Law Relating to Digital Signature and its Protection Mechanism: A Comparative Study

*By **Henry Peter***

LLM (University of Iringa), LLB (University of Iringa), Assistant lecturer in Law at Saint Augustine University, Tanzania

Orcid: 0009-0002-7166-0172

Abstract

The practice of appending signature to documents has a long history, as the existence of human beings on the Earth. This practice started even before the invention of current handwriting, whereby societies such as, Sumerians and Egyptians in the era 3000 -2500 BC; employed pictographs (meaning picture and symbols) to convey message, appending signature on clay tablet or stone and to identity the sender of the message. In medieval era people used signature appended on documents to attest its authentication through endorsements of thumb inked prints or signing under official seal or in certain circumstance the use of signet ring from the Crown. The enlighten era came with both, know–how knowledge and technological advancement, the technological advancement introduced a new sophisticated mechanism of attestation to the authentic of document, through electronic means, which came to be known as electronic or digital signature. This paperwork examined in a comparative study; on the analysis of law relating to digital signature and the protection mechanism on how these digital signature can be protected.

Keywords: Digital Signature, Laws governing digital signature, Methods of protecting digital signature.

Introduction

Digital Signature, there is no universal agreed definition of what is digital signature, however; the meaning of this concept has been attributed to mathematical scheme of electronic messages or data send from one party to another, which validates the contents of the message, remained unaltered and authentic of sender identity.[i] The term may mean a mathematical algorithm that provides the sender with unique encryption verification keys attached to the document which validate the authentic of the contents of document as signed by the maker.[ii] Moreover, this term can be defined as the electronic fingerprint of analog handwritten signature; use to assure the third party the integrity of information and the identity of the sender or signer.[iii] This term may mean an encrypted codes of information which is signed electronically, that provides the receiver with a public key of the sender enough to decrypt the document to attest its authentication and the identity of the sender.[iv]

Digital signature and electronic signature are used interchangeably, however; the term digital signature is only a form of electronic signature which applies asymmetric algorithm (with encryption and decryption keys) to attest the validity of document and the identity of the sender. While electronic signature embodies different types of e-signature to include click mouse signature, or by fingerprint on the document or via handwritten signature on electronic devices, such as pad or tablet.[v] It's argued that digital signature plays an equivalent role with traditional handwritten signature on its validity and legal enforcement, due to number of legislations both domestic and international which recognize and validate its applicability.[vi] Hence, digital signature, is a digital file that is attached to electronic document which use algorithm encryption and decryption codes to attest the authentic of the content of the document sent and the sender identity.

The creation of digital signature starts with asymmetric cryptography; being algorithm keys, one public keys and private keys. Where public key being a decrypted key will be sent to the receiver of data message and the sender retains private encrypted key which is a secret key. Creation of plain text, which generates the hash algorithm, this hash algorithm generates digest. Digest is informed of verification codes to be used in comparison with the digest that will be generated by the receiver of an electronic document. Then the private key encrypts the digest

which forms asymmetric cryptography algorithm, this process creates what is called "digital signature".

The receiver get the document (data message) with sender digital signature appended on it, the receiver use public key to decrypt the digital signature to verify if the document sent came from the claimed sender.[vii] If the public key decrypts the asymmetric cryptography algorithm, then the document is verified; moreover, the receiver must generate the hash algorithm to compare the digest he generates from that of the sender to test the authentic and integrity of the data message; if the digest matches then, the document is genuine and the sender identity is un-repudiable.

But if digest doesn't match; then the document was tempered in the process of transit from the sender to the receiver, and the data message is no longer authentic or integrity and the same to the identity of the sender, this will automatically send an alert to both parties (sender & receiver) about compromise or breach of digital signature.[viii] Moreover, it's worth noting that what is encrypted is not the message, but the signature, which gives the receiver access to the digital message sent with attached digital signature.

The application of digital signature or electronic signature is in different areas including; financial institutions/banking, health services centers and government authorities. The application is mainly for security purposes, such as credential for access control, network access control point, and electronic transaction security and documentation workflow. Moreover, these electronic signatures are now widely legally used in contractual agreements, biometric security verification in developed countries digital signature is used in point of sale transaction, and in bank signature cards.[ix] Hence; due to the development of ICT the applicability of electronic or digital signature in different transactions mainly of economic/business nature is inevitable.

Purpose of Digital Signature

The use of digital signature serves mainly four purposes, the first purpose is authenticity of information/data message; to the effect that digital signature validates the information/message

sent.[x] Gives the receiver the reason to believe that the information came from the claimed sender, due to his attestation attached to the message[xi]. The law recognize that digital signature authenticates the information just like traditional handwritten signature, enough to give validity of the attested information.[xii] Another purpose is to ascertain the integrity of the information, the comparison of digest, generated by receiver with that of the sender, test to integrity of document to see whether there was any compromise, alteration or breach in the course of transmission of information from the sender to receiver.[xiii]

Moreover, digital signature serves as non-repudiation clause, to the effect that, the sender cannot later deny the document. The asymmetric cryptography algorithm binds the sender, due to the reason that, only his private encrypt keys matches with the public decrypt keys used by the receiver to decrypt the digital signature attached to the document.[xiv] Also digital signature serves confidential and privacy purpose between sender and receiver of information. This is because only the sender and receiver know decryption codes to access the information, and in case if there is any compromise of information, then the sender and receiver will be alerted about the breach.[xv]

