : E-commerce, Digital Signature, Legal aspect

I. INTRODUCTION

Digital signatures are very important to be examined in terms of legal aspects, because digital signatures determine the validity of contracts in e-commerce. In e-commerce there is a digital signature, which is not like a signature that has been known so far, that is by using different methods to mark a document so that the document or data not only identifies the sender, but also to ensure the integrity of the document so as not to change during the transmission process.

There have been some previous researches, among others, the validity of digital signatures in e commerce agreements, by Rehulina[1], the study only discussed one aspect is the validity of digital signatures in the agreement, without elaborating on other legal aspects related to digital signatures in e-commerce. according to his opinion, the digital signature must be accepted as a signature with the following reasons: A digital signature is a signature that can be affixed by someone or some person who is authorized by someone else who wishes to be legally bound; using mechanical equipment, such as traditional / conventional signatures; A digital signature is very likely to be safer or more insecure as it is possible this also occurs in traditional / conventional signatures; as in traditional / conventional signatures. In another study, about digital signature there is research about digital signature in e-commerce, but the results of this study only explain that Information technology is a sector which grows rapidly from year to year. The current development of technology has greatly affected human's life globally. Computer and internet have experienced rapid growth so people can access, communicate, and access anything without limit. The internet is the unifier of people around the world. Due to the advancement and development of information technology, many changes happen. One of them is the increased transactions, which are carried out *through telecommunication media or the internet. In regards to this, digital signature system is developed. Digital signature under Article 1 paragraph (12) of the Electronic Information and Transaction Law is a signature consisting of electronic information attached, associated or related to other electronic information used as a means of verification and authentication[2]. Another study from Kalama M. Lui Kwan explained that digital signatures essentially allow parties to authenticate their document when communicating online. This is particularly useful for parties who want to know that their contract is enforceable, or for companies that want to be assured that customers with whom they are dealing inline thruthfully representing themselves[3]. The other opinion such as form Charles R. Merrill say that digital signature using cryptographic software and the signer of a digital signature will use the sender's private key to transform the message into a digital signature[4].Paul R. Katz and Aron Schwartz say that digital signature is a sequence of bits created when a person, intending to sign an electronic document, runs his or her message, through a one way function to create a unique identifier used for sender verification purpose[5]. The current conditions have been new laws governing the internet and cyberspace, namely the promulgation of Law Number 19 Year 2016 About Amendments to Law Number 11 Year 2008 About Information And Electronic Transaction (Then written UU ITE) concerning Information and Electronic Transactions, but have not explicitly regulated criminal acts of digital signature forgery.*

This research aims to find out the legal aspects related to digital signature authentication in e-commerce. The research method used is a normative juridical approach and the resulting data were analyzed qualitatively juridical. The results obtained are that digital signatures have an important role in the validity of contracts in e-commerce. One of the legal requirements of the agreement is the agreement of the parties or the suitability of the parties' wishes which must be proven by the signature, so that in electronic trading any agreement between the parties must be proven by the presence of a digital signature. The results of this study can provide an understanding of digital signatures used in e-commerce, so that the public can know the benefits and role of digital signatures as a sign of contract authentication in e-commerce as well as the public can be more careful in using digital signatures in e-commerce.

II. METHOD

The specification of the research is descriptive analytical, ie giving the facts systematically. Approach method to be used is normative juridical approach method, in this case test and review secondary data about legal aspect of digital signature on e commerce. All the data obtained are analyzed by qualitative juridical, in this case the analysis is done by considering the hierarchy of legislation so that the one legislation does not contradict other laws and legal certainty.

