Electronic Signatures in Tanzania: Appraisal of the Legal Basis

DESDERIUS M Hekwe
An Appraisal of the Legal Basis for Electronic Signatures in Tanzania

A Dissertation Submitted in Partial Fulfillment of Requirements for the Award of the
Degree of Bachelor of Laws of St. Augustine University of Tanzania

Desderius Hekwe

LLB 12492

May 2013
CHAPTER ONE

INTRODUCTION

1.1. Background to the Problem

Beginning in 1836, the American artist Samuel F. B. Morse, the American physicist Joseph Henry, and Alfred Vail developed an electrical telegraph system\(^1\). This system sent pulses of electronic current along wires which controlled an electromagnet that was located at the receiving end of the telegraph system. Hence it has been traced from the year 1860’s during the American Civil War when the Morse code discovery was used to send messages electronically by telegraph, and some of these messages were agreements to terms that were intended to be enforceable. In 1869, the New Hampshire Supreme Court was the first to give an early validation of electronic signatures. At that time, there was an issue concerned with contractual agreement established via the telegraph or Morse code in the case of *Howley v. Whipple*\(^2\) where it was held that;

"It makes no difference whether [the telegraph] operator writes the offer or the acceptance in the presence of his principal and by his express direction, with a steel pen an inch long attached to an ordinary penholder, or whether his pen be a copper wire a thousand miles long. In either case the thought is communicated to the paper by the use of the finger resting upon the pen; nor does it make any difference that in one case common record ink is used, while in the other case a more subtle fluid, known as electricity, performs the same office"

In the year 1980s many companies and some individual began using fax machines for high priority or time sensitive delivery of documents, although the original signature on the original document was on paper, the image of the signature and its transmission was in

---

1 48 N.H. 48 New Hampshire Supreme Court.
electronic form. Courts in various jurisdiction have decided that the enforceable electronic signatures can include agreements made by email, entering a Person Identification Number (PIN) into a bank Automatic Teller Machines, signing a credit or debit slip with a digital pen pad device at a point of sale, installing software with a click-wrap software license agreement on the package and signing electronic documents online.

In 1966 the United Nations published the UNICTRAL Model Law on Electronic Commerce. The Model Law was influential in the development of electronic signature laws around the world including the U.S, Canada, EUROPE and ASIA. For instance, Article 13 provides that, if an electronic signature concurrently meets the following conditions, it shall be deemed enforceable electronic signature: (1) when the creation data of the electronic signature are used for electronic signature, it exclusively belongs to an electronic signatory (2) when the signature is entered, its creation data are controlled only by the electronic signatory; (3) after the signature is entered, any alteration made to the

---

5 The Personal Information Protection Electronic Documents Act, 13th April, 2000, it define electronic signatures as a signature that consist of one or more letter, characters, numbers or other symbols in digital form incorporated in, attached to or associated with an electronic document, it further provides to the effects that a digital signature is applied in verified in a specific manner.
7 Electronic Signature Law of the People's Republic of China (Adopted at the 11th Meeting of the Standing Committee of the Tenth National People's Congress on August 28, 2004 and promulgated by Order No.18 of the President of the People's Republic of China on August 28, 2004), Article 1 of the law, provides to the effect that "This Law is enacted in order to standardize acts of electronic signature, validate the legal effect of electronic signature, and safeguard the lawful rights and interests of the parties concerned"
8 Ibid.
electronic signature can be detected; and (4) after the signature is entered, any alteration made to the contents and form of a data message can be detected. The parties concerned may also choose to use the electronic signatures which meet the conditions of reliability they have agreed to. This reflects what was intended by the United Nations Commission on International Trade Law (UNCITRAL) Model Law on Electronic Commerce, 1996 as to the authenticity of electronic signature in electronic transactions.

It is well noted that the use of electronic networks to exchange information, products, services and payments for commercial and communication process between consumers and businesses, between businesses themselves, governments and businesses or between governments suffices for the development of electronic commerce around the world which has marked easiness in transacting. For instance, in aspect of commercial or business, electronic signatures has been employed as authenticating instrument that a person consented to the recorded document. Electronic signature therefore took the position of a seal in a paper based document. The eUCP V1.1 Supplement to UCP 600 requires electronic record to be capable of authentication both as to the identity of the sender and that the message has not been intercept or tempered with at the time of transmission, and that authentication can be achieved by the use of an electronic signature.

Tanzania is evidenced to have been influenced with this global changes, as companies, individuals and the government itself is in use of electronic as a means in transacting.

10 The Uniform Customs and Practice for Documentary Credits for Electronic Presentation ("eUCP") supplements the Uniform Customs and Practice for Documentary Credits (2007 Revision ICC Publication No. 600, ) ("UCP") in order to accommodate presentation of electronic records alone or in combination with paper documents.
Meaningwhile, the country have adopted a number of international instruments like UNICTRAL (1996), World Intellectual Property Organisation, World Trade Organisation and at the national level there are laws enacted like The Bills of Exchange Act, Banking laws, Law of Contract Act, the Evidence Act which are highly regulating off-line transactions, and recently the Electronic and Postal Communication Act, 2010 which covers only the registration of telephone sim-cards and to regulate telephone and postal communications within Tanzania only, hence it did not provide regulations on any other electronic means of transacting like internet under which at huge extent commercial transactions are being employed through. This has therefore left the lacunae which were intended by the international community to be covered by each member state engaging in electronic commerce. Therefore the question laid down is on what is the legal basis for electronic signatures in Tanzania

1.2. Statement of the Problem

In Tanzania, like any other country, recently companies, individuals and the country is in use of internet as a means of transacting. Still this study believes that there is mismatching of the law regulating such transactions, and most specific in aspect of authentication of electronic transactions. To this point, the study having reveals this lacunae, it further suggests and give ways for better formulation of the matching legal basis for electronic signatures as a tool for authenticating any electronic records.

1.3. Literature Review

Much have been written recently with regards to electronic commerce of which at large extent the concept of electronic signatures has been advocated as the means of authenticating such transactions made online or on open networks, as reviewed here below;

*Mollel A* in his article\(^\text{12}\), he noted among other things that the evolution of ICT has come with it a new way of authenticating electronic documents. The tool he refers to as electronic signatures, the author poses questions such that whether electronic signatures can meet the degree which is met by manuscript or paper based signatures. He contends further that electronic signatures must meet legal standards for it to be reliable in evidence. Andrew has failed in his work by not providing the frameworks for Tanzania legal basis to that effect, the framework which this study is intending to propose.

*Mambi A*\(^\text{13}\) he asserts that the increase use of electronic authentication techniques as substitutes for manuscript or handwritten signatures and other paper based authentications procedures suggest the need for creating a legal framework that will regulate e-signatures. He admitted that laws in Tanzania neither cover online transactions nor recognize cyberspace or digital signature. Adam further adds that the laws governing business transactions provides that the contract must be in writing and dully signed or authenticated before witnesses, and that this requirement is no longer applicable in online trades, then off-lines laws have to be changed and reformed to accommodate e-commerce principles.

\(^{12}\) Mollel A: *The Legal and Regulatory Framework for ICT in Developing Countries: Case Study of ICT and the Law of Evidence in Tanzania*, at p. 9

Adam Mambi though gives this good position but he neither did propose nor provide the relevant legal basis, as he suggested, the basis which this study is intending to show.

