LEGAL ISSUES ON ADMISSIBILITY OF ELECTRONIC SIGNATURES UNDER THE ELECTRONIC SIGNATURES ACT IN UGANDA'S CIVIL PROCEEDINGS

Paul Mukiibi*

ABSTRACT

The Electronic Signatures Act (ESA), 2011 has been in force for more than one decade now. It is an Act to make provision for and to regulate the use of electronic signatures and to provide for other related matter. There are concerns, however, whether documents signed electronically under this Act can be admissible in evidence. Specific attention has been put on affidavits and statutory declarations which require physical presence of a deponent or declarant before a commissioner for oaths, notary public or justice of peace. Accordingly, this article examines the challenges associated with e-signatures in civil proceedings. The article concludes that e-signatures have been embraced globally and are applied with principles of non-discrimination, technological neutrality and functional equivalence. Despite this, e-signatures are faced with challenges of parallel existing laws requiring physical presence and writing of a signature in the presence of an authorised officer. This happens during notarising, commissioning, attesting and sealing of such documents. Other challenges relate to absence of adequate public key infrastructure to manage the system, electronic print against handwritten print and the nature of an electronic signature under the ESA. The article recommends harmonizing laws governing admissibility of evidence in civil proceedings with ESA, technological infrastructure improvement, training efficient and reliable human resource infrastructure, use of password and hybrid methods to enhance security of the signature, licence more public key infrastructure and certification services providers, use of biometrics to safeguard the system, video witnessing of signatures, amending legislation that is incompatible with modern technology and training and sensitization facilities of all the stakeholders.

* MITPL (UMU); MBA (UMI); LLM (Mak); PG.Dip LP (LDC); LLB (Mak). Head, Department of Law Reporting, Research and Law Reform LDC; Lecturer LDC; and Part-Time Lecturer, Kyambogo University. Advocate; Commissioner for Oaths; and Notary Public. E-mail: pmukiibi@ldc.ac.ug

INTRODUCTION

In 2011, Parliament of Uganda enacted the Electronic Signatures Act (ESA).[1] This Act was assented by the President of the Republic of Uganda on 17 February 2011[2] and came into force on 18 March 2011.[3] The ESA among others was enacted to make provision for and to regulate the use of electronic signatures and to provide for other related matters.[4] Prior to this Act, signatures in any legal proceedings and transactions were only deemed authentic if they appeared in manual and physical form of a person or persons appending such signatures. Simply put, electronic signatures were not admissible under the law as they had no enabling law to enforce them. Reliance on admissibility of evidence was majorly governed by the Evidence Act of Uganda which provided no room for electronic signatures.[5]

With the coming into force of ESA, it was hoped that appending signatures on legal documents would become more easier especially on categories of persons who are very far, or outside jurisdiction and their evidence is very critical in specific legal proceedings. Indeed, the legislator intended to avoid wastage of time and costs to have a person physically append a signature on a particular document and manually transport the document to the destination it is needed to be relied upon in evidence in legal proceedings. Consequently, legal documents like tenancy agreements, mortgages, land sale and purchase agreements, powers of attorney, witness statements, among others can pass the test of validity if they conform to the provisions of the ESA.[6]

Although the ESA came into force in 2011 and prior to the declaration of Covid-19 as a global pandemic by the World Health Organisation (WHO), on 18th March 2020, the Government of Uganda (GOU), through the Office of the President, announced a series of public health measures to prevent the spread of Covid-19 across the country.[7] This ushered in the first lockdown in the country since the declaration of Covid-19, a global pandemic by the WHO. The same announcement was repeated on 18th June 2021 which ushered in a second lockdown.[8] Of concern

[1] Act No. 7 of 2011.
[2] See Date of Assent in the Act itself.
[3] The Act commenced on 18 March 2011. See The Uganda Gazette No. 19 Volume CIV dated 18 March 2011. Printed by UPPC, Entebbe, by Order of the Government.
[4] See the Long title to ESA.
[5] The Evidence Act Cap. 6, Laws of Uganda came into force on the 10th day of December 1963. Electronic evidence in Uganda then was unheard of.
[6] See Sec. 4 (3) of the ESA on reliability of an electronic signature.
[7] *See* for e.g., COVID-19 Guidelines for mass gatherings, available at <www.COVID-19-GUIDELINES-FOR-MASS-GATHERINGS.pdf> (accessed 26 November 2021); Africa News, Uganda imposes another lockdown: What are the restrictions? 7 June 2021, available at <https://www.africanews.com/2021/06/07/uganda-imposes-another-lockdown-what-are-the-restrictions> (accessed 26 November 2021).
[8] *Ibid.*

to this article is that electronic signatures applied so much on legal documents as they were considered among the protective measures to avoid the spread of the pandemic, despite the fact that very few Ugandans can use this kind of technology. This among other concerns justifies the relevance of the legislation which perhaps the legislator had not thought about in 2011.

At the coming into force of ESA, there were other laws governing evidence in Uganda's civil procedure, specifically, the Evidence Act;[9] the Oaths Act, Cap 19;[10] the Statutory Declarations Act, Cap 22;[11] and the Civil Procedure Rules, SI.71-1.[12] These legislations are still in force notwithstanding the coming into force of the ESA. Some of these laws for example require a deponent or declarant to append his or her signature on an affidavit or declaration as proof that he or she made such an affidavit or declaration.[13] The requirement goes further to demand such a deponent or declarant to do so before a commissioner for oaths or a person authorised under the law to administer oaths in Uganda.[14] This in itself may require physical presence of the deponent or declarant before such a commissioner for oaths and the presumption of the law is that such a person appends his or her signature physically before the commissioner for oaths or the officer authorised to administer oaths under the law.[15] This brings in context concerns as to whether or not the framers of the ESA had in mind that affidavits and statutory declarations are legal documents and whether the same can be subjected to the provisions of the ESA.

In civil and common law countries, the enforceability of many types of contracts is subject to certain formalities. The most common formality is the requirement of a contract reduced in writing signed by the parties to it. In Uganda as in other commonwealth jurisdictions written contracts would necessitate signification of agreement. Furthermore, the witnessing of that signification is also desired. Such signification is generally manufactured in terms of personified marks such as signatures and seals. Further proof by witnesses is desired.

The above concerns give rise to legal issues as to whether an affidavit or declaration can be made electronically or subjected to electronic signature under the ESA when the law requires the deponent or declarant to physically appear before the officer administering the oath before signing the said affidavit. Against this backdrop, this article critically examines the legal issues surrounding admissibility of electronic signatures under the ESA in Uganda's civil proceedings.

---

[9] Cap. 6, Laws of Uganda

[10] Sec. 5 (1) of the Act gives the way an oath can be taken. The third schedule gives a form of a jurat that is made by the officer administering the oath and must state that the deponent or declarant appeared before him or her.

[11] Sec. 5 (1) of the Act requires a judge, the registrar, a magistrate, or a justice of the peace, a notary public and any commissioner for oaths to take and receive the statutory declaration of any person voluntarily making it before him or her and shall certify it under his or her signature. See also Sec. 6 (1) & (2) regarding taking out statutory declarations outside Uganda.

[12] S.I. 71-1 (as amended by S.I. NO. 33/2019).

[13] *Supra at 12*.

[14] *Ibid.*

[15] *Ibid.*

It analyses the inception of e-signatures in Uganda, challenges associated with use of e-signatures in Uganda's civil proceedings and measures to improve the use of e-signatures in Uganda's civil proceedings.