Equivalence purpose, this is the creature of laws across the global, that digital signature is of equal legal value, recognition, validity and enforcement just like the traditional handwritten signature. Laws in many jurisdictions advocates that digital or other forms of electronic signature serves the same purpose, such as authentication of information, integrity attached to the message and the identity of the sender, just like what traditional handwritten signature serves.[xvi] Laws of different jurisdictions supplement this purpose; such as, *Section 14 (2) & 16,* of Uganda Electronic Signatures Act, 2011; the same effect is found under *Section 7,* of U.S Uniform Electronic Transactions Act of 1999; and *Section 6 & 10,* of Tanzania, Electronic Transactions Act, 2015; and the same is supplemented by *Article 3,* of UNCITRAL Model Law on Electronic Signatures with Guide to Enactment 2001.

Evidential purpose, the use of digital signature serves as evidence of the intention of the signatory. Traditionally, handwritten signature once affixed on the document used to show the intention of the signatory, this applies the same to a signatory under digital signature to the effect that, the signatory intended to sign and to be bound by the contents of data message to which his signature is appended. Signatory intention has been the prima facie requirement

under various laws, to the effect that, the signatory later will not be in the position of denying the authentic of contents which the intention adopts and acknowledges through his appended signature.[xvii] The signatory intent requirement is also supplemented by various provisions of the laws, such as *Section 6 (2) (a),* of the Electronic Transactions Act, 2015, as the Section reads;

> "…the method is used to identify the person and to indicate the intention of that person in relation with information communicated…"[xviii]

Hence; digital signature serves as evidential function of signatory intention on the contents of the document, because his signature may be used to *prima facie* establish, as evidence of his intention to adopt the document of contents therein.

Conclusively, digital signature falls under electronic signature, but it's more secure than any other form of electronic signature, as it relies on asymmetric cryptography algorithm to authenticate the information or data message and the identity of the sender; which is so different with other types of electronic signature, which do not use unique encryption algorithm to append signature on the document.

Historical Perspective on the Development of Digital Signature

The history, development and technological advancement of signature is old as the history of human beings on Earth. In ancient era people appended signature on documents (even before the invention of paper documentation), via various ways, such as thumb ink or fingerprint appended to document, or the use of Crown Signet Rings where the messenger carries with it to the intended receiver and in certain circumstance under official crown seal. It's argued that the earliest form of literature and signs of signature dated back from 3000 BC to 2500 BC, during the era of Sumerians and Egyptians, these society used pictographs (meaning the use of symbols and picture to sign), these ancient scribes (mainly or all where in clay tablet) used by these society to convey meaning, attest the authentic of the message and identify the sender.[xix]

Moreover, the development of signature came under the era of Greek and Romans, as it's argued that World alphabet came from Greek, as in the era around 1200 BC, Greek invented

Phoenician alphabet which contained only 22 letters, with written style from right to left, which was after changed from left to right. It's also contended that, Romans borrowed these Phoenician alphabets from Greek; around 439 AD, during the reign of Valentinian III, Romans started to use signature. Furthermore, it argued that; the notorious signature figure appeared in the history books, was from famous nobleman and military leader "El Cid" from Medieval Spain, in the era 1069.[xx]

In 1677 the English Parliament passed the State of Frauds Act, which recognized and mandated the use of traditional handwritten signature, to be appended to document, such as contract, for the purpose of preventing fraud. In 1976, Whitfield Diffie and Martin Hellman introduced the first notion of modern/electronic or digital signature, this marked the development of electronic or digital signature in the World, as we current perceive.[xxi]

Whereby a year later, in 1977 the first primitive digital signature was recorded, being the result of RSA algorithm invention (named after Ron Rivest, Adi Shamir and Len Adleman), which was the set of asymmetric cryptography algorithm, which used two set of keys, one private and public keys to encrypt and decrypt the document, also this algorithm enabled the user to append digital signature over the message.[xxii] The history continued, to the effect that; in the years 1980s, the development of fax machines, started to revolutionize the traditional signature from handwriting to electronic scanned signature (through the use of more sophisticated chip or pin to sign documents, such as contract). Goldwasser, Micali and Rivest, in the year 1988 were the first to rigorously establish security requirement/measures for the use of digital signature scheme (meaning set of asymmetric cryptography algorithm to be used in constituting digital signature). Moreover, in 1989 & 1999 the first software that offered digital signature called Lotus Notes 1.0, was released, as it's argued that the first digital signature were form Lamport signatures, Merkle signatures and Rabin signatures, followed the RSA algorithm, this invention was followed by PDF Format, which added the of insertion of digital signature into document.[xxiii]

During the 21st Century, Parliaments around the World started to enact laws, which recognized, validated and enforced the use of digital signature or online signature (electronic signature) in transactions. The first laws include, the U.S Uniform Electronic Transactions Act of 1999, and Electronic Signatures in Global and National Commerce Act, of 30th June 2000; the Indian

Information Technology Act, 2000 (No. 21 of 2000) of 9th June, 2000. Moreover, International Organization also enacted treaties that legalized the use of digital or other form of electronic signature, this includes the UNCITRAL Model Law on Electronic Signatures with Guide to Enactment 2001, which legalized the use of digital and other forms of electronic signature. In East Africa, Parliaments of different States enacted laws that regulate the use of digital and electronic signature, such as the Electronic Transactions Act, 2015 of Tanzania, the Electronic Signatures Act, 2011 of Uganda, and the Kenya Information and Communications Act, 1998 with Amendments of 2013.