According to Davidson A\textsuperscript{14} he pointed out that the signature has been the prime method used as the proof of identity, and as a material intent and execution of documents. A signature on a document indicates the provenance of a document and the intention of the signatory with regards to the contract. With the advent of electronic era, a form of signature is adopted for electronic documents. The author\textsuperscript{15} asserts further that electronic signature has different risks. While the simple electronic signature merely typed at the end of an electronic record may be less secure than traditional signature “... anyone could type a person’s name at the end of a typed electronic communication. Such signature, while valid in the right circumstances, is most insecure”. Alan does not suggest for mechanisms for securing and validating such electronic transactions, as he does not give much credits on electronic signatures as a tool for security, a tool which this study believes as the only one for authenticating any electronic record.

According to Lewis M\textsuperscript{16}, on his article he advocated for the Canadian legislative approach designed to ensure that electronic signatures have the validity and trustworthiness required by businesses to compete in the global marketplace. The author has tried to cover the traditional objective of signatures and on how those objectives can be met by applying digital signature. However the author has failed to show the framework that develops a

\textsuperscript{14}Davidson A (2009) “The Law of Electronic Commerce” First Published, Cambridge University Press, pp. 74
\textsuperscript{15}Op. cit.
systematic methods for promoting secure electronic commerce transactions between parties over open networks.

According to Stephen E. B\textsuperscript{17}, he define electronic signature as data in electronic form which are attached to or logically associated with other electronic data and which serve as a method of authentication. He added that an electronic signature may take a number of forms, as a digital signature, biometric identifiers such as a voice pattern, facial recognition, a retinal scan, a digitized fingerprint or a digitized handwritten signature, a pin number or merely a name typed at the end of an e-mail message. Professor Stephen Blythe has failed therefore to give the legal verifications on whether if the above mentioned mechanisms or systems are capable of ensuring security in aspect of business transactions as he asserts being the authenticating mechanisms of an electronic signature.

Also Prins C\textsuperscript{18}, while addressing to the Canadian authority he asserts that the government transition to electronic services has been seen as if its services were analogous to those of enterprises that sell or offer services online. Moreover, he suggested that the Canadian government should become a model user of information and communication technologies (ICTs) given that a government’s commitment to electronic commerce would be a key means of unleashing the enabling effect of ICT in government and in the economy as a whole, putting in mind the fact that governments around the world have recognized widely this potential but new technologies. However, the author was in the view that even states


do transact other than private individuals, but he fails to show remarks on how does electronic signatures verify business transactions in legal sense.

*Turban E*\(^{19}\) his work is of significance. He among other things asserts that in E-Commerce we have what is so called the distance selling contracts using distance communication through internet. In real sense he was in the view that a distance selling contract is any contract concerning goods and services concluded between supplier and a consumer under an organized distance sales or services provision scheme run by the supplier, who for the purpose of the contract, makes exclusive use of one or more means of distance communication up to the moment which the contract is furnished. He similarly failed to point out means which can verify such distance trading, since they employs internet as means of communicating.

*Edward L*\(^{20}\) in his work, he tries to give solutions on questions raised out of transactions done over the internet, as when communications is deemed to be an offer and bind the offeror and when the acceptance is effective. These all come into being since the problem which might be observed in online contracts is on how to determine the rule with regards to instantaneous communication which should apply or whether the postal rule is the more appropriate analogy, out of which the author suggested that dispatch of the accepting email or response form is more effective. He is silent then failed by not addressing the issues on whether the dispatch of the accepting email is comparable to seal or electronic signature, also the author similarly failed by not pointing the authenticity of an email in verifying online contracts.

---


\(^{20}\) Edward L (1977) *Law and the Internet, Regulation Cyberspace*
Jianying Z et al.\textsuperscript{21} in their work they noted that the important feature of digital signatures is to serve as non-repudiation evidence. To be eligible as non-repudiation evidence, a digital signature on an electronic document should remain valid until its expiry date which is specified by some non-repudiation policy. As signature keys may be compromised and the validity of signatures may become questionable, additional security mechanisms is needed to be added on digital signatures. Meanwhile, the authors have failed to point out on what is to be added on digital signatures as a tool and evidence that electronic data or record have not tempered with in course of its transmission to the other part, as they were not exhaustive in suggesting other modes as comparable to digital signatures and as electronic signatures in electronic commerce.

Zaremba J\textsuperscript{22} his work is of significance as he tries to respond to hypothetical issues on how electronic contracts are made and the applicable law. He added that internet allows the instantaneous communications of digitized information which is an ideal of negotiation and closing of contracts between distant parties, he went further giving advantages of online contracts as time efficiency and storage savings, for businesses and all the world, and that due to these incentives more and more parties will be transacting over internet for distant parties. He also failed to give solution and position on parties transacting from different jurisdictions, as the other part for instance might be trading from Tanzania the country which do not have good electronic regulatory instrument and the

\textsuperscript{21} Jianying & Robert Deng: \textit{On the validity of Digital Signatures}, Kent Ridge Digital Labs, 21 Heng Mui Keng Terrace Singapore 119613
developed one like United State of America, he fails also by not showing the authenticity of such transaction in case of default by one part.

In his work *Dr. M. Patterson*\(^{23}\) he pointed out that even though legal issues in electronic transactions like the applicable law, jurisdiction and enforcement of legal rights, commercial protection and unsolicited email have been appropriately resolved, internet users will be unlikely to use the internet on a routine basis for commerce, unless they have confidence that their communications and data are safe from unauthorized access or modification. Here the author was in view that electronic data especially in electronic transactions need appropriate security and authentication however the writer is silent by not suggesting on what can authenticate such communications.

1.4.1. **Objectives of the Study**

1.4.2. **Main objectives**

- To examine the legal basis for Electronic Signatures in Tanzania

1.4.3. **Specific objectives**

- To find out whether Tanzania reaches the international standard in recognition of electronic signatures.
- To determine the role of electronic signatures as a tool for authentication of electronic record.

---

\(^{23}\)Dr. M. Patterson (2001) “E-Commerce Law, Session 4b: Infoeconomy issues” Hyatt Hotel, Canberra (Law school of Monash University)
• To give suggestions and provide ways for Tanzania to follow in reaching the international standards of E-Commerce by formulating the matching legal basis for E-Signatures.

1.5. Hypothesis

This study is being guided with the following assumptions;

• That lack of effective legal mechanisms in recognition of electronic signatures has weakened the protection and realization of rights of persons who are transacting through internet.

• That lack of, and ineffective legal institutions, especially in providing security, has marked the failure to meet the demands of the modern commercial transactions and the adopted global changes.

• That weak and poor policy in electronic commerce of the state in Tanzania exposed business man, consumers and the government into huge financial loses and dormant economy.

1.6. Significance of the Study

This study realized many goals;

• As a researcher acquired new knowledge on the effectiveness and validity of electronic signatures in verification of business transactions

• The study creates awareness to the society, as private individual and companies are engaging daily into international transactions by using online ways.
• The Government benefits as with regards to recommendations given out by the researcher, if are to be implemented, also the government is put aware in enacting supportive regulations.

• To St. Augustine University of Tanzania, the copy acts as source of literature review after being put at library. It further enriches learning resources to other students.