The article is presented under the following themes: (a) electronic evidence, electronic signatures and digital signatures; (b) admissibility of electronic signatures; (c) effectiveness of electronic signatures; (d) international, regional and domestic instruments on electronic signatures; (e) a review of court decisions on the authenticity of electronic signatures; (f) challenges associated with electronic signatures; and (g) recommendations.

2. ELECTRONIC EVIDENCE, ELECTRONIC SIGNATURES AND DIGITAL SIGNATURES

2.1. Electronic Evidence

Different jurisdictions have attempted to define electronic evidence, however, there is no specific definition per se. Some precepts defining the term, however, exist. The Finnish legal Proceedings Code refers to it as "deeds that support action,"[16] meaning both the digital support and the paper support. A more direct reference exists in the Police & Criminal Evidence Code of the United Kingdom: "evidence is all information contained in a computer."[17] This equally does not give a precise definition of the term.

George and Stephen Mason define electronic evidence as all information with probative value that is included in an electronic media or is transmitted by media.[18] They further give an expansive definition as data (comprising the output of analogue devices or data in digital form) that is manipulated, stored or communicated by any manufactured device, computer or computer system or transmitted over a communication.[19]

Electronic evidence is derived from electronic devices such as computers and their peripheral apparatus, computer networks, mobile telephones, digital cameras and other portable equipment (including data storage devices), as well as from the internet. The information it contains does not possess an independent physical form.[20]

However, in many ways, electronic evidence is no different from traditional evidence in that the party introducing it into legal proceedings must be able to demonstrate that it reflects the same set of circumstances and factual information as

[16] Legal Proceedings code of Finland. Chapter 17, Section 11b.
[17] Police and Criminal Evidence Act, PACE, United Kingdom.
[18] Electronic Evidence, George, Madson University of London Press, Institute of Advanced Legal Studies, 2017. Available at https://www.jstor.org/stable/j.ctv512x65 accessed on 09 June 2022.
[19] *Ibid.*
[20] Electronic Evidence Guide. A Basic Guide for Police Officers, Prosecutors and Judges. European Union, 2014. p. 11.

it did at the time of the offence.[21]

In other words, they must be able to show that no changes, deletions, additions or other alterations have (or might have) taken place. The intangible nature of any data and information stored in electronic form makes it much easier to manipulate and more prone to alteration than traditional forms of evidence. This has created special challenges for the justice system which requires that such data be handled in a special way to ensure the integrity of the evidence it offers.[22]

Given its special characteristics, electronic evidence could be defined as: any information generated, stored or transmitted in digital form that may later be needed to prove or disprove a fact disputed in legal proceedings.[23]

In Uganda, the term is neither defined under the ESA nor the Electronic Transactions Act.[24] Courts of record have however, attempted to define the term electronic evidence. *Justice Margaret Mutonyi* in the case of *Amongin Jane Francis Okili Vs Lucy Akello and The Electoral Commission*[25] has defined electronic evidence as any probative information stored or transmitted in digital form that a party at a trial or proceeding may use. It is used to prove a particular proposition or to persuade court of the truth of an allegation.

2.2. Electronic Signatures

In the network environment, e-government and e-commerce are dependent on electronic documents and signatures as the foundation of electronic communications and transactions. In order to encourage the development of digital economic activity, the norm for legal electronic documents and signatures according to the Law of E-Signature is required. Legitimizing e-signature to set up a safe and authentic environment for electronic transactions that incorporate e-commerce applications has become a global issue.[26] Nowadays, the technology of e-signature can be applied to purchase on the internet, distance education, web entertainments, and internet finance such as the electronic trading of stocks and bonds.

An e-signature consists of e-signature image and digital signature. E-signature is generally associated with a number of technologies, allows a person (or machine) to electronically mark a document,[27] and can enable innovative document management processes.[28] In other words, e-signature provides electronic

[21] *Ibid.*
[22] *Ibid.*
[23] *Ibid.*
[24] Act No. 8 of 2011.
[25] HCT-02-CV-0001-2014. Available at https://ulii.org/ug/judgment/election-petitions/2015/1 accessed on 09 June 2022.
[26] MOEA Electronic Signatures Act, Ministry of Economic Affairs, R.O.C. 2002. http://www.esign.org.tw/English.asp Accessed on 09 June 2022.
[27] Nunnally J.C. 2nd ed. McGraw-Hill; New York: 1978. Psychometric Theory. [Google Scholar]
[28] Nunno R.M. Electronic signatures: technology developments and legislative issues. *Government Information Quarterly.* 2000;17(4):395–401. [Google Scholar]

authentication and a process to verify the identity of users with a stand-alone mainframe, network, or internet-based system to control access or authorize transactions.[29]

There are many forms of e-signature. Benjamin Wright, a noted e-commerce attorney and co-author of The Law of Electronic Commerce, concluded that "How, where, and when e-signatures are used requires the same care and common sense that one would apply to the use of pen and ink signatures".[30] In many states and industry sectors of the US, e-signatures attached to electronic records (documents created, stored, generated, received, or communicated by electronic means) are legally recognized in the same manner as handwritten signatures on paper.[31]

The term "electronic signature" is defined under the ESA to mean data in electronic form affixed to or logically associated with a data message, which may be used to identify the signatory in relation to the data message and indicate the signatory's approval of the information contained in the data message; and includes an advance electronic signature and the secure signature.[32]

The ESA further defines "electronic signature product" to mean configured hardware or software or relevant components of it, which are intended to be used by a certification service provider for the provision of electronic signature services or are intended to be used for the creation or verification of electronic signatures.[33]

On the other hand, "advanced electronic signature" is defined both under the ESA[34] and Electronic Transactions Act[35] to mean an electronic signature, which is: (a) uniquely linked to the signatory; (b) reliably capable of identifying the signatory; (c) created using secure signature creation device that the signatory can maintain under his sole control; and (d) linked to the data to which it relates in such a manner that any subsequent change of the data or the connections between the data and signature are detectable.

2.3. Digital Signatures

The ESA defines a "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: (a) whether the transformation was created using the private key that corresponds to the signer's public key; and (b) whether the message has been altered since the transformation

[29] Poon P., Wagner C. Critical success factors revisited: success and failure cases of information systems for senior executives. *Decision Support Systems.* 2001; 30:393–418. [Google Scholar]

[30] Premkumar G., Ramamurthy K. The role of interorganizational and organizational factors on the decision mode for adoption of interorganizational systems. *Decision Sciences.* 1995;26(3):303–336. [Google Scholar]

[31] Premkumar G., Roberts M. Adoption of new information technologies in rural small business. *Omega.* 1999;27(4):467–484. [Google Scholar]

[32] See Sec. 2 of the ESA.