III. RESULT AND DISCUSSION

Digital signatures are not manual signatures scanned and affixed to documents or emails that we send. Digital signature is one of the uses of cryptographic methods that aims to detect unauthorized modification of data and to check identity authentication from the sender and non repudiation (refusing denial)[6]. The purpose of a digital signature in a document is to ensure the authenticity of the document. A digital signature is actually not a signature as it is known so far, digital signatures use different methods to mark a document so that digital signatures not only identify data from the sender, but digital *signatures also ensure the integrity of the document, not changing during transmission process. A digital signature is based on the contents of the message itself[7].*

Giving digital signatures to the electronic data sent will be able to show where the electronic data actually came from. Guaranteed integrity of the message can occur because of the existence of the Digital Certificate. Digital Certificate is obtained on the basis of application to Certification Authority by user / subscriber. Digital certificate contains information about users including:

1. *Identity*
2. *authority*
3. *legal standing*
4. *status of the user*

This digital certificate has various levels, the level of the digital certificate determines how much authority the user has. An example of this authority or qualification is if a company wants to do a legal act, then the party authorized to represent the company is the board of directors. So if a company wants to do a legal action, the Digital Certificate used is a digital certificate owned by the directors of the company.

The existence of this digital certificate, the third party associated with the digital certificate holder can feel confident that a message / message is true from that user. Integrity / integrity is related to the integrity of the data sent. A message recipient / data can be sure whether the message received is the same as the message sent. He can feel confident that the data has been modified or changed during the shipping or storage process.

The use of digital signatures that are applied to electronic messages / data sent can guarantee that these electronic messages / data do not experience a change or modification by an unauthorized party. This guarantee of authenticity can be seen from the hash function in a digital signature system, where data recipients can compare the hash value. If the hash value is the same and is appropriate, then the data is truly authentic, no action has ever taken place to modify the data during the shipping process, so the authenticity is guaranteed. Conversely, if the hash value is different, then it should be suspected and immediately it can be concluded that the recipient (recipient) receives data that has been modified.

Non repudiation or cannot be denied the existence of a message related to the person who sent the message. The message sender cannot deny that he sent a message when he sent a message. He also cannot deny the contents of a message different from what he sent when he sent the message. Non repudiation is very important for e-commerce if a transaction is done through an internet network, electronic contracts (electronic contracts), or payment transactions[8]. This non repudiation arises from the presence of digital signatures that use asymmetric encryption (asymmetric encryption). This asymmetric encryption involves the existence of the private key and public key. A message that has been encrypted using a private key can only be opened / description using the sender's public key. So if there is a message that has been encrypted by the sender using his private key, he cannot deny the existence of the message because it is proven that the message can be encrypted with the sender's public key. The integrity of the message can be seen from the existence of the hash function of the message, noting that the signature data will be entered into the digital envelope. The messages in the form of electronic data sent are confidential / confidential, so not everyone can find out the contents of electronic data that has been signed and *entered in the digital envelope. The existence of a digital envelope that includes an integral part of a digital signature causes an encrypted message to be opened only by the rightful person. The level of confidentiality of a message that has been encrypted depends on the length of the key / key used to encrypt. At this time the standard key length used was 128 bites. Safeguarding data in e-commerce with cryptographic methods through the digital signature scheme is technically acceptable and applied, but if discussed from the point of view of law, it still lacks attention. The lack of attention from legal science is understandable because especially in Indonesia, the use of computers as a means of communication through the internet has only been known since 1994. Thus, safeguarding internet networks with digital signature methods in Indonesia is certainly still new to computer users.*

Some properties that exist in digital signatures, namely[9]:

1. *It is authentic, a message containing a digital signature can also be evidence, so that the party making the ratification (who signed) cannot deny that he never signed it.*
2. *It is exclusive, only valid for the document (message) or the exact copy. The signature cannot be transferred to another document. This also means that if the document is changed, the digital signature of the message is no longer valid.*
3. *It is global verification, checks can be done easily, even by people who are not related or have never met with the party who did the ratification (who signed) though.*

Digital signatures are used as contract authentication in e commerce.[10]

UU ITE stipulates that electronic signatures have legal force and legal consequences as long as they comply with the provisions of this law, meaning that as long as it can be ascertained the relationship between the electronic signature and the signatory concerned and the electronic signature is made and stored in conditions guarantee integrity with the deed attached to it, then an electronic signature has the same legal value as an ordinary signature.