1.7. The Scope of the Study

That, the scope of this study covers arenas which recognizes the applicability of electronic signatures, the applicability at international level, from South African Development Community (SADC) in which the practices in Mauritius is observed, and at national level, since it is the place of this case study and where data are being retrieved from government institutions, like the Law Reform Commission, companies, banks, law practitioners and law firms on how electronic signatures is practiced.

1.8. Research Methodology

This study employs both quantitative and qualitative methodology. Data were analysed and presented in themes and tables. The researcher applied both primary and secondary data collection.

Under primary data was collected by interviewing members from government institutions, from TRA, Information Communication Technology (UCT) office at Mwanza, also banks were consulted especially CRDB, NBC and NMB Singida Branch, law firms at Mwanza and Singida, the High Court (Commercial Division) of Tanzania at Mwanza and
companies engages in use of electronic means of transacting, and supplying questionnaires to the same, as respondents.

Secondary data was obtained through text books and case laws, it was a library consultation. Also due to its inadequacy different websites were visited. The purpose being to see how other commentaries of E-Commerce look at E-Signatures and seeing practices from other jurisdictions.
CHAPTER TWO

CONCEPTUAL AND THEORETICAL FRAMEWORK

2.1. Introduction

This chapter focuses on legal basis for E-Signatures based from the overview of computer system revolution, historical background of ICT in Tanzania, concepts relating to E-Signatures, including what is E-Signatures, its forms, the concept of authenticity and the law and trust in E-Commerce, looking at legislative frameworks from other jurisdiction’s laws.

2.2. Overview of Computer System Revolution.

It is true that with the development of computer system in the world, life has become easier with the use of internet, as trade and other stuffs, like contracts to which individuals, banks, accounts, lawyers, businessman and even governments in the world use electronic as a means of communicating or disseminating information. As once noted by Alfonso Lenhardt that;

“We need strong laws to protect the builders and users of the internet in order to foster innovation and creativity, safeguard consumers, drive economic growth and protect our borders.”

24 US ambassador Alfonso Lenhardt and Tanzanian Attorney General Frederick Werema officially opened the cybercrime legislation and capacity building workshop for Eastern and Southern Africa on Wednesday 23rd February 2011.
Here the US ambassador was in the view that states in the world are in need of enacting laws to cope with such global changes. It is well founded that the only tool to be used in authenticating any electronic record, as being advocated in different E-Commerce laws from different perspectives is E-Signatures, which in real sense is the only tool, however being in different forms. It is therefore the requirements of electronic transactions that there must be clear legal basis for E-Signatures at least in each country.

2.3. Historical Background of ICT in Tanzania.

As per Mgaya K\textsuperscript{25} the first computer in Tanzania, an Information Communication Technology 1500, was installed in the Ministry of Finance in 1965. By 1974 there were seven computers in the country and the Ministry of Finance had already acquired a new computer, an ICL 1900. The program of which at the end of the day failed following a number of reasons, like lack of Information Technology personnel, uncoordinated planning and the government intervention after it appears that a lot of resources were used unsuccessful.

With influences from other jurisdictions, especially ICT after being recognized by the United Nations with the adoption of UNCITRAL\textsuperscript{26} following the already existing practices of E-Commerce in countries like USA, Australia, Canada and others, the UN


\textsuperscript{26} Model Law on Electronic Commerce with Guide to Enactment 1996, with additional \textit{article 5bis} as adopted in 1998
was in the view of harmonizing such an electronic transaction. Further with significance role played by the UNCTAD\textsuperscript{27} when the Tanzania E-Commerce practice and the use of internet was examined with the conclusion that the use of electronic as means of transacting was very low at that time, since its infrastructures were poor in comparison with other developing countries like Ethiopia.

The year 2003 is remarkable as it was when ICT sector gets its root in the government planning, it is when the ICT policy was adopted. The policy among other things it intended to create conducive environment for ICT infrastructures in Tanzania, the purpose being to coup with current global-social, political, economic and technological changes.

2.4.1. Concepts Relating to E-Signatures.

These concepts to be discussed herebelow are essential part in this study. They are discussed not just as the cornerstone but as linkage of the coming discussion at hand.

2.4.2. What is E-Signatures?

Electronic signature is referred to as data in electronic form in affixed to or logically associated with, a data message, which may be used to identify the signatory in relation to the data message and to indicate the signatory’s approval of the information contained in a data message\textsuperscript{28}.

\footnote{\textsuperscript{27} The United Nations Conference on Trade and Development, held on 30-31 May, 2000 at Johannesburg, South Africa.}

\footnote{\textsuperscript{28} Section 2 of the UNICTRAL Model Law on Electronic signatures of 2001, also see section 2 of the UNICTRAL Model Law on Electronic Commerce with Guide to Enactment 1996 with additional article 5 \textit{bis} as adopted in 1998, see also section 106 of the U.S Electronic Signatures in Global and National Commerce Act, 2000 it defines electronic signature as “\textit{an electronic sound, symbol or process attached to or logically associated with a contract or other record and executed or adopted by a person with intent to}
A. Davidson (2009)\textsuperscript{29} in his writing asserts that;

“The signature has been the prime method used as the proof of identity, and as a material intent and execution of documents. A signature on a document indicates the provenance of a document and the intention of the signatory with regards to the contract. \textit{With the advent of electronic era, a form of signature is adopted for electronic documents}”. (Emphasis mine)

Stephen E. B (2010)\textsuperscript{30} defines electronic signature as data in electronic form which are attached to or logically associated with other electronic data and which serve as a method of authentication.

Example of E-Signatures includes;

a. A name typed at the end of an e-mail by the sender, as it was determined in Mehta Vs. J Pereira Fenandes SA\textsuperscript{31} to the effect that if a person sent an email typing his name or his principal's name then such an email amounts to a valid signature.

b. A digitized image of a hand-written message signature that is attached to an electronic document \textit{(sometimes created by biometrics-based technology called signature dynamics)}

c. A secret code, password, or PIN to identify the sender to the recipient \textit{(such as used with ATM cards and credit cards)}

d. A unique biometric-based identifier \textit{(such as fingerprints, voice print, or a retinal scan)}

\textit{sign the record}”. The definition which was initially provided under the U.S Uniform Electronic Transactions Act, 1999

\textsuperscript{29}A Davidson (2009) “The Law of Electronic Commerce” First Published, Cambridge University Press, pp. 74


\textsuperscript{31}[2006] EWHC 813 (Ch.) (07 April 2006)
e. A mouse click (such as “I accept” button also called web-click in case a person orders goods by visiting website of the seller and initiates the transactions)

f. A sound (such as the sound created by pressing “9” on your phone to agree)

g. A “digital signature” (created through the use of public key cryptography)\textsuperscript{32}

Therefore, the term electronic signature implies a stylized script associated with a person. It is comparable to a seal in paper based documents. In commerce and the law, a signature on a document is an indication that a person adopted the intention recorded in the document in question.