Conclusively, the history of signature in the World is long as the history of human beings on the Earth. Human beings started to append signature on clay tablet and stone even before the invention of paper documentation. The technological advancement on literature, which resulted into sophistication of writing methodologies, introduced electronical means of appending signature into a document. This developments in 20th Century, forced modern Parliaments to enact of legal instruments, which regulate, validate and enforce digital signature and other forms of electronic signature.

Law Relating to Digital Signature

This chapter examined law relating to digital signature in a comparative analysis between laws different States, such as some laws of East Africa Countries (Tanzania, Kenya and Uganda), the laws of U.S, India and International Instrument (the UNCITRAL Model Law on Electronic Signatures with Guide to Enactment 2001). The Author focused her study on laws from different jurisdictions, to examine how these laws provided for the treatment of digital signature and other forms of electronic signature; this is because laws across jurisdictions provide different legal standards, extent and consequences on the treatment of digital signature.

Digital signature

What amount to digital signature varies across laws of jurisdictions, example; in Tanzania, the law that regulate all matter pertains to electronic transactions, digital signature inclusive, is the Electronic Transactions Act, 2015. Which provides *inter alia* the treatment of digital signature in the Country to the effect that; this law recognized and validates the use of digital signature

under the umbrella of electronic signature, because the Act provides for electronic signature not digital signature *per see*. In its interpretation Section, the Act, defined digital signature in-line with electronic signature to means:

> "means data, including an electronic sound, symbol or process, executed or adopted to identify a party, to indicate that party's approval or intention in respect of the information contained in the electronic communication and which is attached to or logically associated with such electronic communication"[xxiv]

The words of this Section are to the effect that digital signature may take any form of either sounds, or symbol inform of electronic communication, which is appended or logically connected to such electronic communication. The definition of this law does not clearly establish what digital signature is, because not all electronic signature amount to digital signature. In other jurisdiction, such as Uganda, its Act distinguishes between electronic and digital signature. The Act defined the term electronic signature in the same footing, as that of Tanzanian Electronic Transactions Act, but, this law defined term digital signature to mean:

> "a transformation of a message using an asymmetric cryptosystem such that a person having the initial message and the signer's public key can accurately determine; whether the transformation was created using the private key that corresponds to the signer's public key; and whether the message has been altered since the transformation was made".[xxv]

This clearly established a demarcation of which type of signature once appended on the document, amount to digital signature and which amount to other forms of electronic signature, because not all forms of electronic signature amount to digital signature, as digital signature employs the use of asymmetric cryptography algorithm to encrypt key and decrypt key to the signature appended to the document, which is not employed in other forms of electronic signature.[xxvi]

Moreover, in Kenya the term digital signature is defined under the umbrella of "advanced electronic signature" to mean digital signature, which is different from the position adopted by Tanzania.[xxvii] However, the term electronic signature is defined on the same footing, of electronic signature as defined by provision of Tanzanian Electronic Transactions Act.[xxviii] The

study further revealed that, in U.S particularly, the Uniform Electronic Transactions Act, defined the term digital signature in-line with electronic signature, hence; standard on the same footing, as the definition adopted by the Tanzanian law.[xxix]

However, the study found out that in Indian, the definition of the term digital signature, have been interpreted in-line with asymmetric crypto system and hash function. Moreover; unlikely other laws, Indian and Ugandan laws have expounded intensive what amount to digital signature compared to other forms of electronic signature, because they have separate provisions that address intensively the two likelihood concepts.[xxx]

Hence; its Author's observation that, although digital signature falls under electronic signature; but there is a clear need for adoption of interpretation which distinguishes the two, (such as the law of Uganda and India provided), because digital signature required unique asymmetric cryptography algorithm for its application and legal validity; which is quite different compared to other forms of electronic signature.

Legal recognition and validity of digital signature

Under this aspect, laws across the World, now recognize and give due legal validity to electronic signature (digital signature inclusive), to the effect of being equivalent to the traditional handwritten signature. Moreover; it's undisputed that laws of different jurisdictions also enforce transactions, such as contract which signature is appended via electronic/digital means or device. In Tanzania the applicability of digital signature is legally recognized under provision of *Section 6(1) and 10,* of the Electronic Transactions Act, 2015 as the Act provides that;

> "…signature, statement or a document to be notarized, acknowledged, verified or made under oath, that requirement shall be deemed to be met if the electronic signature of the person authorized to perform those acts is attached to, incorporated in or logically associated with an electronic signature or a data message…" [xxxi]

This Section gives legal recognition and validity of digital signature under the broad term of electronic signature. Laws in other jurisdictions also stands on the same ground as that of

Tanzania; example is the provision of Section 3 & 14 (2), of the Electronic Signatures Act, of Uganda which provided for *e*qual treatment of signature technologies (non-discrimination), between traditional handwritten signature and electronic signature.