[33] *Ibid.*

[34] *Ibid.*

[35] See Sec. 2 of the Act.

was made.[36]

Digital signatures involve the use of the hash function. A digital signature permits signing a message in order to enable detection of changes to the message contents, to ensure that the message was legitimately sent by the expected party, and to prevent the sender from denying that he or she sent the message, known as nonrepudiation. To digitally sign a message, the sender would generate a hash of the message, and then use his private key to encrypt the hash, thus generating a digital signature. The sender would then send the digital signature along with the message, usually by appending it to the message itself.[37]

When the message arrives at the receiving end, the receiver would use the sender's public key to decrypt the digital signature, thus restoring the original hash of the message. The receiver can then verify the integrity of the message by hashing the message again and comparing the two hashes. Although this may sound like a considerable amount of work to verify the integrity of the message, it is often done by a software application of some kind and the process typically is largely invisible to the end user. A digital signature is considered legally binding and if it is lost or stolen must be revoked.[38]

Digital signatures are very different from the handwritten signatures used on paper. Because data on a computer can be easily copied, an image of a person's written signature could be cut and pasted into a new document, making signature forgery a simple task. A different type of signature had to be designed for the digital realm.[39]

Digital signatures can provide data integrity, authentication, and support for nonrepudiation. After a message has been signed, it cannot be modified without being detected. A valid digital signature can only be created by the original signer (i.e., cannot be forged) and thus can prove who signed the message. While signature creation relies on private information, signature verification must be possible with public information. The signer cannot later deny signing the message.[40]

In today's digital world, the average person doesn't think twice about using electronic signatures, however, the position for practitioners like attorneys is different. Attorneys should be more cautious with electronic signatures. Over the past 20 years, electronic signature use has been on the rise globally. Due to their convenience, they are now used daily in myriad contracts and agreements. Practitioners, however, should consider the applicable statutes and practical downsides to using electronic signatures. Electronic signatures present unique issues in litigation. For example, an electronic signer can more easily deny that he

[36] Sec. 2 of the ESA.

[37] Jason Andress, in The Basics of Information Security (Second Edition), 2014 https://www.sciencedirect.com/topics/computer-science/digital-signature. Accessed on 09 June 2022

[38] *Ibid.*

[39] Jeff Gilchrist, in:
Encyclopedia of Information Systems, 2003, https://www.sciencedirect.com/topics/computer-science/digital-signature. Accessed on 9 June 2022

[40] *Ibid.*

actually signed the document. And it may be difficult to determine how to lay proper foundation for an electronic signature.

In the next section, the article examines the admissibility of electronic signatures and examines the burden of proof in proving the validity of such a signature.

3. ADMISSIBILITY OF ELECTRONIC SIGNATURES

Consider this common question: how will an electronic signature hold up if challenged in court? After all, electronic signatures are becoming a vital business tool in today's remote environment and people want to know if they end up in litigation that the authenticity of an e-signature can be proved like a traditional wet signature. Authenticity is easier to prove, in fact, thanks to built-in digital audit trails. In disputes over agreements, courts are sometimes charged with establishing whether a signature is valid and attributing it to the signer, based on an evidentiary burden of proof. A digital audit trail does that brilliantly and in a way that other methods can't touch, because the data captured around an electronic signature provides more concrete evidence around the authenticity of someone's signature, and thereby their obligations under a contract, making it easier to meet the burden of proof.[41]

Practitioners thus need to check local rules regarding the use of electronic signatures to avoid potential sanction. In December 2016, a bankruptcy judge for the Eastern District of California imposed sanctions on a bankruptcy lawyer for permitting a debtor client to use DocuSign to sign documents requiring an original signature. In *Re Mayfield*,[42] the bankruptcy attorney submitted various documents which the debtor had signed using DocuSign. The United States Trustee argued that DocuSign did not constitute an original ("wet") signature as required under the applicable bankruptcy and local rules. The court noted its concerns that an electronic signature could be more easily forged, or placed by someone other than the debtor, leading to potential disputes over the validity of critical case documents.[43] The essential point is that an individual's handwritten signature is less easily forged than any form of software-generated electronic signature, and the presence of forgery is more easily detected and proven.

Typically for wet signatures, validity and attribution are established by comparing copies of signatures and presenting testimony from handwriting experts or witnesses who were present at the signing. Not only is this expensive and time

[41] Tyler Newby, Partner at Fenwick & West LLP does a fantastic job outlining just how valuable audit trails are in authenticating e-signatures in court in his article, "Using E-Signatures in Court—The Value of an Audit Trail." Available at https://www.fenwick.com/publications/Pages/Using-E-Signatures-in-Court-The-Value-of-an-Audit-Trail.aspx (accessed on 5 August 2022).

[42] [2016] WL 3958982, No. 16-22134-D-7.

[43] Available at https://www.govinfo.gov/content/pkg/USCOURTS-caeb-2_16-bk-22134/pdf/USCOURTS-caeb-2_16-bk-22134-0.pdf (accessed on 5 August 2022).

consuming but also less reliable due to the human element. By removing the chance for human error and automating the entire data capturing process, audit trails make it easier to establish authenticity and address disputes over signatures in courts of law.

In his article, Newby outlines a variety of cases where audit trails were effective in establishing a signatory because of information they contain. Data establishing IP addresses, date, time and location for when a contract was received, viewed and signed has proven particularly relevant to establishing signature authenticity.[44] One state case that Tyler cited, *IO Moonwalkers, Inc. v. Bank of America*,[45] went as far as to say that the DocuSign system established an electronic trail of information (send, receipt, signature, review) that wasn't available before the digital age and is a more credible method of establishing evidence than a sworn statement of whether an agreement was sent via mail.

All audit trails are not created equal, so how the audit trail is set up is crucial. If done right, there's an amazing amount of case law to support their admissibility in court. The DocuSign eSignature audit trail includes all the components mentioned in the case law and follows a secure and documented process necessary for court admissibility. This includes inter alia: a complete, automated history of every viewing, printing, sending, signing or declining activity, including key event timestamps; Identifying data, such as the signer's IP address or officially affiliated email address; Geolocation of signers, if they agree to share that information; A tamper-evident seal that validates documents haven't been altered outside of each signing event; A court-admissible certificate of completion available to all participants in the transaction; Multiple levels of authentication based on email, access code, SMS, phone, geo-location, among others.[46]

DocuSign also takes a security-first approach to e-signatures to ensure all audit trails, certificates of completion and customer documents that flow through the DocuSign Agreement Cloud stay safe, secure and unaltered before, during and after signing.[47]

In the next section, the study examines the legal purpose of a signature and what makes it effective in civil transactions and proceedings.

4. EFFECTIVENESS OF ELECTRONIC SIGNATURES

A manuscript signature is accepted without question as legally effective in all jurisdictions, assuming it has not been procured by fraud, and it is rarely asked

[44] *Ibid*

[45] [2018] 814 S.E.2d 583.
Available at https://www.courtlistener.com/opinion/4483402/io-moonwalkers-inc-v-banc-of-am-merch-servs/ (accessed on 5 August 2022).

[46] Available at https://www.docusign.com/trust/security/product-security (accessed on 5 August 2022).

[47] *Ibid*

what effects such a signature is required by law to achieve. However, in those cases where the validity of alternatives has been considered, other methods of signing a document, such as signature by means of a printed or rubber stamp facsimile, have been assessed for validity. The most common approach is to define the functions that a signature must perform, and then to treat signature methods that affect those functions as valid signatures. The primary function of a physical signature is to provide evidence of three matters: the identity of the signatory; that the signatory intended the signature to be his signature and that the signatory approves of and adopts the contents of the document.

Manuscript signatures meet these functional requirements in a number of ways. Identity is established by comparing the signature on the document with other signatures that can be proved, by extrinsic evidence, to have been written by the signatory. The assumption is that manuscript signatures are unique, and that, therefore, such a comparison is all that is necessary to provide evidence of identity. In practice, manuscript signatures are usually acknowledged by the signatory once they are shown to him, and extrinsic evidence is only required where it is alleged that the signature has been forged.