2.4.3. Digital Signatures.

As there is no central authority controlling the Web, it is assumed that anyone can say anything about anything. This freedom of expression is a great idea, but it can lead to misuse of this freedom and result in mistrust. If the Web has to become the single source of all information, it has to provide a mechanism of proving trustworthiness. The digital signature is the mechanism that is going to be used to provide proof that a certain person wrote (or agrees with) a document or statement. This will create trust to users.

\begin{table}[h]
\centering
\begin{tabular}{|c|c|c|}
\hline
Self-desc. doc. & Data & Rules \\
\hline
Data & Ontology vocabulary & Trust \\
\hline
RDF + rdfschema & Proof & \\
\hline
XML + NS + xsmlschema & Digital Signature & \\
\hline
Unicode & URI & \\
\hline
\end{tabular}
\caption{Effecting that in E-Commerce one may initiate any transaction and assert anything about it, but in E-Signature what is deemed to give proof on certain electronic data is digital signatures\textsuperscript{33}}
\end{table}

\textsuperscript{32}Professor J. M. N Kakooza, Chairman of the Uganda Law Reform Commission: A study report on electronic transactions law; Kampala, Uganda. 2004 (LAW COM PUB. NO. 10 of 2004) at pp. 76

\textsuperscript{33}Encyclopedia of E-Commerce, E-Government, and Mobile Commerce; Mehdi Khosrow-Pour Information Resources Management Association, USA, at pp. 1141
Digital signature provide information regarding the sender of an electronic document. It provide data integrity, thereby allowing data to remain in the same state in which it was transmitted. Here the most widely used type of cryptography is the public key, where the sender is assigned with two keys, one public and another private key. The original message is encrypted using public key while the recipient of the message requires private key to decrypt the message. Then the recipient will be in position to determine whether the message is altered or not.

However, although this system guarantees the integrity of the message, it does not guarantee the identity of the sender (the public key owner). Then in order to remedy this a “Certificate Authorities” (CAs) is required.

The Certificate Authorities are trusted third parties who provide a variety of cryptography service to their clients. CAs are trusted third parties who have been given license to produce digital certificates authenticating digital signatures. In order for this to work the Licensed CA must be reliable and have the confidence of the public and business community. And for those acquires license from the CAs are to be held liable upon any errors by themselves. Hence this provide assurance that electronic commerce are secured.

2.4.4.1 The Concept of Authenticity

2.4.4.2 Authenticity

This is concerned with the source of information, or the sender of such information. Then as the legal requirement and in order to meet this requirement, the most common and popular way of accomplishing this identity check is to use an e-mail based identifier. This
is a process most people have experienced at some point while using the Internet. If you sign up for a web based service you generally need to create a user name and password. When you create this account many systems will send a verification e-mail to the e-mail address you entered for your record, thus proving that you own this e-mail address. Another way to verify an identity is to use a known third party validation mechanism. That you may have experienced it with a web site requiring you enter in your home zip code, an account number or in some cases a credit card number. Many web sites will have you enter your credit card information into a form, allowing them to cross reference the information you provide them with a credit card merchant. Presumably if you told the credit card company the truth about you, then it will match with the information you provided the website.

2.4.4.3 Integrity

Integrity simply means providing a reasonable belief that any file electronically signed on a system cannot and has not been tampered with by anyone or anything. Integrity is critical in e-commerce in negotiation and contracts formation online, licensing of digital content, payment through internet and proving the content of the same at later.

2.4.4.4 Non-Repudiation

Non-repudiation is the ability to hold the sender to his communication in the event of a dispute. A party’s willingness to rely on a communication, contract or funds transfer request is typically contingent upon having same level of comfort that the party can

---


35 Adam J. Mambi (2010); ICT Law Book: A Sourcebook for Information & Communication Technologies and Cyber law; Mkuki na Nyota Publishing Ltd. Dar es Salaam, Tanzania, at pp. 122
prevent the sender from denying that he sent the communication or from claiming that the content of the communication as received are not the same as to what the sender sent.\textsuperscript{36}

2.4.4.5 Security Procedures

Establishing trust in electronic transactions involves the use of security procedures. Security procedure in this context means a procedure employed for purpose of verifying that electronic signature, record or performance is that of a specific person or for detecting changes or error on an electronic record. There are number of procedures to be employed as security in this aspect, like the use of digital signatures, e-mail based identifiers, replies and acknowledgements, repeat-back acknowledgements, date or time stamping, encryption and or the use of Trusted Third Parties (TTPs), (TTPs) in this context referred to mean Certificate Authorities (CAs).\textsuperscript{37}

2.5. The Law and Trust in E-Commerce.

A trustworthy electronic signatures is a precondition to enforceability as a signature. This approach requires an electronic signatures possess four attributes, such that it must be unique to the person using it, it must be capable of verification, it must be under sole control of the person using it and lastly it must be linked to the data such a manner that if the data is changed, the signature is invalidated.\textsuperscript{38}

2.6. Conclusion

It is well notable that with the advancement of computer systems in the world individuals are being in frequent use of that system, Tanzanian are not behind with this global changes

\textsuperscript{36} Opt cit.

\textsuperscript{37} A Green Paper on E-Commerce for South Africa; Co-ordinated and compiled by the Department of Communications Republic of South Africa November 2000, at pp. 64

\textsuperscript{38} This position is notable under section 2 of Canadian Law (PIPEDA), section 5 of ESIGN Act (USA), section 8 of UETA and Article 9 (1,2 and 3) of the Electronic Signature Law of the People’s Republic of China
since internet is in use\textsuperscript{39}. It is also found that the \textit{UNCITRAL Model Law on E-Commerce} intends for state parties to have a universal recognized system of transacting through internet, and in fact it is in this point when Tanzanian are left behind, if we are to compare with other developing countries like Mauritius who has \textit{Electronic Transactions Act (2000)}, also with our dearest neighbor Uganda in 2011 they enacted an \textit{Electronic Signature Law} who in fact are in compliance with the \textit{UNCITRAL} framework. Hence the intention of this study in this chapter is to show how the advancement of computer compels Tanzania to come up with the best infrastructure in enhancing this revolution, and that the enactment of an electronic signature law is of inevitable.

\textsuperscript{39}The National Information and Communication Technologies Policy of Tanzania, of March 2003.
CHAPTER THREE

A LEGAL ASPECT OF ELECTRONIC SIGNATURES

3.1. Introduction

The importance of signatures in any transaction can hardly be overstated. A signature constitutes an authenticity on any record through which any legal obligation is born. With the advent of E-Commerce, online transactions are at climax as billions of people in the world use internet as means of transacting\(^\text{40}\). Therefore, it is the legal requirements that with this technological revolution, there be a well framed system for authenticating the same, to which E-Signatures is referred to as the only tool. Hence this chapter intends to show the legal aspect which is the basis for a well legal framework for electronic signatures in Tanzania.

3.2. International Position in E-Signatures

Under international level E-Commerce is well framed with a number of international organisations\(^\text{41}\), national or regional entities\(^\text{42}\) and Non-Government Organisations\(^\text{43}\) heavily involved in E-Commerce. Also there are laws, such as the UNCITRAL Model Law on

---


\(^{41}\)UNCITRAL, OECD, WIPO, ICAN, The Hague Conference on Private International Law, WTO

\(^{42}\)European Union (EU), Council of Europe, APEC, United States, Colombia, Tunisia, Australia and Argentina.

\(^{43}\)Global Business Dialogue on E-commerce (GBDe), Internet Law & Policy Forum (ILPF), Consumers International, Electronic Privacy Information Centre (EPIC) and the International Chamber of Commerce (ICC)
Electronic Commerce (1996), UNCITRAL Model Law on Electronic Signatures (2001), the Supplement to the Uniform Customs and Practice for Documentary Credits for Electronic Presentation (“eUCP”) revision of 2007 and European Directives which are given time to time.