Kenya recognizes the use of electronic/digital signature as equivalent to traditional signature without discrimination, through the provision of Section 83P, of the Information and Communications Act, 1998 with Amendments of 2013, as the Section reads;

> "Where any law provides that information or any other matter shall be authenticated by affixing a signature or that any document shall be signed or bear the signature of any person, then, notwithstanding anything contained in that law, such requirement shall be deemed to have been satisfied if such information is authenticated by means of an advanced electronic signature affixed ...".[xxxii]

Moreover; under international arena, electronic signature is legal valid as equivalent to traditional handwritten signature, as the provision of UNCITRAL Model Law on Electronic Signatures with Guide to Enactment 2001, established that there will be equal treatment between signature technologies (meaning, signature appended through digital and other electronic means), and traditional handwritten signature.[xxxiii] In India, the law clearly established for the legal recognition an validity of electronic signature and digital signature in separate provision of the law, due to the reason that digital signature is a unique form of electronic signature, compared to other forms of electronic signature.[xxxiv]

Hence, it's Author's observation that, due to the technological advancement on the field of information and communication, many Countries adopted legislations or introduced amendments into their domestic laws, to provide for the legal recognition and validity of digital signature and other forms of electronic signature, as equivalent to traditional handwritten signature. But this legal recognition should distinguish as much as possible between what is legally recognized as digital signature and other forms of electronic signature.

Legal requirements/conditions for recognition and validity of digital signature

Laws in many jurisdictions established legal requirements, which a signature purported to be electronically or digitally appended to the data message must meet, this is because not all digital

or electronic signatures are recognized and valid under the eyes of the law. In Tanzania the law established that electronic signature in order to have legal recognition, must meet the following conditions;

> "…the requirement for an electronic signature made under subsection (1) shall be met if; (a) the method is used to identify the person and to indicate the intention of that person in relation with information communicated; and (b) at the time the method was used, that method was reliable and appropriate for the purposes for which the information was communicated..."[xxxv]

This Act established that, intention of the sender of data message, is the first cardinal rule for recognition of digital/electronic signature. And that the method of the creation must be reliable and appropriate for purpose of communication of data message. In other jurisdictions, such as Uganda, their law provided intensive details of legal requirement for the recognition of electronic signature compared to the provision set under the law of Tanzania, as the Ugandan Act provides;

> "Where the law requires a signature of a person, that requirement is met in relation to a data message if an electronic signature is used which is as reliable as was appropriate for the purpose for which the data message was generated or communicated, in light of all the circumstances, including any relevant agreement. (2)SubSection (1) applies whether the requirement referred to in that subSection in the form of an obligation or whether the law simply provides consequences for the absence of a signature. (3)An electronic signature is considered to be reliable for the purpose of satisfying the requirement referred to in subSection (1) if; (a) the signature creation data are, within the context in which they are used, linked to the signatory and to no other person; (b) the signature creation data were, at the time of signing, under the control of the signatory and of no other person; (c) any alteration to the electronic signature, made after the time of signing, is detectable;…." [xxxvi]

This Section stands on same footing, with that of Tanzania, however; this Ugandan law further provided for matter of alteration, the detection of alteration if present and integrity of date

message, which is not the case with Tanzanian law. The law in Kenya stands on the same footing with the legal requirements, as that adopted by Ugandan Electronic Signatures Act.[xxxvii]

Moreover, this requirement has been further expounded by laws of other jurisdictions, such as U.S the law provided different circumstances under which the requirement of signer's intention may be inferred. The same law further established the requirement of necessary connection between the digital signature and data message to which the claimed digital signature is appended.[xxxviii] The study found out that, the provision of UNCITRAL regarding legal requirement, stands on the same stage with the provision of Ugandan law.[xxxix]

Its Author's point of view that, legal requirement/conditions which validate, as which type of electronic signature amount to digital signature, plays an important role toward establishing a clear and accurate stand point, as to what type of signature though electronic appended to the data message amount to digital signature. This is reasoned from the fact that not all claimed electronic signature qualify as digital signature (because digital signature demands unique asymmetric cryptography composition, unlike other forms of electronic signature which don't follow this algorithm).

Obligation of party under digital/electronic signature

Laws in many jurisdiction imposes an obligation to a party who wish to rely on the conduct of electronic/digital signature, to the effect that he owes a duty to verify and prove the authentic and validity of the data message and signature appended on the document. In Tanzania the law provides that;

> "…person who relies on an electronic signature shall bear the legal consequence of failure to take reasonable steps to verify the; (a) authenticity of an electronic signature; or (b) validity of a certificate or observe any limitation with respect to the certificate where an electronic signature is supported by a certificate"[xl]

This obligation as expounded by the Tanzanian law is also reflected in the provision of *Section 7* of Uganda law to the effect that it imposes obligation to the party who relies on digital/electronic signature, as the words of the cited Section reads;

> "…a relying party shall bear the legal consequences of his or her failure to; (a) take reasonable steps to verify the reliability of an electronic signature; or (b) where an electronic signature is supported by a certificate, take reasonable steps; (i) to verify the validity, suspension or revocation of the certificate; and (ii) to observe any limitation with respect to the certificate…"[xli]

Moreover, this obligation is not only imposed by domestic laws, but it's further supplemented by international instruments such as UNCITRAL Model Law on Electronic Signatures with Guide to Enactment 2001; which provides that signatory shall exercise reasonable care to avoid unauthorized use of its signature and creation data signature, and signatory shall bear the legal consequences of its failure to satisfy this obligation.[xlii]