Also, intention to sign is normally presumed because the act of affixing a manuscript signature to a document is universally recognized as signing. Intention to sign is normally only disputed where the affixing of the signature has been procured by fraud, and in those cases the signatory bears the burden of displacing the presumption that he intended to sign. Intention to adopt the contents of the document is similarly presumed because it is general knowledge that affixing a manuscript signature to a document has that effect. In both cases, the burden of displacing the presumption is on the signatory.[48] The following explanation has been offered by the Sri Lankan Ministry of Justice:

> In the context of Internet communications, the thing to be signed, an electronic document, exists more as a matter of metaphysics than as a physical object. For this reason, it is very difficult for an electronic signature method to meet any physical requirement of form.[49] For example, some of the English cases and statutes on physical world signatures appear to state that a signature must take the form of a mark on a document.
>
> An electronic signature, by itself, cannot provide sufficient evidence of the signatory's identity. To explore this matter further, evidence is required that links the signature key or other signature device to the signatory himself. But the

[48] Ministry of Justice, Sri Lanka, 'Electronic Signatures – Perspectives and Problems', available at:

https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwiomYuJ15qAAxXL6aQKHf2cDZsQFnoECAgQAQ&url=https%3A%2F%2Fwww.lawnet.gov.lk%2Felectronic-signatures-perspectives-and-problems%2F&usg=AOvVaw2c89cR8a0VHtTtrB-dxOSm&opi=89978449

[49] See, e.g., *Saunders v. Anglia Bldg. Society* [1971] AC 1004.

> recipient wishes to be able to rely on the signature without needing to collect evidence for use in the unlikely event that the signature is disputed. For this reason, most electronic signatures used for e-commerce communications are likely to be accompanied by an ID Certificate issued by a Certification Authority. The Certification Authority takes traditional evidence of identity, for example, by examining passports, and, in the case of public key encryption digital signatures, checks that signatures effected with the signatory's secret key are verifiable using the public key. Once the Certification Authority is satisfied as to the signatory's identity, it issues an ID Certificate, which includes, inter alia, a certification of the signatory's identity and of his public key. This certificate may be used by the recipient to prove the signatory's identity.
>
> It is useful to look at how analog "wet ink" signatures are authenticated in court when, for example, a party attempts to show that the scribble on a signature block is the signature of another party. If contested, parties typically have used comparisons between known signatures and the questioned signature with corroborating witness testimony that a separate individual saw the signing of the document or the testimony of handwriting experts confirming the similarity of the signatures. All the proponent needs to produce is "sufficient" evidence that the signature is that of the other party; questions as to the strength of that evidence will go to the weight the fact finder gives the evidence in court.
>
> E-signatures backed by an audit trail help clear this low authenticity bar even more easily. Audit trails are digital records maintained by the e-signature service that, among other things, identify when a document was sent, opened and signed, as well as the names, email addresses and unique signing identifiers of the signatories. They also may include records like IP addresses or machine IDs to further trace when and where a document was opened and signed.[50]

In the next section, this article examines the international, regional and domestic instruments governing admissibility of e-signatures in different jurisdictions.

5. INTERNATIONAL, REGIONAL AND DOMESTIC INSTRUMENTS ON E-SIGNATURES

International trade has evolved over the years with electronic commerce taking centre stage in how international business is conducted. The use of electronic signatures has streamlined international trade by reducing the time involved to exchange physical documents signed by parties to a global business transaction. Clearly, the legal validity of electronic signatures is of international importance since no progress can be made in developing the legal institutions needed for conducting international electronic commerce without unique or identical

[50] Supra (n 48).

definitional frameworks. Electronic commerce's exceptional success will depend more on facilitating and encouraging trade between unknown parties in different jurisdictions than on interactions between known parties, whether within the same jurisdiction or not. The study hereunder examines some of the global, regional and domestic instruments in place to enforce e-signatures.

5.1. United Nations Model Law of Electronic Commerce, 1996

In 1996, the United Nations adopted a Model Law on Electronic Commerce (MLEC) to provide a common policy structure for nations in the drafting of their e-commerce statutes. It is important to note that this was just a guideline and nations had to complement it with comprehensive rules and regulations in order to achieve its implementation. It has had a profound impact on the evolution of international e-commerce law, including definitions, variation by agreement, legal recognition and admissibility of electronic form, incorporation by reference in e-contracts, use of electronic signatures, carriage contracts among others.

The MLEC had many consequences. It approved the use of electronic signatures, claimed that electronic signatures would have the same legal impact as ink signatures and remained technologically neutral, i.e., did not mandate the utilization of any specific type of technology. They also came up with a Model Law on Electronic Signatures (MLES) in 2001 to provide a standard model structure for nations to use when writing their e-signature laws.

The MLES is based on the fundamental principle underpinning Article 7 of the UNCITRAL Model Law on Electronic Commerce with regard to the fulfilment of the signing function in an electronic environment by a technologically neutral approach, which avoids promoting the use of any particular technology or process.

A signature, whether electronic or on paper, is primarily a symbol which signifies intent. Thus, the Standard Commercial Code definition of "signed" includes "any symbol" so long as it is "executed or adopted by a party with the present purpose of authenticating a written document.

Many attempts have been made by the United Nations Commission on International Trade Law to strengthen the quality of these legal rules by adopting model legislation which countries can use as a reference when developing their own legislation. In generating electronic records, the MLEC promotes principles of non-discrimination, technological freedom and functional equivalence. The concept of non-discrimination is at the core. The law ensures that a document is not denied legal meaning, validity or enforceability solely on the grounds that it is in electronic form.

More than 70 nations have embraced the 1996 Model Law on Electronic Commerce (MLEC), and over 30 countries have implemented the 2001 Model Law on Electronic Signatures (MLES). A legally binding treaty was also signed by 18 countries, the 2005 United Nations Convention on the Use of Electronic Media in Foreign Contracts. Regional legal gaps in electronic signature regulations exist for cross-border traders. When states are using the U.N. Model Laws, their respective

governments may choose to implement the elements they like and discard the others. This creates serious uncertainties and makes the system unpredictable.

5.2. United Nations Convention on the Use of Electronic Communications in International Contracts (New York, 2005)

This was adopted on 23 November 2005 and came into force on 1 March 2013. The Electronic Communications Convention aims at facilitating the use of electronic communications in international trade by assuring that contracts concluded and other communications exchanged electronically are as valid and enforceable as their traditional paper-based equivalents.

Certain formal requirements contained in widely adopted international trade law treaties, such as the Convention on the Recognition and Enforcement of Foreign Arbitral Awards (the "New York Convention") and the United Nations Convention on Contracts for the International Sale of Goods (CISG) may pose obstacles to the wide use of electronic communications. The Electronic Communications Convention is an enabling treaty whose effect is to remove those formal obstacles by establishing equivalence between electronic and written form. Moreover, the Electronic Communications Convention serves additional purposes further facilitating the use of electronic communications in international trade. Thus, the Convention is intended to strengthen the harmonization of the rules regarding electronic commerce and foster uniformity in the domestic enactment of UNCITRAL model laws relating to electronic commerce, as well as to update and complement certain provisions of those model laws in light of recent practice. Finally, the Convention may provide those countries not having yet adopted provisions on electronic commerce with modern, uniform and carefully drafted legislation.