Specifically speaking of E-Signatures in international level is framed by the UNCITRAL Model Law on Electronic Signatures\(^4^4\). Article 1 of the Model Law gives the scope for its application and it is when electronic signature is used in commercial activities. Article 6 effect that if there is requirement of signature, such is met by data message. The Model Law provide further for an E-Signature to be reliable it must meet four requirements, such that first, the data creation must link with the signatory. Second, the data creation was in sole control of the signatory. Third, any alteration of electronic signature, made after signing, must be detectable. And fourth, where the purpose of the signature is to provide for the integrity of the underlined information, then the alteration must be detectable, respectively.

Under the eUCP\(^4^5\) it requires for electronic records to be capable of authentication both as to identity of the sender and that the message has not been intercepted, read or tempered with during transmission. The eUCP provides further that if electronic record cannot be authenticated, it is deemed not to have been presented. Under eUCP authentication can be achieved by the use of an electronic signature. The eUCP’s definition of electronic

---

\(^4^4\) The Model Law was approved by the UNCITRAL Working Group on Electronic Commerce at its thirty-seventh session, held at Vienna from 18 to 29 September 2000. It took effect in 2001.

\(^4^5\) The Uniform Customs and Practice for Documentary Credits for Electronic Presentation (“eUCP”) supplements the Uniform Customs and Practice for Documentary Credits (2007 Revision ICC Publication No. 600,) (“UCP”) in order to accommodate presentation of electronic records alone or in combination with paper documents
signature is broader enough to cover any form of encryption technology, including the public and private keys provided by the Certificate Authorities (CAs), keys which are used to lock electronic records. As electronic signature is defined to mean;

“A data process attached to or logically associated with an electronic record and executed or adopted by a person in order to identify that person and indicate that person’s authentication of the electronic record”

3.3. Tanzania ICT Policy

The main policies guiding developments in the ICT sector in the country are the National Telecommunications Policy (1997), the National ICT Policy (2003), The National Postal Services Policy (2003) and the National Information and Broadcasting Policy (2003). The policies aim at ensuring accelerated development of ICT infrastructures and services so as to accelerate access to ICT services by all sectors of the national economy as part of the national development strategy.

Tanzania’s ICT Policy was approved by parliament in 2005 to provide Government guidance on ICT issues. Lack of an overall ICT Policy and poor harmonization of initiatives had previously led to the random adoption of different systems and standards, unnecessary duplication of effort and waste of scarce national resources on the one hand, and lack of strategies for the utilization of ICT as a driving force for national development on the other. The policy articulates ten main focus areas in harnessing ICT in Tanzania; strategic ICT leadership, ICT infrastructure, ICT industry, human capital, legal and

---

46 The Uniform Customs and Practice for Documentary Credits for Electronic Presentation (“eUCP”) supplements the Uniform Customs and Practice for Documentary Credits (2007 Revision ICC Publication No. 600,) (“UCP”) in order to accommodate presentation of electronic records alone or in combination with paper documents

regulatory framework, productive sectors, service sectors, public service, local content and universal access.\textsuperscript{48}

Frankly speaking, the National ICT policy as it addresses for legal and regulatory framework for ICT issues in the country, it presupposes that there be initiatives for the same, but in vein. For instance, with regards to digital signatures the policy\textsuperscript{49} provides to the effect that there shall be effective legislations for it, but practically there are no such kind of legislation in place, regardless the Electronic and Postal Communications Act, 2010 which is being enacted to regulate matters relating to telephone communications, while leaving behind the aspect of internet or electronic commerce, this being lacking legal mechanisms for authentications of electronic records. Therefore, one may come to the conclusion that ICT technology in Tanzania is at its initial stage, and that the implementation of the National ICT Policy with regards to electronic commerce, specifically in providing legal basis for electronic signatures is not yet seriously taken into account since no legislation has been enacted to that effect.

3.4.1. The Tanzania Legal Basis for E-Signatures

It is well established out of findings and as per inquiries of this study that Tanzania being among the Sub-Saharan African countries, which is under SADC has got no specific legislation dealing with matters relating to electronic commerce, and so as to say in case of electronic signatures. This study has come out with the findings that the Law Reform Commission of Tanzania has a lot of position papers with regards to enactment of laws to


\textsuperscript{49} The National ICT Policy, 2003, at para. 3.5
regulate internet related transactions, the idea which got rooted from the ambit of the UNCITRAL Model Law on Electronic Signatures (2001), National ICT Policy, 2003 as well as the influence from her neighbors, like Uganda, Namibia and Mauritius whose system with regard to electronic commerce is far reached as I submit.

This study has also come up with the findings that regardless Tanzania has no specific legislation to regulate electronic commerce, including the legal basis for electronic signature, as one part of ICT sector in the country, but sectors like that of telephone and postal communications is well regulated. This as per information from the Tanzania Law Reform Commission evidences that Tanzania has the so called “related laws\(^{50}\)” with regards to electronic commerce. The summary chart below may assist in cementing the above argument.

<table>
<thead>
<tr>
<th>Country</th>
<th>Legal effect of e-transaction</th>
<th>Legal requirement for the validity of e-documents</th>
<th>Contracts formation</th>
<th>Electronic signatures</th>
<th>Consumer protection</th>
<th>Intermediary and Telecommunications Providers</th>
</tr>
</thead>
<tbody>
<tr>
<td>Angola</td>
<td>NONE</td>
<td>NONE</td>
<td>NONE</td>
<td>NONE</td>
<td>NONE</td>
<td>NONE</td>
</tr>
<tr>
<td>Botswana</td>
<td>NONE</td>
<td>NONE</td>
<td>NONE</td>
<td>NONE</td>
<td>NONE</td>
<td>GOOD/LIMIT</td>
</tr>
<tr>
<td>DRC</td>
<td>NONE</td>
<td>NONE</td>
<td>NONE</td>
<td>NONE</td>
<td>NONE</td>
<td>NONE</td>
</tr>
<tr>
<td>Lesotho</td>
<td>NONE</td>
<td>NONE</td>
<td>NONE</td>
<td>NONE</td>
<td>NONE</td>
<td>NONE</td>
</tr>
<tr>
<td>Madagascar</td>
<td>NONE</td>
<td>NONE</td>
<td>NONE</td>
<td>NONE</td>
<td>NONE</td>
<td>NONE</td>
</tr>
<tr>
<td>Malawi</td>
<td>NONE</td>
<td>NONE</td>
<td>NONE</td>
<td>NONE</td>
<td>NONE</td>
<td>NONE</td>
</tr>
<tr>
<td>Mauritius</td>
<td>GOOD</td>
<td>GOOD</td>
<td>GOOD</td>
<td>GOOD</td>
<td>POOR</td>
<td>GOOD (FAIR)</td>
</tr>
<tr>
<td>Mozambique</td>
<td>NONE</td>
<td>NONE</td>
<td>NONE</td>
<td>LIMITED</td>
<td>NONE</td>
<td>NONE</td>
</tr>
<tr>
<td>Namibia</td>
<td>GOOD</td>
<td>GOOD</td>
<td>GOOD</td>
<td>GOOD (FAIR)</td>
<td>GOOD/LIMIT</td>
<td>GOOD/LIMITED</td>
</tr>
</tbody>
</table>

\(^{50}\)Electronic and Postal Communications Act, 2010, Tanzania Communications Regulatory Authority Act, 2003, Miscellaneous Amendments Act, 2007
Table II. Shows the results of the comparative analysis or key elements and status of SADC counties with regards to established system in regulating electronic transactions, and as it appears Tanzania is still at its initial stage.