Extra-territorial legal recognition of digital signature

The framers of laws in many jurisdictions have put into their legislations, provisions that recognized foreign digital signature certificate and electronic signature. This validate digital/electronic signature that was appended in one jurisdiction to be used in another jurisdiction regardless of geographical boundaries. Domestic and international instruments supplement this legal position, such as UNCITRAL Model Law which provides that;

> "In determining whether, or to what extent, a certificate or an electronic signature is legally effective, no regard shall be had; (a) To the geographic location where the certificate is issued or the electronic signature created or used; or (b) To the geographic location of the place of business of the issuer or signatory. 2. A certificate issued outside [the enacting State] shall have the same legal effect in [the enacting State] as a certificate issued in [the enacting State] if it offers a substantially equivalent level of reliability…"[xliii]

This legal position is affirmed by the provision of *Section 37* of Uganda Electronic Signatures Act, 2011; to the effect that digital signature signed in other jurisdiction may have the same legally validity as that issued in Uganda, subject to certain requirements imposed by the claimed Section. Moreover; the similar legal effect on extra-juridical recognition, as such adopted by Uganda; is reflected under *Section 19* of Indian Information Technology Act, 2000; to the effect of making digital signature or other forms of electronic signature to apply globally.

Hence; its Author's observation that; digital signature and other forms of electronic signature; enjoys extra-territorial juridical application and with similar legal effect as domestic issued digital signature under laws of various jurisdictions.

Conclusively; laws relating to the treatment of digital signature and other forms of electronic signature in many jurisdictions have provisions which tends to offer similar legal jurisprudence, meaning the definition of what amount to digital signature, its legal recognition, validity and enforcement, the equivalence of digital signature to traditional handwritten signature and signatory obligation and consequences pertain to conduct under digital signature.

Hence; its Author's observation that; laws on treatment of digital signature in many jurisdiction though offers similar legal jurisprudence, however; these laws have expounded this concept in different level and extent, as in some jurisdictions their laws are very intensive and comprehensive on the subject matter (i.e. India, U.S and Uganda), while other jurisdictions have simple piece of legislation (Tanzania), which need both review and revision/amendments (*mutatis mutandis*) to comprehensively address the matter.

Protection Mechanism of Digital Signature

This chapter examined different methods which can be employed to secure protection of digital signature, from being compromised or misused or obtained through unauthorized access. These protection mechanisms ranged from legal point of view to asymmetric or physical mechanism. The protection is due to reason that there are circumstances which may invalidate digital signature, these includes; where the data message was altered after signed, then the current hash-algorithm obtained from the alteration will be different from the original hash-algorithm, because the two different data messages correspond to different hash-algorithms.

In other words, where public key (decrypt key) does not match up to the private key (encrypt key) digitally signed the contents of data message, due to any misappropriation to the original hash-algorithm decryption key.[xliv] Hence; in order to eliminate breach or misappropriation, which may render digital signature invalid; this paperwork under this chapter focus on proposed legal secure mechanism for the protection of digital signature as provided in number

of legal instruments, and other forms of mechanism which are used to secure both digital signature and data creation of digital signature.

Legal protection mechanism of digital signature.

This sub-chapter, analyzed methods which are legally used as secure to digital signature. These methods are enshrined in number of legal instruments, both domestic and international instruments. Under the law, digital signature may be protected through the concept known as "secure digital signature", which demands that in order for digital/electronic signature to be protected, the digital signature should be "uniqueness, secrecy and confidential", this means that the signature should be of its kinds for the purpose of which it was meant to be used.

This will make the intended digital signature secured and protected from breach or unauthorized access. This method is advocated under various laws, including the provision of *Section 7(a)* of the Tanzania Electronic Transactions Act, the same legal effect is under the provision of *Section 2 (1) (a)* of the Kenya Information and Communications Act, 1998 with Amendments of 2013; which advocated for uniqueness of digital signature linked to the signatory. Moreover, this method is supplemented by *Section 11*, of Uganda Act, which establish that, "the signature creation data used for signature creation is unique and its secrecy is reasonably assured."[xlv] The same effect is reflected under *Section 15 (a)*, of the India Information Technology Act, 2000. Hence, in-line with provisions of the laws from different jurisdiction; one of the protected mechanisms for securing digital signature is that it must be a personal secret, unique and confidential linked to the signatory and signatory only.

Moreover; digital signature must be created using means that; only signatory can personally maintain under his sole control, cannot be readily duplicated or compromised and confidence in nature. This method advocate for the use of "Public Key Infrastructure"; which only the signatory knows its algorithm. The mechanism applied in the creation of digital signature must be only known and accessed under the personal control of signatory only, for the purpose of protecting digital signature form unauthorized access or other misappropriation of the same.[xlvi]

This control mechanism is advocated by number of provisions of law, such as *Section 2 (1) (c)* of the Kenya Information and Communications Act, 1998 with Amendments of 2013; and *Section 7 (c) (d)* of the Tanzania Electronic Transactions Act, 2015 which provide same legal

protection mechanism. Also the provision of *Article 26,* which supplemented that digital signature should be of high level of confidentiality, for the purpose of protection of the same.[xlvii] Furthermore, *Section 11 (c)* of Uganda law, established that this personal control for the protection of digital signature, should not be readily easy to duplicate or compromised (the use of strong encryption and decryption algorithm which only signatory knows its composition). This method ensures that only signatory will have the sole maintained control of the digital signature and it's under his personal confidence.