The rise of cases of electronic crime (cyber crime) has become one of the backgrounds for the use of digital signatures. Now, the Ministry of Communication and Information is actively implementing digital signatures for online transactions. Hopefully, with this technology, the community can carry out various online activities.

In addition to reducing the case of cyber crime, digital signatures also aim to facilitate business activities. The signature can be used to authorize documents. For example, you want to sign a business agreement with someone face to face. Digital signatures can be substituted for wet signatures. The Ministry of Communication and Information is collaborating with the Financial Services Authority to launch the program. Signature validation questions, submitted to Root CA (Certification Authority). This institution is tasked with determining the identity of the digital signature user and continuing the process[11].

Electronic signatures are said to be valid if they meet certain requirements stipulated in the law. In the UU ITE , the legal requirements for digital signatures include the following. Manufacturing data is privacy and only known by the owner of the signature. When creating a signature, only the original owner has the power to use it. If there is a change after making an electronic signature, it can be known with certainty. Digital signatures including those used in e-commerce contracts can be used as electronic evidence, and therefore must be obtained in accordance with existing *laws and best practices to ensure receipt in court.[12]*

All changes to electronic information relating to signatures; can be known. Have a special way to know for sure the owner of his signature. Have a special way to prove that the signature owner has given legal approval regarding certain electronic information. Signing a document has four main objectives, namely as evidence, a sign of agreement, fulfillment of formality, and efficiency. For this purpose to be achieved, there are two attributes of electronic signatures that must be met. Signature owner authentication. That is, the electronic signature is not easy to imitate and is able to show the owner's identity also Document authentication. This gives meaning, under an electronic signature must be able to characterize the authenticity of the signed document. Thus, the document is not easily faked or changed without being known by the author.

In essence, the authentication of the signing and the document must be able to prevent someone from the case of cyber crime, such as forgery. Therefore, electronic signatures must adhere to the concept of nonrepudation. This is one form of guaranteeing the authenticity of the file to prevent denial from the owner of the signature.

In verification of digital signatures, the hash function needs to be considered. Hash is an algorithm used to make a fingerprint type. One hash can usually only be used in one document. The value is smaller than the original file.

There are two elements associated with the hash function, namely:

1. *Making an electronic signature uses a hash value that comes from the file and the privacy key (must have been defined). Electronic signatures are applied to the same two documents, but have different private keys.*
2. *When verifying digital signatures, the process must be referenced to the original file and public key. Thus, the signature can be accessed by the recipient.*

Regarding the validity of electronic signatures, the government has issued several official regulations. Guided by these rules, digital signatures have legal powers. So, as if there were frauds or cases of disputes, we can follow up on legal channels.

The results obtained are that digital signatures have an important role in the validity of contracts in e-commerce. digital signatures that are certified or not certified are recognized by law and have legal force, provided that the identity of the signatory and all processes of signing are known, however the use of digital signatures can also lead to legal problems. The impact of the research that has been done can provide an understanding related to the use of digital signatures, especially in e-commerce, so that people can be more careful in using these digital signatures.

IV. CONCLUSION

Based on the above legal analysis, Electronic signatures certified as valid status are almost the same as authentic certificates, whereas if not certified in the process of proof requires digital forensic testing. Both are recognized by law, but their position is much stronger which is certified. Electronic signatures have legal force and legal consequences with the following conditions: Data on the manufacture of Electronic Signatures related only to Signatories; Data on the manufacture of Electronic Signatures during the electronic signing process is only in the power of the Signatory; All changes to the Electronic Signature that occur after the signing time can be known; All changes to Electronic information related to the Electronic Signature after the signatory can be *known; There are certain ways that are used to identify who is the signatory; There are certain ways to indicate that the signatory has given approval of related electronic information.*

V. ACKNOWLEDGMENTS

This project is support by The Rector of Universitas Komputer Indonesia.