<table>
<thead>
<tr>
<th></th>
<th>Seychelles</th>
<th>GOOD</th>
<th>GOOD</th>
<th>LIMITED</th>
<th>GOOD</th>
<th>POOR</th>
<th>GOOD/LIMITED</th>
</tr>
</thead>
<tbody>
<tr>
<td>S. Africa</td>
<td>GOOD</td>
<td>GOOD</td>
<td>GOOD</td>
<td>GOOD</td>
<td>GOOD</td>
<td>GOOD</td>
<td>GOOD</td>
</tr>
<tr>
<td>Swaziland</td>
<td>NONE</td>
<td>NONE</td>
<td>NONE</td>
<td>NONE</td>
<td>NONE</td>
<td>NONE</td>
<td>NONE</td>
</tr>
<tr>
<td>Tanzania</td>
<td>NONE</td>
<td>NONE</td>
<td>NONE</td>
<td>LIMITED</td>
<td>LIMITED</td>
<td>GOOD</td>
<td>GOOD</td>
</tr>
<tr>
<td>Zambia</td>
<td>GOOD</td>
<td>GOOD</td>
<td>GOOD</td>
<td>GOOD</td>
<td>GOOD</td>
<td>GOOD</td>
<td>GOOD (FAIR)</td>
</tr>
<tr>
<td>Zimbabwe</td>
<td>NONE</td>
<td>NONE</td>
<td>NONE</td>
<td>LIMITED</td>
<td>LIMITED</td>
<td>NONE</td>
<td>NONE</td>
</tr>
</tbody>
</table>

3.4.2. The Related Laws to E-Signatures and the Influence of Electronic Commerce in Tanzania

It is the findings of this study, as contended above, that with the advent of ICT and the adoption of a new means of transacting, this development has left lacunae in the Tanzania legal frameworks in aspect of legal basis for authenticating electronic record, and in this context the reference is made to the lack of a well legal framework for E-Signatures. This study has therefore discover to the effects that, regardless that Tanzania has no specific legislation to that effect but it has some related laws, which are to be discussed hereunder;

The Electronic and Postal Communications Act the law is with a view to abreast with developments in the electronic communications industry, which further intends to provides for a comprehensive service regulatory regime for electronic communications service providers and postal communications service providers, the law also intend to establish the Central Equipment Identification Register for registration of detachable SIM card and

---


52 The Electronic and Postal Communications Act No. 3 of 2010
built-in SIM card mobile phones, the law also provides for duties of communications and postal service providers and their competition, respectively. This law, as per section 2\textsuperscript{53} has its operation in Tanzania mainland and in Zanzibar. The law is said to have some relation with regards to electronic signatures, due to its effect as some concepts has been defined under section 3\textsuperscript{54} of the Act, concepts like “computer” and “electronic communication” which in implications comprises electronic record, but specifically referring to the Act itself, does not provide for any regulation with regard to neither electronic commerce nor electronic signatures.

Written Laws (Miscellaneous Amendments) Act\textsuperscript{55} under which section 35 of the Act\textsuperscript{56} has amended section 78\textsuperscript{57} by adding section 78A which provides for admissibility of electronic record in evidence. The tension for admitting electronic records has started since 2000 when the wisdom of the High Court of Tanzania was called upon to rule whether electronic evidence is admissible as best evidence in the case of Trust Bank Ltd v. Le-Mash Enterprises Ltd., Joseph Mbu Magari, Lawrence Macharia\textsuperscript{58} In this case, the court ruled that the electronic evidence is admissible in Tanzania courts and this was a departure from the strict rule of best evidence rule. Again in R v. Prof. Costa Ricky Mahalu and Another\textsuperscript{59} when the court allowed for electronic means be employed in hearing evidence from Italy. These all has further, furnishes for the legislature to amend the Evidence Act

\textsuperscript{53}The Electronic and Postal Communications Act No. 3 of 2010  
\textsuperscript{54}Ibid. section 3  
\textsuperscript{55}The Written Laws (Miscellaneous Amendments) Act No. 15 of 2007  
\textsuperscript{56}Ibid. section 35  
\textsuperscript{57}The Evidence Act, CAP. 6 (R:E 2002)  
\textsuperscript{58}High Court of Tanzania Commercial Case No. 4 of 2000  
\textsuperscript{59}2006 (Unreported case) who were charged for loss of 2 million Euros during the purchase of an embassy building
which in effect provides for a room for verifying any electronic records, including an electronic signatures.

Banking laws, in this context the reference is to be made with regards to electronic payments system as adopted by mobile companies, like TIGO PESA, M-PESA and ZIP, which are presupposes to be regulated under the Tanzania Communications Regulatory Act\textsuperscript{60} which is to make link between these companies. But the Bank of Tanzania under its report\textsuperscript{61} has proved that banks has adopted an electronic payments system. Mechanisms like the Society for World Interbank Financial Telecommunications (SWIFT) code till December, 2010 about 36 banks operating in Tanzania had adopted this system, and that in 2004 an Electronic Funds Transfer System was adopted, which currently, this as per interview with the Singida’s National Microfinance Bank manger Miss. CHRISTINA on 16\textsuperscript{th} September, 2012, she laments that banks are faced with the ongoing world economic commerce but there are some aspects which lacks legal framework, as in cases of authenticating same records.

3.5.1. A Comparative Analysis of the Legal Basis for E-Signatures from Mauritius.

It is the findings of this study that among the fifteen SADC member states, namely, Angola, Botswana, Democratic Republic of Congo (DRC), Lesotho, Madagascar, Malawi, Mauritius, Mozambique, Namibia, Seychelles, South Africa, Swaziland, Tanzania, Zambia and Zimbabwe, although some has enacted laws regulating e-transaction and e-commerce,

\textsuperscript{60}Tanzania Communications Regulatory Act No. 12 of 2003

\textsuperscript{61}The Tanzania Mainland’s 50 years of independence: A Review of the Role and Functions of the Bank of Tanzania (1961-2011), June, 2011, pp. 63
but it is Mauritius which has the best provisions of law on electronic signatures than any other country in the region\textsuperscript{62}

The legal framework for e-commerce infrastructures in Mauritius although in line with the UNCITRAL Law Model, 1996\textsuperscript{63} but at high extent she adopted the Indian e-commerce mode, as delegations from India since 2000 has played a bigger role in term of technology and financing such national plans. Speaking in December, 2002, Mauritian Finance Minister, SUSHIL KUSHIRAM\textsuperscript{64} announced that the Indian Government would be assisting in the e-development initiative, providing a credit line of USD100 million to finance the development of the Mauritius 'cyber city'

3.5.2 Laws

The work group responsible for the drafting of the Mauritian legislation examined the UNCITRAL Model Law and considered e-commerce legislation introduced in countries such as Singapore, United Kingdom (UK) and Australia. The following guiding principles were adopted, that the need to conform to international standards and international models in order to be integrated with the global e-commerce framework, second, the need to avoid over regulation, third, the need to be flexible and technologically neutral to adapt quickly to a fluid global environment and the need for transparency and predictability.