The use of detectable algorithm methods; digital signature may also be protected through the use of algorithm which may detect if there is any misappropriation, or unauthorized access of breach of data message on creation or during transit. Because digital signature is appended on the data message, then it's logically and reasonable to protect not only the appended digital signature but also to the data message on which the claimed digital signature is appended.[xlviii] Laws in many jurisdictions, advocated the detectable protective mechanism which linked to the data message to which it relates in such a manner that any subsequent alteration, breach or unauthorized access to the data message is detectable. These laws include, the provision of *Section 7(e)* of the Tanzania Electronic Transactions Act, 2015; the provision of *Section 15 (c)* of India law which advocated for the use of not only a detective mechanism, but a mechanism under exclusive control of the signatory, as the words of the claimed Section reads;

> "…created in a manner or using a means under the exclusive control of the subscriber and is linked to the electronic record to which it relates in such a manner that if the electronic record was altered the digital signature would be invalidated…"[xlix]

Hence; one among of the protection mechanism for digital mechanism is through detectable algorithm which reveals if there is any breach of data message during the creation or on transit of the same, or any misappropriation of digital signature, and further that, if there is any breach, then; as the protection mechanism, the digital signature should be invalid.

Asymmetric and physical protection mechanism of digital signature

This category employs protection methods which are more technical and less legal, these methods include both hardware and software mechanism; this includes, the use of asymmetric

passwords, firewalls and network security, which control the access and use of digital signature, to the effect that only signatory can access and use the intended digital signature. Because these traditional passwords, firewalls and network security are administered to authorize who can lawfully access and use the restricted service.[l]

It's advised that for security purpose signatory should affix password of any kind (i.e. fingerprint, words, codes, and facial) to lock down the access of digital signature. Also these fire walls and network security are configured for the purpose of blocking any cyber-attack, which can be perpetrated for the aim of breaching or compromising the integrity of digital signature and data message upon which digital signature is appended. Thus, if fire walls can be used to block any malicious activities directed against digital signature, then digital signature will be protected. Hence, digital signature like other data message stored in cyber space may be well protected via the use of passwords, firewalls or other forms of network security against any cyber-attack.

Clearance credential requirements; moreover, digital signature system should be configured to require certain confirmation credentials, or two-factor authentication verification codes, or other login requirements to the intended recipient of data message, for the purpose of protecting digital signature against any sort of unauthorized access or use, and to ensure that only the intended signee access the contents of the documents.[li] The application of verification codes will ensure that only the intended recipient can open the data message, second this will secure the appended digital signature from any misuse due to requirement of authentic verification codes which will only be known by the sender and recipient of data message.

Digital signature certificates agencies; are people or entities who/which provide the service of creating digital signature platforms. These agencies are discharged with the function of not only offering the creation of digital signature platforms; but also maintaining and providing security measures against any sort of breach or compromise of digital signature data creation and certificate. It's undisputed that these firms or people have advanced technology and network security (using cryptographs) which can provide unquestionable protection to their client digital signature platforms. This will ultimately ensure that digital signature is duly protected against misappropriation either on creation or during transit as appended on the data

message. Example of these entities include Thales, a French Corporation, which is regarded as one of the leading multinational corporations in the World on digital systems.[lii]

These agencies are legal recognized under various laws in different jurisdictions, such as under *Section 18 & 20* of the Uganda Electronic Signature Act, 2011; also the UNICTRAL Model Law recognized this mechanism of protecting digital signature, as it provides that certificate service providers should ensure that the signature creation data are valid and have not been compromise, this obligation is for the sole purpose on protecting digital signature.[liii] In Tanzania, this protection mechanism is reflected under *Section 33-36* of the Electronic Transactions Act, 2015 to the effect that entity which engage in this service, must ensure that digital signature and digital signature certificate are under protection from any misappropriation or compromise.[liv]

Conclusively; it's argued that the effectively mechanism towards the protection of digital signature is only through the use of passwords to the effect that digital signature and other electronic signature will be secured because only the signatory will be having access digital signature credentials. However, this is without prejudice to protection offered by other protective mechanism which have been analyzed in this paperwork.

Conclusion

Digital signature, being a form of electronic signature which is different from other forms, due to application asymmetric cryptographs algorithm in its creation, provides a secure system of authentication of documents and singer's identity. Unlikely other forms of signature such as the traditional handwritten signature which is too exposed to tendency of forgery. Because a digital signature assures the recipient that the document is valid, hence free from any sorts of forgery or false information. Moreover, digital signatures serve the purpose of validating the authentication, and verification of the information contained in data message. This makes digital signature an essential aspect for creating secure business and economic environment for electronic transactions.

Moreover, the study revealed that, the treatment of digital signature and other forms of electronic signature, is more like the same in various jurisdictions, because laws from different

jurisdictions offers the same or similar legal standards on aspects such as; legal interpretation of what is digital signature, recognition, requirements and consequences on the treatment of both digital signature and electronic signature. The Author in his study, objectively examined in a comparative analysis, the provisions of laws on how and to what extents these laws provide for the treatment of digital signature. Hence; through this comparative the Author found out that the treatment of digital and other forms of electronic signature in various jurisdictions stand of the same footing.