The Convention builds upon earlier instruments drafted by the Commission, and, in particular, the UNCITRAL Model Law on Electronic Commerce and the UNCITRAL Model Law on Electronic Signatures. These instruments are widely considered standard legislative texts setting forth the three fundamental principles of electronic commerce legislation, which the Convention incorporates, namely non-discrimination, technological neutrality and functional equivalence.

The Convention applies to all electronic communications exchanged between parties whose places of business are in different States when at least one party has its place of business in a Contracting State.[51] It may also apply by virtue of the parties' choice. Contracts concluded for personal, family or household purposes, such as those relating to family law and the law of succession, as well as certain financial transactions, negotiable instruments, and documents of title, are excluded from the Convention's scope of application.[52]

[51] See Art. 1 of the Convention
[52] *Id.* Art. 2

As noted above, the Convention sets out criteria for establishing the functional equivalence between electronic communications and paper documents, as well as between electronic authentication methods and handwritten signatures.[53] Similarly, the Convention defines the time and place of dispatch and receipt of electronic communications, tailoring the traditional rules for these legal concepts to suit the electronic context and innovating with respect to the provisions of the Model Law on Electronic Commerce.[54]

Moreover, the Convention establishes the general principle that communications are not to be denied legal validity solely on the grounds that they were made in electronic form.[55] Specifically, given the proliferation of automated message systems, the Convention allows for the enforceability of contracts entered into by such systems, including when no natural person reviewed the individual actions carried out by them.[56] The Convention further clarifies that a proposal to conclude a contract made through electronic means and not addressed to specific parties amounts to an invitation to deal, rather than an offer whose acceptance binds the offering party, in line with the corresponding provision of the CISG.[57] Moreover, the Convention establishes remedies in case of input errors by natural persons entering information into automated message systems.[58]

Finally, the Convention allows contractual parties to exclude its application or vary its terms within the limits allowed by otherwise applicable legislative provisions (Art. 3).[59] Moreover, States may also consider adopting the provisions of the Convention at the domestic level. Such decision would promote uniformity, economizing on judicial and legislative resources as well as further increasing certainty in commercial transactions, especially in light of the diffusion of mobile devices for electronic transactions. It is particularly recommended for those jurisdictions that have not yet adopted any legislation on electronic commerce. Otherwise, purely domestic communications are not affected by the Convention and will continue to be governed by domestic law.

5.3. Regulation (EU) No 910/2014 of the European Parliament and Council, 2014

This Regulation was passed pursuant to Article 114 of the Treaty on the Functionality of the European Union on 23 July 2014. The Regulation is on electronic identification and trust services for electronic transactions in the internal market and it repealed Directive 1999/93/EC.[60]

The Regulation establishes a legal framework for electronic signatures,

[53] *Ibid.* Art. 9
[54] *Ibid.* Art. 10
[55] *Ibid.* Art. 8
[56] *Ibid.* Art. 12
[57] *Ibid.* Art. 11
[58] *Ibid.* Art. 14
[59] *Ibid.* Art. 3
[60] Regulation (EU) No 910/2014 of The European Parliament and of The Council, 2014

electronic seals, electronic time stamps, electronic documents, electronic registered delivery services and certificate services for website authentication.[61] The Regulation further gives the legal effect of electronic signatures. Article 25 (1) provides as follows:

> An electronic signature shall not be denied legal effect and admissibility as evidence in legal proceedings solely on the grounds that it is in an electronic form or that it does not meet the requirements for qualified electronic signatures.[62]

The regulation also places an electronic signature on the same footing with a handwritten signature. Article 25 (2) provides as follows:

> A qualified electronic signature shall have the equivalent legal effect of a handwritten signature.[63]

The Regulation harmonises the legal position on electronic signatures among all Member states to the European Union. Article 25 (3) provides as follows:

> A qualified electronic signature based on a qualified certificate issued in one Member State shall be recognised as a qualified electronic signature in all other Member States.[64]

This Regulation is very critical in guiding regional, sub-regional and national legislations on e-signatures. It clearly emphasises that an electron signature has the same legal effect with the handwritten signature. It further emphasises that an e-signature shall have the same legal effect with the handwritten signature in all member states under the European Union. The EAC and Uganda in particular can benchmark from this Regulation in enhancing and strengthening their sub-regional and national legislations on e-signatures.

5.4. National Laws

With varying degrees of flexibility, policymakers have used direct regulation, co-regulation, and self-regulation in recent decades to adapt to the growth of global information technology and e-commerce. Different states have signed and ratified various treaties relating to electronic signatures such as the Model Electronic Commerce Act, Model law on Electronic Signatures, the United Nations Convention on the Use of Electronic Communications in International Contracts, among others. Below are some of the countries that have enacted national legislation on electronic signatures.

[61] *Ibid.* Art. 1 (c)
[62] *Ibid.* Art. 25 (1)
[63] *Ibid.* Art. 25 (2)
[64] *Ibid.* Art. 25 (3)

5.4.1. United Kingdom (The Electronic Communications Act 2000)

The Electronic Communications Act 2000 is an important piece of legislation signed into law by the Parliament of the United Kingdom and went into force on March 8, 2002. The ECA has allowed the growth, expansion and use of electronic commerce services in the United Kingdom since then. The primary purpose of the Act was to help build trust in electronic commerce and the technology underlying it by providing businesses and other organizations providing cryptographic support services such as electronic services and confidentiality services with an approval scheme.

5.4.2. Australia (The Electronic Transactions Act 1999)

The Electronic Transactions Act was introduced in 1999. The existing legal provisions prior to 1999 were capable of dealing with electronic transactions but the Electronic Transactions Act 1999 was enacted to provide a more secure environment for e-commerce and the creation of electronic signatures in Australia. By Australian law, contracts are enforceable if the parties have signed the agreement verbally or with a wet-ink (physical) or electronic signature. The law on electronic signatures in Australia is regarded as permissive or minimalist.

5.4.3. New Zealand (Electronic Transactions Act 2002)

The New Zealand Electronic Transactions Act 2002 sets down guidelines for promoting the use of email and other electronic technologies, both in industry and in contact between government and public. In fact, the 2003 Regulation on Electronic Transactions (SR 2003/288) lays down some comprehensive guidelines for different circumstances. On 21 November 2003 the Act and Regulations came into effect.

5.4.4. China (People's Republic of China Electronic Signature Law)

The Electronic Signature Law of the People's Republic of China, published in 2005 and revised in 2015 (the "E-signature Rule") provides legal basis for determining the validity of electronic legislation. Under the law, contracts can be electronically signed. Under Chinese law, a written signature is not necessarily required for a contract to be valid. A contract is valid if parties agree on the terms whether verbally, electronically or in a physical paper document.

5.4.5. European Union (Regulation 910/2014) on electronic identification and trust services for electronic transactions in the internal market (eIDAS Regulation)

The electronic identification and trust services (the eIDAS Regulation) entered into force on 17 September 2014 and was applicable from 1 July 2016. The eIDAS regulation provides a comprehensive legal framework to ensure trustworthiness and legal validity of electronic transactions in the European Single Market. It was meant to provide a predictable regulatory environment for safe and seamless electronic interactions between companies, citizens and public authorities in the European Union. With eIDAS, the EU has succeeded in laying the right foundations and a clear legal framework for citizens, businesses (especially small and medium-sized enterprises) and public administrations to access services securely and make transactions online and across borders in just one click.' Indeed, the roll-out of eIDAS means greater security and convenience for any online e-commerce activity.