REFERENCE

[1] Rehulina, Keabsahan Digital Signature Dalam Perjanjian E-Commerce, The Journal of Law, Volume 1, 2019, P.45.

[2] Meina Diniari Basani, Perkembangan Tandatangan Elektronik di Indonesia, Jurnal Hukum UNPAD, Volume 1, 2017, P. 45.

[3] Kalama M. Lui Kwan, Recent Developments in Digital Signature Legislation Electronic Commerce, Barkeley Technology Law Journal, Vol 14 No. 1, Annual Review of Law and Technology, 1999, P. 463-481.

[4] Charles R. Merrill, Science & Technology Digital : Signature Guidline For Electronic Commerce, Best ABA Sections Journal, Solo & Smal Firm Section, Vol. 1, No. 2, 1997,P. 50-51.

[5] Paul R. Katz & Aron Schwartz, Electronic Documents and Digital Signaturing : Changing The Way Business is Conducted and Contracts are Formed, Best of ABA Section Journal, Solo & Smal Firm Section, Vol. 1 No. 1, 1997, P. 36-37.

[6] Rahmat Sobari, Penggunaan Tanda Tangan Digital untuk Pengamanan Pertukaran Informasi, Tugas Akhir Proteksi dan Teknik Keamanan Sistem Informasi Bab IV: Cryptography, Program Magister Teknolgi Informasi Fakultas Teknik Komputer Universitas Indonesia 2005, Hlm. 15.

[7] Edmon Makarim, Kerangka Hukum digital Signature Dalam Electronic Commerce, Makalah Dipresentrasikan Di Hadapan Masyarakat Telekomunikasi Indonesia Pada Bulan Juni 1999 Di Pusat Ilmu Komputer Universitas Indonesia, Depok Jawa Barat

[8] Ilja Ponka, Legal Aspects of Digital Signatures and Non Repudiation, The Journal of Information Law and Technology, Vol. 2, 1999, P.5.

*[9] Julius Indra Dwipayono Singara**,** Pengakuan Tanda Tangan Elektronik Dalam Hukum Pembuktian Indonesia, sumber data dari situs www.legalitas.org pada tanggal 1 Juni 2019.*

[10] Ferhi Afifa, Credit Risk and Banking Stability: A Comparative Study between Islamic and Conventional Banks, International Journal of Law and Management, Volume 5, Issue 4, Longdom, Barcelona, Spain, 2017, P.1010.

[11] Anthony J. Diana & David G. Krone, Electronic Signatures : Legal & Practical Considerations for E-Signing On The Virtual Dotted Line, New York Law Journal, Vol. 1 No. 1, 2019, P. 2.

***[12]** Kancauskiene, Jolita**,** Computer forensics and electronic evidence in criminal legal proceeding, Digital Evidence & Electronic Signature Law Review Journal, Volume 16, SAS University of London, 2019, P.11.*

Print this page

ICOBEST 2019

ICOBEST 2019

International Conference on Business, Economics, Social Sciences, and Humanities 2019
Auditorium UNIKOM, 21 November 2019
Website: http://icobest.unikom.ac.id
Email: icobest@email.unikom.ac.id

Date: 26 July 2019

Letter of Acceptance

Dear Authors: Hetty Hassanah & Eman Suparman

We are pleased to inform you that your abstract (ABS-7, Oral Presentation), entitled:

"Legal Aspects of The Digital Signature in E-Commerce Connected To Undang-Undang Number 19/2016 About Amendments to Undang-Undang Number 11/2008 About Information And Electronic Transactions"

has been reviewed and accepted to be presented at ICOBEST 2019 conference to be held on 21 November 2019 in Bandung, Indonesia.

Please submit your full paper and make the payment for registration fee before the deadlines, visit our website for more information.

Thank You.

Best regards,

Dr. Poni Sukaesih Kuniati, S.IP,M.,Si
ICOBEST 2019 Chairperson