\textsuperscript{63}http://www.icta.mu/laws/ict_laws.htm, accessed on 20th Feb, 2013

\textsuperscript{64}http://www.businessinmauritius.com/e_commerce.html, accessed on 06th December, 2012
The key electronic signature legislation in Mauritius is the **Electronic Transactions Act**\(^{65}\) enacted with the view to provide for an appropriate legal framework to facilitate electronic transactions and communications by regulating electronic records and electronic signatures and the security thereof. The objectives which is incorporated for under section 3 (a-h) of the Act\(^{66}\)

The Act has provide the legal basis for electronic signatures, starting with its definition under section 2 of the Act, to effect that an electronic sound, symbol, or process attached to or logically associated with an electronic record and executed or adopted by a person with the intent to sign the electronic record qualifies as signatures in electronic document, the definition which includes digital signatures employed under Public Key Infrastructure (PKI), whereby public and private keys are used in encryption and decryption of an electronic record.

PART II of the Act\(^{67}\) provides for the legal recognition of electronic records. Which effects that the requirement for writing shall be mate by electronic signature, and that electronic record shall be kept in electronic form, and that for it be recognized legally it must be kept in same form and content also that the same must be accessible. Under the ETA\(^{68}\) a digital signature shall be treated as a secure digital signature if it can be verified, through the application of a prescribed security procedure or a commercially reasonable security procedure agreed to by the parties involved so long as the signature is unique to the person using it, capable of identifying such person, created in a manner or using a means under the sole control of the person using it; and linked to the electronic record to which it

---

\(^{65}\) The Mauritius Electronic Transactions Act No 23 of 2000  
\(^{66}\) Ibid. section 3 (a-h)  
\(^{67}\) Ibid. PART II  
\(^{68}\) The Mauritius Electronic Transactions Act No 23 of 2000
relates in a manner such that if the record is changed, the digital signature would be invalidated.

There are four ways in which a digital signature can be given legal recognition under the Act, such as first, the use of certificates issued by a licensed Certificate Authorities, second, the use of certificates issued by a Certificate Authorities outside Mauritius but recognized by the Controller of Certificate Authorities, third, use certificates issued by an approved Government Certificate Authorities and, or establish a contractual agreement between the parties involved in the transaction to use a prescribed digital signature mechanism that is secure\(^{69}\)

**The Electronic Transactions (Certification Authorities) Regulations\(^{70}\)** its rationale is found during online transactions, when transacting parties may not be able to reliably verify each other identity. A Certification Authorities (CAs) thus plays the important role of a trusted third party in vouching for the identities of holders of certificates that it issues (to its subscribers). The Regulations seek to set a benchmark for the integrity and security of the services offered by Certification Authorities. The Regulations aim to ensure high standards of integrity, security and service levels for licensed CAs in Mauritius by putting in place a licensing scheme for CAs, laying down the administrative framework for licensing by the Controller of CAs, and stipulating the licensing criteria for CAs in Mauritius and the continuing operational requirements after obtaining a license.

---

\(^{69}\) Section 19 of the Mauritius Electronic Transactions Act No 23 of 2000  
\(^{70}\) The Electronic Transactions (Certification Authorities) Regulations, 1\(^{st}\) of December 2010. Government Notice No. 213 of 2010
Other legislations include the **Data Protection Act**\(^{71}\) which is to provide for the protection of the privacy rights of individuals in view of the developments in the techniques and technologies used to capture, transmit, manipulate, record or store data relating to individuals. **The Information and Communication Technologies Act**\(^{72}\) establishes the Information and Communication Technologies Authority, the Information and Communication Technologies Advisory Council, the Information and Communication Technologies Appeal Tribunal and to provide for the regulation and democratisation of information and communication technologies and related matters. The Authority in reference above means the ICT Authority established under section 4 of the Act, to deal with all matter relating with ICT in the Mauritius, and the Advisory Council above is there to advise the ICT Authority while the Appeal Tribunal is to determine matter relating with ICT in the country.

### 3.5.3. Institutions

The Mauritius’s institutional framework for electronic signatures is framed in the sense that securities for electronic records is highly reached. This can be seen from the established legislative mechanisms in regulating the same. Even the institutions to be looked hereunder are well legally framed.

Starting with the Government of Mauritius. It is obvious seen from this study that the government has enacted the ETA in 2000 followed with other laws. But much enough is the government resources spent in enriching this sector with the view to coup with global changes. The legislature on the other hand has played a virtue role in enacting e-

---

\(^{71}\) The Data Protection Act No. 13 of 2004  
\(^{72}\) The Information and Communication Technologies Act No. 44 of 2001
transactions laws. And the National ICT Policy\textsuperscript{73} of 2007, has its long plan which ends in 2011 with a lot of realizable achievements in the industry of e-commerce.

Coming to established institutions for specific dealing with provision of licenses and authenticity of the same. Here the government of Mauritius has employed itself in improving the Public Key Infrastructure (PKI), and its major components are the Controller Certificate Authorities (CCAs), the Certification Authorities (CAs) and the Registration Authority (RA). PKI is a framework of policies, services and encryption software that gives users the guarantees that they can transmit sensitive information online be it on the Internet or other networks.

For instance the CCAs acting under section18 of ICTA, section 7 of ETA has the duty to regulate and license the activities of CAs in Mauritius\textsuperscript{74}. As CAs perform a trusted role in verifying the identities of parties in electronic transactions, the CCAs seeks to provide the assurance that the CAs responsibilities are met and that these services are made available with high integrity, security and service standards. The duties of a CA as per sections 24 to 32\textsuperscript{75} include using trustworthy systems in performing its services and maintaining secure procedures for the issuance, renewal, suspension, revocation and publication of its certificates.

The procedure to acquire a license for using a particular digital signature is by an application submission in a prescribed form, application processing and award or rejection of the same. An application has to be accompanied by the following documents, certified true copies of the insurance certificate, cheque or bank draft for prescribed amount as fee,

\textsuperscript{73}The Mauritius ICT Policy 2007-11
\textsuperscript{74}section 37 of the Electronic Transactions Act, 2000
\textsuperscript{75}The Mauritius Electronic Transactions Act, 2000
certified true copies of the company’s resolution, business plans (including cash flow projections and budget statements), audited accounts for the past three years (if applicable), the CA’s Certification Practice Statement (CPS), technical specifications of the CA system and CA security policies and standards, organisational chart and details of all trusted personnel, report of the initial audit within four weeks upon completion of the audit (if available at that point in time), a certified copy of the licence of an existing foreign CA applying for recognition in Mauritius, copy of Data Controller Certificate issued by the Data Protection Office under the Data Protection Act, 2004

3.6. Conclusion.

The findings of this study on the legal basis for electronic signature in Tanzania has the proof that Tanzania lacks the legal framework neither for e-commerce nor e-signatures totally, and thus there are related laws, such as the Electronic and Postal Communications Act the law which does not have specific provisions to regulated e-signatures and e-transactions specifically. It is also been noted from the finding of this study that banking laws are in dilemma since under today’s technological evolution with the adoption of ICT in the world, banks has also resorted to a new system of trading, for instance in Tanzania poor legal framework for e-transaction has exposed not only business man but also investor and tourist into hardships. The Bills of Exchange Act for example, provides for cheque to be in writing and signed by the maker, the effect of which if not so complied with, the person therein cannot be held liable, this position currently in Tanzania do favors paper- based banking, hence with the advent of ICT revolution a new legal regime need be employed to coup with such global changes.