5.4.6. Hong Kong (Electronic Transactions Ordinance Act of 2000)

Hong Kong's Electronic Transactions Ordinance provides that contracts cannot be invalidated merely because they were concluded electronically. Under the law, electronic signatures have been recognised as having the same legal status as a wet-ink signature.

6. A REVIEW OF COURT DECISIONS ON THE AUTHENTICITY OF ELECTRONIC SIGNATURES

While not strictly necessary under the rules of evidence, audit trails have proven very effective in authenticating a record to demonstrate that the e-signature is that of the signatory. Courts in different jurisdictions have confirmed this position while in others it is still problematic. This section analyses the different approaches that courts in the United States of America (USA) and the United Kingdom (UK), as a case study, have given to e-signatures.

6.1. Schrock v. Nomac Drilling, LLC, [2016] WL 1181484

In this case, a USA federal court found that detailed e-signature audit logs satisfy the authentication requirement. An employer sought to enforce an electronically signed agreement with a former employee. The court rejected the former employee's challenge to the authenticity of the electronic signature as his own because the employer presented evidence that the e-signature program required the entry of the last four digits of the former employee's social security

number, and the audit trail showed that the document was electronically signed at a specific location at a time when the former employee was at that same location.

6.2. Obi v. Exeter Health Resources, Inc. [2019] WL 2142498

A USA federal district court in New Hampshire rejected the party's argument that her electronic signature on an agreement had been forged, where DocuSign eSignature audit logs showed that she had viewed and signed the agreement through her DocuSign eSignature account.

6.3. Moton v. Maplebear Inc. [2016] WL 616343

A USA district court in the Southern District of New York, found that an e-signature provider's "time-stamped audit trail that tracks using IP addresses and other identifying data when each [signatory] receives, views and executes each agreement" was sufficient to establish that the signer's signature was his own, and that this evidence, in turn, established assent to the agreement.

6.4. IO Moonwalkers, Inc. v. Banc of America, [2018] 814 S.E.2d 583

A DocuSign eSignature audit trail showed that a business accessed a document it claimed it had not signed, which supported the trial court's finding that the business had ratified the signature of the agreement with the other party. There, the party had argued that no one affiliated with his business had signed the agreements at issue and speculated that one of the other party's employees had signed them. However, the evidence showed that the owner of the business had provided the other party with an email address to send agreements for electronic signature, and that the business was familiar with how DocuSign eSignature worked. The DocuSign eSignature audit trail showed that someone with access to the business's email account accessed and then signed the agreements at issue. This audit trail evidence was critical to the court's rejection of the business's effort to create a material dispute of the facts in the case as to whether the agreements at issue had been signed by a representative of its business.

6.5. Harpham v. Big Moose Inspection, [2015] WL 5945842

A USA court found that a more rudimentary audit trail of the party's receipt and electronic signing of agreement was sufficient to overcome the party's unsupported affidavit that he did not recall signing the agreement.

6.6. R v Pusey [1972] Imm AR 240

In this UK case, evidence of the use of an electronic signature was the basis for the court's decision to convict the accused on fraud charges. The defendant, Mr. Pusey, was a former staff director at the Fred Victor Center (the "Center"), a charitable organization based in Toronto. He was also the head of two companies (the "Companies"). These companies billed the Center for more than one hundred thousand dollars for work that was performed by other employees or subcontractors of the Center, in violation of the Center's Code of Conduct regarding Conflicts of Interest. The scheme was discovered when the Center's employees questioned some invoices for payments made to the Companies following the cheque details signed by the accused. As a result, the Center paid out to the Companies various payments totaling more than $115,000 over 16 months. The accused testified that the arrangement was approved by the Center's Executive Director. Allegedly, the scheme was that the Companies billed the Center for work done by subcontractors. Mr. Pusey then paid them in cash to get savings and tax benefits for the Center. The only documentary evidence presented by the accused were contracts allegedly signed by Mr. Pusey (on behalf of the Companies) and the Center's Executive Director. The Center's Executive Director testified that the contracts were fake, and he had refused to sign them. The court examined evidence that the accused's computer and flash drive contained electronic versions of the Executive Director's signature and found that the accused would have had access to the signature. Versions of the electronic signatures on the accused's hard drive were created and modified on the same day, which coincided with the first date when one of the Companies billed the Center. The report of the Center of Forensic Sciences found that the electronic signature and the "contract" signature came from the same signature source "within the limits of practical certainty.". The Judge declared that "the signature on the so-called contract and the electronic signature found on Mr. Pusey's computer are identical." The court rejected Mr. Pusey's explanations and alternative theories when finding him guilty of fraud.

This case demonstrates the legal provability and security problem associated with electronic documents and signatures on negotiable instruments. In most common law jurisdictions, including Ontario, legislation has been in place for many years making the use of electronic signatures legally provable.

The above cases demonstrate that, while audit trails may not be required to authenticate electronic signatures and establish assent to an agreement, they greatly simplify the task of an attorney who must overcome an adversary's claim that he did not sign an agreement or that his e-signature was somehow forged. These cases also reinforce the more general takeaway that an audit trail associated with other types of contracts, such as a clickwrap, also will greatly help in enforcing such contracts. Further, these cases demonstrate that not only does an electronic signature with an audit trail strengthen a party's position, but it also provides no practical downside. Rather than needing to proactively cultivate corroborating

evidence for a challenged paper-and-ink signature, counsel can justifiably rely on an e-signature audit trail to provide heightened substantiation of the authenticity of an electronic document.

7. CHALLENGES ASSOCIATED WITH ELECTRONIC SIGNATURES

In civil evidence, a record or document is regarded as "authentic" if there is evidence that the document or record "is what its proponent claims".[65] The notion of "document" as such is fairly broad and generally encompasses "anything in which information of any description is recorded".[66] This would include, for example, such things as photographs of tombstones and houses,[67] account books[68] and drawings and plans.[69] The relevancy of a document as a piece of evidence is established by connecting it with a person, place or thing, a process which in some common law jurisdictions is known as "authentication".[70] Signing a document is a common albeit not exclusive means of "authentication", and, depending on the context, the terms "to sign" and "to authenticate" may be used as synonyms.[71]

Most legal systems have special procedures or requirements that are intended to enhance the reliability of handwritten signatures. Some procedures may be mandatory in order for certain documents to produce legal effects. They may also be optional and available to parties that wish to act to preclude possible arguments concerning the authenticity of certain documents. Typical examples include the following:

7.1. Notarisation

In certain circumstances, the act of signing has a particular formal significance due to the reinforced trust associated with a special ceremony. This is the case, for instance, with notarization, i.e., the certification by a notary public to establish the

[65] See the USA Federal Rules of Evidence, Rule 901(a):

> The requirement of authentication or identification as a condition precedent to admissibility is satisfied by evidence sufficient to support a finding that the matter in question is what its proponent claims.