Furthermore, its revealed that; despite security assurance presented by the use of digital signature, but this does not mean it cannot be tempered, this means that, there may be a compromise circumstances with the digital signature itself, though hacking of data creation algorithm, which create encrypt and decrypt keys which are important components used in creating digital signature, this will automatically result into forgery of digital signature. Or through alteration of contents of the documents after the appending of digital signature or on the transit of the data message from the sender to the intended receiver, although any alteration of the content will invalidating the digital signature. Moreover, it's argued that, not at all time digital signature can be used to sufficiently identify the correct sender of the data message. This is because in event of forgery of signature, then the identity of sender cannot be ascertained, as the correct and desired signer was not the one who signed the data message.

Author's Observation

It is undisputed that human beings invented and used signature, even before the technology of paper documentation was invented. It's also undeniable that the concept of signature has evolved from time to time, due to changes of circumstances and modes of production, which human beings adopted. Currently, the mode of production is technological oriented; this technological advancement facilitated the improvement in signature methodology(s), hence; brought in place digital / electronic signature, as a means of attesting authentic of the document and the identity of the signer, which is legally equivalent to traditional handwritten signature.

Moreover; it's Author's consideration that, due to advanced and rapid development of technology on information and communication sector, the current concept of electronic or digital signature will be further developed to the extent that, we shall be having automated /

automatic signature appended on data message / document. This is because the development on information communication and technology cannot be stopped nor escaped.

Bibliography

Articles

Yadav, Priyanka, Srivastava, Sindhu, & Trehan, Vani, *Digital Signature*, International Journal of Engineering and Management Sciences, Haryana, Vol 3, 2012.

Christopher, Reed, *Legally Binding Electronic Documents: Digital Signatures and Authentication*, Spring, The International Lawyers, London, Vol 35, 2001

Books

Heidi, H. Harralson, Larry, S. and Miller, *Developments in Handwriting and Signature Identification in the Digital Age*, Anderson Publishing (Elsevier), USA, 2013.

Jonathan, Katz, *Digital Signatures*, Springer, New York, 2010.

Convention & Statutes

Electronic Transactions Act, 2015 (Tanzania)

The Information and Communications Act, 1998 with Amendments of 2013. (Kenya)

Electronic Signatures Act, 2011 (Uganda)

Uniform Electronic Transactions Act of 1999 (U.S)

Electronic Signatures in Global and National Commerce Act, of 30th June 2000; the Indian Information Technology Act, 2000 (U.S)

The Information Technology Act, 2000 (India)

UNCITRAL Model Law on Electronic Signatures with Guide to Enactment 2001. (United Nations Commission on International Trade Law)

Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on Electronic Identification and Trust Services for Electronic Transactions in the Internal Market and Repealing Directive 1999/93/EC (EU)

Website

https://www.emptrust.com/blog/benefits-of-using-digital-signatures. Accessed on 18th June, 2020 at 11:12 pm

https://www.pcmag.com/encyclopedia/term/digital-signature Accessed on 19th June, 2020 at 12:06 am

https://www.yourdictionary.com/digital-signature. Accessed on 19th June, 2020 at 22:36 pm

https://legalesign.com/blog/history-of-signatures/. Accessed on 20th June, 2020 at 01:14 pm

https://www.signix.com/. Accessed on 19th June, 2020 at 20:37 pm

https://www.di-mgt.com.au/rsa_alg.html. Accessed on 21st June, 2020 at 03:22 pm

https://www.signix.com/.Accessed on 19th June, 2020 at 20:37 pm

https://www.corridorcompany.com/blog/the-importance-of-having-a-secure-digital-signature-platform. Accessed on 21st June, 2020 at 20:15 pm

https://www.forbes.com. Accessed on 22nd June, 2020 at 21:59 pm

Prof. Sunny Sun, YouTube Classroom, Accessed on 21st June, 2020 at 19:25 pm

Report

American National Standard for Financial Services, Public Key Cryptography for the Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA), Washington, DC 20036 USA, Approved: January 7, 1999.

Thesis

Jayakumar, Thangavel, *Digital Signature; Comparative Study of its Usage in Developed and Developing Countries*, Uppsala University (Unpublished Master's Thesis), 2013.