76 the Electronic and Postal Communications Act No.3 of 2010
77 The Bills of Exchange Act, CAP 315 [R:E 2002]
The comparative analysis of the legal framework for e-signature in Mauritius has been of significance in this study, and same proves that for sure Tanzania has not have only laws regulating internet transactions but also even the said to be related laws can play nothing in either glorifying or authenticating electronic signatures. The system being well framed, like having good laws, as for cases of Electronic Transactions Act, 2000, the Data Protection Act, 2004 and the Information and Communication Technologies Act, 2001 in Mauritius, also being established legally with strong institutions like the government, Controller Certification Authorities, Certification Authorities, Registration Authorities and ICT Authority, can be beyond doubts a good system with realizable legal basis for electronic signatures, respectively.
CHAPTER FOUR

CONCLUSION AND RECOMMENDATIONS

4.1. Introduction

The findings of this study are centered on appraisal of the legal basis for electronic signatures in Tanzania, out of which a comparative analysis of the Mauritius’s legal basis for e-signatures is being of significance for reframing the Tanzania e-commerce legal framework. Therefore, this chapter in upholding the findings above comes with a conclusive remarks and recommendations to the government and stakeholders, who are beneficiaries of e-transactions, as hereunder.

4.2. Conclusion

Normally, the real meaning of development is the changes occurs either automatically or brought by forces of something not easily controllable, but which demands for its adherence for better ending.

With the ICT development in the world, changes has been noted from individual to government perspectives, as billions of people are using internet or electronic in transacting. The development which is brought by technological changes, which in any society are inevitable. With this technological evolution, different sectors of society’s mode of social, economic, political and technological life are in need to be changed in compliance with this global changes. In this aspect the society is in need of changes in legal framework as it regulate every aspect of changes which affect an individual’s life, as this study tries to single it out;
“Law is the informing principle of society at every stage of development, from the maxim *ubi societas ibi ius, ibi ius ubi societas*, meaning where there is society there is law and where there is law there is society, and the law grows with this society, from flint stones to genetic clones, from oral contracts to paper based contracts to cyber contract, law is a governing aspect that must reflect the reality to a particular aspect existing at that particular time.”

The study shows that Tanzania does not have any legislation providing provisions for authentication of electronic signatures. Meanwhile individual, companies and the governmental institutions in Tanzania employs in the use of electronic or internet as means of transacting, the country and stakeholders while about and before testing the sweetness of using cyber system they faces bad fumes even before they open their mouth, to mean that the system in Tanzania is not secured, since it lacks a well-established legal basis to regulated the same, as this study tries to show.

**4.3.1. Recommendations**

**4.3.2. To the Executive**

The executive, as it is the organ of the state. Serious measures need to be taken and put in practice, since the executive with the assistance of the Ministry of Communication, Science and Technology is under duty to make sure that it keep on adopting such evolution. With regards to electronic signature laws, the ministry is to come up with proposal to that effect, for launching a bill on electronic signature, as in the case of Uganda, they enacted the Electronic Signatures Act\(^79\). So that the executive with its ministries should study the legal frameworks of other countries, as in the case of Mauritius it adopted the Indian model of PKI system.

---


\(^{79}\) Uganda Electronic Signatures Act No. 7 of 2011, which came into force on 18\(^{th}\) March, 2011
4.3.3. To the Parliament

Being the organ with inherent constitutional power of enacting and amending laws, by virtue of Article 97(1)\(^80\), therefore, this organ of the state must use this power to fill this lacunae, since there is no law which is enacted to regulate e-transaction related matter, apart from the Electronic and Postal Communications Act\(^81\)

There are existing laws which merely regulate only manuscript or handwritten documents (paper based system), laws like the Law of Contract Act\(^82\) has huge impact in contract formation, and here the reference is to be made with regards to contract formed off-line while living contract formed online uncovered, then this laws is subject to amendment or there be enacted the law to carter for online contract. The Bill of Exchange Act\(^83\) this law demands for cheque be in writing and signed by the maker, the effect of which non-compliance the maker will not be liable, so this law need be review to cover the position of electronic form of making and delivering cheque. The Interpretation of Laws Act\(^84\) it defines writing as “any expression referring to writing include printing, lithography, typewriting, photography and other modes of representing or reproducing words in visible form”. From this definition, it is clear that digital information is not a representation or reproduction of words in a visible form. Therefore, even this law need be reviewed to cover concepts of electronic records. The Fair Competition Act\(^85\), an Act to promote and protect effective competition in trade and commerce, to protect consumers from unfair and misleading

---

\(^{80}\)The Constitution of the United Republic of Tanzania, 1977  
\(^{81}\)The Electronic and Postal Communications Act No. 3 of 2012  
\(^{82}\)The Law of Contract Act, CAP. 345 [R:E 2002]  
\(^{83}\)The Bill of Exchange Act, CAP. 315 [R:E 2002]  
\(^{84}\)The Interpretation of Laws Act, CAP. 1 [R:E 2002]  
\(^{85}\)The Fair Competition Act No. 8 of 2003
market conduct and to provide for other related matters. This law does not cater for protection to people who are doing their transition electronically, this law is subject to review for that effect.

In fact the parliament has great role to play in making sure that it enact laws to cover the authentication of electronic signatures and e-transactions at large.

4.3.4. To the Law Reform Commission

The Law Reform Commission of Tanzania was established by the Law Reform Commission of Tanzania Act\textsuperscript{86}, its function among of which is to review existing laws, also to provide position papers for proposing the enactment of certain laws. With this effect there is plans of proposing for the parliament to enact the law to give effect to e-commerce, the same shall give legal basis for authentication and framework for electronic signatures in the Tanzania legal basis. It is the recommendation of this study that the commission to have studied models of other counties, especially under SADC region, where there are countries with laws with good provision in relation to electronic signatures, like the Electronic Transactions Act, 2000 of Mauritius.

4.3.5. To E-Commerce beneficiaries

Beneficiaries of e-commerce includes individuals, enterprises and governments in the world. With regard to Tanzania individuals and financial institutions are highly in use of e-commerce. It is the recommendation of this study to them that, by virtue of being stakeholders in this respect they are to be updates with this evolution and that they participate fully in contributing for better formation of good legal basis for electronic signature in the country.

BIBLIOGRAPHY

Books


Paper and Journals


Dr. MOIRA, Patterson (2001) “E-Commerce Law, Session 4b: Infoeconomy issues” Hyatt Hotel, Canberra (Law School of Monash University)

EDWARD, L (1977) “Law and the Internet” Regulation Cyberspace


Websites


http://www.uncitral.org/english/texts/electcom/mlecomm.htm, visited on 20/08/2012

http://www.europa.eu.int/comm/internal_market/, visited on 20/08/2012


http://www.businessinmauritius.com/e_commerce.html, visited on 06th December, 2012