[66] United Kingdom of Great Britain and Northern Ireland, Civil Evidence Act 1995, chapter 38, section 13.
[67] Lyell v. Kennedy (No. 3) (1884) 27 Ch.D. 1 (United Kingdom, Chancery Division).
[68] Hayes v. Brown [1920] 1 K.B. 250 (United Kingdom, Law Reports, King's Bench).
[69] J. H. Tucker & Co., Ltd. v. Board of Trade [1955] 2 All ER 522 (United Kingdom, All England Law Reports).
[70] Farm Credit Bank of St. Paul v. William G. Huether, 12 April 1990 (454 N.W.2d 710, 713) (United States, Supreme Court of North Dakota, Northwestern Reporter).
[71] In the context of the revised article 9 of the United States Uniform Commercial Code, for example, "authenticate" is defined as "(A) to sign; or (B) to execute or otherwise adopt a symbol or encrypt or similarly process a record in whole or in part, with the present intent of the authenticating person to identify the person and adopt or accept a record".

authenticity of a signature on a legal document, which often requires the physical appearance of the person before the notary.

7.2. Commissioning

Just like notarisation, commissioning a document requires physical appearance of the deponent before a commissioner of oaths. The rationale is to certify by a commissioner of oaths the authenticity of a signature on a legal document, which often requires the person signing the document to physically appear before the commissioner. This may not be possible under the ESA.

Section 4 of the Commissioner for Oaths (Advocates) Act Cap 5 which provides for the powers of the commissioner and section 5 thereof provides for the particulars to be stated in a jurat or attestation clause in the following words:

> Every commissioner for oaths before whom any oath or affidavit is taken or made under this Act shall state truly in the jurat or attestation at what place and on what date the oath or affidavit is taken or made.[72]

Section 5 of the Act states that:

> Every commissioner for oaths before whom any oath of affidavit is taken or made shall state in the jurat or attestation at what place and on what date the oath or affidavit is taken or made.[73]

Rule 9 of the schedule to the Act provides that the form of the jurat is set out in the third schedule to the rules which requires to state that the oath was sworn and declared before a commissioner for oath in a particular specified place and the date of making it.

Failure to comply with the above requirements, specifically physical presence and writing your signature before the commissioner for oath may render the entire oath defective.[74]

7.3. Attestation

Attestation is the act of watching someone sign a legal document and then signing one's name as a witness. The purpose of attestation is to preserve evidence of the signing. By attesting, the witness states and confirms that the person whom he or she watched sign the document in fact did so. Attesting does not extend to vouching for the accuracy or truthfulness of the document. The witness can be

[72] See Cap. 5, Laws of Uganda
[73] *Id*
[74] See HCMA NO. 31 of 2020, Attorney General vs Okello James Enos & Opolot Edward. High Court of Uganda at Soroti decided on the 02nd day of July 2021.

called on to testify as to the circumstances surrounding the signing.[75]

7.4. Seals

The practice of using seals in addition to, or in substitution of, signatures is not uncommon, especially in certain regions of the world.[76] Signing or sealing may, for example, provide evidence of the identity of the signatory; that the signatory agreed to be bound by the agreement and did so voluntarily; that the document is final and complete; or that the information has not been altered after signing.[77] It may also caution the signatory and indicate the intent to act in a legally binding manner.

7.5. Electronic Print versus Handwritten Print

In *the Matter of an Application for a writ of Habeas Corpus ad subuciendum by Kyagulanyi Sentamu and Another v Attorney General and 2 Others,*[78] the High Court of Uganda was faced with a challenge of determining whether an electronic print of a signature of a deponent on an affidavit as opposed to an original ink print (wet signature) is admissible in evidence or defective. Court noted that it was stated that the affidavit of one of the Respondents was a scanned copy and could not therefore have been sworn before a Commissioner for Oaths and therefore, it is a nullity. In addressing this issue, court made the following observation:

> In resolving this preliminary point, this Court will start with whether the affidavit is a scan and was not therefore signed before a Commissioner for Oaths. I have examined the signature of the affidavit on the court record. It is in black ink and is clearly not an electronic print. It bears an imprint of the pen pressure left when the deponent signed and for that reason the submission that it is a scan is dismissed.[79]

From the above reasoning of court, it appears that the affidavit was simply saved because the Judge was convinced that it was not an electronic print but simply a wet signature. The implication here is that if it was the former, then it would not be saved. The critical concern here is whether the Judge addressed his mind to the provisions of the ESA which were in force at the time of hearing and determining

[75] Adrian McCullagh, Peter Little and William Caelli, "Electronic signatures: understand the past to develop the future", University of New South Wales Law Journal, vol. 21, No. 2 (1998; see chap. III, sect. D, on the concept of witnessing.
[76] Seals are used in several countries in eastern Asia, such as China and Japan.
[77] Mark Sneddon, "Legislating to facilitate electronic signatures and records: exceptions, standards and the impact of the statute book", University of New South Wales Law Journal, vol. 21, No. 2 (1998); see part 2, Chap. II, "Policy objectives of writing and signature requirements".
[78] Miscellaneous Cause 16 of 2021 [2021] UGHCCD 1 (23 January 2021); [2021] UGHCCD 1.
[79] *Id* at pg. 9

this matter.

7.6. The Electronic Signatures Act's Description of the Nature of an Electronic Signature

ESA defines an electronic signature to mean data in electronic form affixed to or logically associated with a data message, which may be used to identify the signatory in relation to the data message and indicate the signatory's approval of the information contained in the data message; and includes an advance electronic signature and the secure signature.[80] By implication, it does not need to be a wet signature by electronic.

It further defines an electronic signature product to mean configured hardware or software or relevant components of it, which are intended to be used by a certification service provider for the provision of electronic signature services or are intended to be used for the creation or verification of electronic signatures.[81]

The effect of the above two provisions of the ESA is that such a signature can neither be wet nor made before a notary public, commissioner for oath any other attesting officer under the law. This means that there is still a variance between the ESA and other legislations governing affidavit evidence in Uganda to wit; the Notaries Public Act;[82] the Statutory Declarations Act;[83] the Oaths Act;[84] the Commissioner for Oaths (Advocates) Act;[85] and the Civil Procedure Rules.[86]

7.7. Absence of adequate Public Key Infrastructure

The National Information Technology Authority – Uganda (NITA-U) in April 2022 announced the issuance of Public Key Infrastructure (PKI) license to Pos Digicert. This license and registration cover provision of certification services as well as date & time stamp services.

PoS Digicert, Mantra Technologies and Digital Trust are part of the Joint Venture that was contracted by Government of Uganda to establish and maintain the digital authentication and electronic signatures solution under the brand name UGPASS. This venture supports use of advanced electronic signatures based on trusted and secure PKI. This brought forth for the first time advanced electronic signatures compliant with the ESA and as such admissible in Courts of Law. UGPASS enables users to utilize their existing smart phones to register for a securely verified digital certificates in order to authenticate themselves online for

[80] See Section 2 of ESA.
[81] *Id.*
[82] Cap. 18, Laws of Uganda.
[83] Cap. 22, Laws of Uganda.
[84] Cap. 19, Laws of Uganda.
[85] Cap. 5, Laws of Uganda.
[86] S.I. No. 71-1 (as amended by S.I. NO. 33 of 2019)

seamless and secure access to a variety of e-services and use advanced electronic signatures to securely e-sign documents with the following benefits:

- high level of security;
- high level of user assurance; and
- non-repudiation of User operations.[87]

Notwithstanding the above development, PKI infrastructure is still weak and inadequate in Uganda to control and manage electronic signatures. No wander most public entities still rely on wet signatures and have not embraced electronic signatures in their systems.

Electronic signatures still have challenges in administration of justice in both civil and criminal jurisdictions. We cannot however avoid use of electronic signatures given technological advancement globally. We need to address the shortcomings and make electronic signatures easily admissible in litigation and other court business. The following avenues can help to address some of the above challenges.