Endnotes

[i] Harralson, H. H, and Miller, S. L, *Developments in Handwriting and Signature Identification in the Digital Age*, Anderson Publishing (Elsevier), USA, 2013, pg. 61
[ii] https://www.emptrust.com/blog/benefits-of-using-digital-signatures. Accessed on 18th June, 2020 at 11:12 pm
[iii] American National Standard for Financial Services, *Public Key Cryptography for the Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA)*, Washington, DC 20036 USA, Approved: January 7, 1999.
[iv] https://www.pcmag.com/encyclopedia/term/digital-signature. Accessed on 19th June, 2020 at 12:06 am
[v] https://www.yourdictionary.com/digital-signature. Accessed on 19th June, 2020 at 22:36 pm
[vi] UNCITRAL Model Law on Electronic Signatures with Guide to Enactment 2001.
[vii] Katz, J, *Digital Signatures*, Springer, New York, 2010, pg. 15
[viii] Prof. Sunny Sun, YouTube Classroom, Accessed on 21st June, 2020 at 19:25 pm
[ix] Harralson, H. H, and Miller, S. L, *Developments in Handwriting and Signature Identification in the Digital Age*, Anderson Publishing (Elsevier), USA, 2013, pg. 55
[x] Katz, J, *Digital Signatures*, Springer, New York, 2010, pg. 18
[xi] Chapter II, under *Section 3 (1)*, of The Information Technology Act, 2000.
[xii] Priyanka, Y, Sindhu, S, & Vani, T, *Digital Signature*, International Journal of Engineering and Management Sciences, Haryana, Vol 3, 2012, pg. 2
[xiii] Katz, J, *Digital Signatures*, Springer, New York, 2010, pg. 18. And *Section 4, (3) (d),* of the Electronic Signatures Act, 2011.
[xiv] Priyanka, Y, Sindhu, S, & Vani, T, *Digital Signatur*e, International Journal of Engineering and Management Sciences, Haryana, Vol 3, 2012, pg. 2
[xv] *Section 4(3) (c) (d),* of the Electronic Signatures Act, 2011.
[xvi]Thangavel, J, *Digital Signature; Comparative Study of its Usage in Developed and Developing Countries*, Uppsala University (Unpublished Master's Thesis), 2013, pg. 24
[xvii] Reed, C, *Legally Binding Electronic Documents: Digital Signatures and Authentication*, Spring, The International Lawyers, London, Vol 35, 2001, pg. 8
[xviii] Electronic Transactions Act, 2015.
[xix] https://legalesign.com/blog/history-of-signatures/. Accessed on 20th June, 2020 at 01:14 pm
[xx] https://legalesign.com/blog/history-of-signatures/. Accessed on 20th June, 2020 at 01:14 pm
[xxi] https://www.signix.com/. Accessed on 19th June, 2020 at 20:37 pm
[xxii] https://www.di-mgt.com.au/rsa_alg.html. Accessed on 21st June, 2020 at 03:22 pm
[xxiii] https://www.signix.com/. Accessed on 19th June, 2020 at 20:37 pm
[xxiv] *Section 3,* of the Electronic Transactions Act, 2015.
[xxv] *Section 2,* of the Electronic Signatures Act, 2011.
[xxvi] *Section 3(1),* of The Information Technology Act, 2000.
[xxvii] *Section 2 (1),* of the Information and Communications Act, 1998 with Amendments of 2013.
[xxviii] *Section 2,* of the Information and Communications Act, 1998 with Amendments of 2013.
[xxix] *Section 2,* of the Uniform Electronic Transactions Act of 1999.
[xxx] *Section 3(2),* of The Information Technology Act, 2000.
[xxxi] *Section 10 (a),* of Electronic Transactions Act, 2015.
[xxxii] *Section 83P,* of the Information and Communications Act, 1998 with Amendments of 2013.
[xxxiii] *Section 3,* of UNCITRAL Model Law on Electronic Signatures with Guide to Enactment 2001.
[xxxiv] *Section 5,* of the Information Technology Act, 2000.

[xxxv] *Section 6 (2)*, of the Electronic Transactions Act, 2015.
[xxxvi] *Section 4*, of the Electronic Signatures Act, 2011.
[xxxvii] *Section 83O*, of the Information and Communications Act, 1998 with Amendments of 2013.
[xxxviii] *Section 7*, of the Uniform Electronic Transactions Act of 1999.
[xxxix] *Section 6*, of UNCITRAL Model Law on Electronic Signatures with Guide to Enactment 2001.
[xl] *Section 12*, of the Electronic Transactions Act, 2015.
[xli] *Section 5 & 7*, of Electronic Signatures Act, 2011.
[xlii] *Article 8 & 11*, of UNCITRAL Model Law on Electronic Signatures with Guide to Enactment 2001.
[xliii] *Article 12*, of UNCITRAL Model Law on Electronic Signatures with Guide to Enactment 2001
[xliv] Priyanka, Y, Sindhu, S, & Vani, T, *Digital Signature*, International Journal of Engineering and Management Sciences, Haryana, Vol 3, 2012, pg. 3
[xlv] The Electronic Signatures Act, 2011.
[xlvi] Katz, J, *Digital Signatures*, Springer, New York, 2010, pg. 18
[xlvii] Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on Electronic Identification and Trust Services for Electronic Transactions in the Internal Market and Repealing Directive 1999/93/EC.
[xlviii] *Section 7 (e)* of the Electronic Transactions Act, 2015. The same legal effect is under *Section 11(d)* of the Electronic Signatures Act, 2011.
[xlix] The Information Technology Act, 2000.
[l] https://www.corridorcompany.com/blog/the-importance-of-having-a-secure-digital-signature-platform. Accessed on 21st June, 2020 at 20:15 pm
[li]https://www.corridorcompany.com/blog/the-importance-of-having-a-secure-digital-signature-platform. Accessed on 21st June, 2020 at 20:15 pm
[lii] https://www.forbes.com. Accessed on 22nd June, 2020 at 21:59 pm
[liii] *Article 9 (d) (ii)*, of UNCITRAL Model Law on Electronic Signatures with Guide to Enactment 2001.
[liv] The Electronic Transactions Act, 2015.