8. RECOMMENDATIONS

8.1. Harmonisation of Laws Governing Admissibility of Evidence with the Electronic Signatures Act

This article has demonstrated that the different laws governing affidavit evidence are at variance with the ESA. The Notaries Public Act, the Advocates (Commissioner for Oaths) Act, the Oaths Act, the Statutory Declarations Act and the Civil Procedure Rules are all providing for a wet signature and require the person writing a signature to do so physically in the presence of commissioner for oaths or notaries public. This is not the position with the e-signature which is predominately electronic. There is urgent need to harmonise these pieces of legislation to be in tandem with the ESA.

8.2. Technological Infrastructure Improvement

Technological infrastructure to facilitate e-signature in Uganda is still very weak. Although the NITA-U has licensed a few companies on application of PKI, less application of the system has been realised even in the greater Kampala metropolitan and most public institutions have not yet embraced this technology which makes the system quite inoperative.

[87] **NITA-U Issues First Public Key Infrastructure (PKI) Provider License.** Available at NITA-U Issues First Public Key Infrastructure (PKI) Provider License | National Information Technology Authority - Uganda (NITA-U) https://www.nita.go.ug/nita-u-issues-first-public-key-infrastructure-pki-provider-license (accessed on 14 August 2022)

8.3. Training Efficient and Reliable Human Resource Personnel

This is yet another problem affecting e-signature and e-justice generally in Uganda. ICT is a practical skill which requires experts to run the system. Most legal practitioners representing parties in courts of law, who also prepare affidavits and statutory declarations have little knowledge in ICT. The judiciary has employed some ICT experts like the technical team on Electronic Court Case Management Information System (ECCMIS) who are of ICT background, but they are overwhelmed as they are very few compared to a number of courts in the country and the different stakeholders, they need to serve at a given period of time. Moreover, ECCMIS itself is still challenged by ICT inefficiencies in the country generally. There is need to train legal service providers in ICT to make them relevant and embrace the use of e-signatures.

8.4. Using Passwords and Hybrid Methods to Enhance Security of the Signature

Passwords and codes are used both for controlling access to information or services and for "signing" electronic communications. In practice, the latter use is less frequent than the former, because of the risk of compromising the code if it is transmitted in non-encrypted messages. Passwords and codes are however the most widely used method of "authentication" for purposes of access control and identity verification in a broad range of transactions, including most Internet banking transactions, cash withdrawals at automated teller machines and consumer credit card transactions. It should be recognized that multiple technologies can be used to "authenticate" an electronic transaction. Several technologies or several uses of a single technology can be utilized for a single transaction. For example, signature dynamics for authentication can be combined with cryptography for message integrity. Alternatively, passwords can be sent over the Internet, using cryptography (e.g., SSL in browsers) to protect them, in conjunction with the use of biometrics to trigger a digital signature (asymmetric cryptography), which, on receipt, generates a Kerberos ticket (symmetric cryptography). In developing legal and policy frameworks to deal with these technologies, consideration should be given to the role of multiple technologies. Legal and policy frameworks for electronic authentication will need to be flexible enough to cover hybrid technology approaches, as those that focus on specific technologies could impede the use of multiple technologies.[88] Technology-neutral provisions would facilitate the acceptance of such hybrid technology approaches.

[88] See Foundation for Information Policy Research, Signature Directive Consultation Compilation, 28 October 1998, which provides a compilation of responses made during consultations on the European Union draft directive on electronic signatures, prepared at the request of the European Commission, available at www.fipr.org/publications/sigdirecon.html (accessed on 14 August 2022).

8.5. Licence more Public Key Infrastructure and Certification Services Providers

We appreciate the fact that NITA-U has this year licensed some PKI service providers. We wish however, note the fact that the efforts are still at the infancy stage and need serious boosting. Setting up a PKI is a way to provide confidence that (a) a user's public key has not been changed and in fact corresponds to that user's private key; and (b) the cryptographic techniques being used are sound. To provide such confidence, a PKI may offer a number of services, including the following: (a) managing cryptographic keys used for digital signatures; (b) certifying that a public key corresponds to a private key; (c) providing keys to end-users; (d) publishing revocation information on public keys or certificates; (e) managing personal tokens (e.g. smart cards) that can identify the user with unique personal identification information or can generate and store an individual's private keys; (f) checking the identification of end-users and providing them with services; (g) providing time-stamping services; and (h) managing cryptographic keys used for confidentiality encryption where the use of such a technique is authorized. This with no doubt will increase public confidence in e-signatures as clear safeguards to control their authenticity is in place.

8.6. Using Biometrics to Safeguard Systems

Biometrical devices are generally considered as offering a high level of security. While they are compatible with a range of uses, their current main usage is in government applications, particularly law enforcement applications such as immigration clearance and access controls. Technical solutions might assist in addressing some concerns. For instance, storage of biometrical data on smart cards or tokens may protect against unauthorized access, which could occur if the data is stored on a centralized computer system. Moreover, best practices have been developed to reduce risks in different areas such as scope and capabilities; data protection; user control of personal data; and disclosure, auditing, accountability and oversight.

8.7. Video/Virtual Witnessing of Signatures

Electronic specifically video witnessing of signatures can be adopted. This is very relevant while signing affidavits and statutory declarations. Commissioners for oaths, Notaries Public and Justices of peace can through legislation be permitted to witness a person appending his or her signature on an affidavit electronically by use of video and other relevant gadgets. This can help in dispensing away the requirement of physical presence before such officers.

8.8. Amending Legislation that is Incompatible with Modern Technology

There is urgent need to amend all legislations in force but incompatible with modern technology. All laws should reflect the current technological discourse to remain relevant and facilitate e-justice system. Without this, we shall have e-justice policies without laws to implement them and technological advancements like cyber legislation will be unproductive.

8.9. Training and Sensitising Stakeholders

For e-justice and e-signature to be effectively managed and implemented, it has to be rolled out to all stakeholders including the judiciary, legal practitioners, legislators, academia, training institutions and litigants generally. ICT skills are involved here, and they are not common to everyone. Serious training of staff of the different stakeholders is critical. Early training of students at the university is equally encouraged.

CONCLUSION

Laws that provide for the legal value of digital signatures typically attribute the same legal value to signatures supported by foreign certificates only to the extent that they are regarded as equivalent to domestic certificates. The review done in this study indicates that proper assessment of legal equivalence requires a comparison not only of the technical and security standards attached to a particular signature technology, but also of the rules that would govern the liability of the various parties involved. The UNCITRAL Model Law on Electronic Signatures provides a set of basic common rules governing certain duties of the parties involved in the authentication and signature process that may have an impact on their individual liability. There are also regional texts, such as the European Union directive on electronic signatures, that offer a similar legislative framework for the liability of certification services providers operating in the region. However, neither of those texts addresses all liability issues arising out of the international use of certain electronic authentication and signature methods.

The ESA is already in force but with less application as it seems incompatible with most laws governing evidence in Civil proceedings in Uganda. It is now more than a decade since the Act came into force and has not been fully operationalised as courts to date still accord wet-ink signatures more value than electronic signatures. Electronic signatures globally operate under the principles of non-discrimination, technological neutrality and functional equivalence. We need to quickly revisit our laws governing evidence in civil proceedings to align with the ESA. This will simplify the duty of courts of law while interpreting such laws in cases before them.