ARTICLE :

Implementing the electronic signature law in Tanzania – successes, challenges, and prospects

By Ubena John

Introduction

Electronic commerce is an example of electronic transactions that have recently been taken up in Tanzania. Thanks to the enabling legal environment, online services such as eHealth services, mobile and electronic banking services, and payment systems have thrived. However, security and trust has not been forthcoming where people conduct business transactions on the internet. From a legal standpoint, electronic signatures are used for a variety of purposes, including to signify willingness to be bound by the terms of a contract, to sign a bank order, to authorise an invoice and to provide authority (for payments). An electronic signature signifies consent of the signatory and their intent to be bound by the transaction.

Thus, where the law requires a signature, that requirement may be met by using an electronic signature, as provided for by s6 of the Electronic Transactions Act 2015 (ETA). For electronic transactions, signatures may include a name at the bottom of email, a personal identity number (PIN), a scanned handwritten signature, etc. Nonetheless, these forms of signature may not be helpful to identify a party or to ensure the integrity of the data. To overcome this challenge, a signature using PKI and involving trusted third parties is utilised.[1]

Tanzania has provided for the legal validity of a signature using a PKI.[2] However, the legal effects of an electronic signature within a PKI does have some deficiencies. It is undisputed that electronic transactions require trust and security. Online market sellers and buyers would like to know with whom they are transacting[3] and to be assured that the documents they are exchanging, or transactions in which they are engaging, are trustworthy. Signatures have a range of functions, which include: identifying the signatory; that the signatory intended the signature to be his signature; that the signatory signified his assent to be bound by the content of the document he signed; and that the signature guarantees trust or offers assurance to respective parties to a particular transaction.[4] In the online world, it is possible to rely on digital signatures for the purposes of trust, integrity, and confidentiality, although online traders tend to rely on the means of payment being linked to the person making the order for goods or services, rather than rely on any form of electronic signature, and this works very well. While the law provides for the legal validity of electronic signatures in Tanzania, the reality of how they are used is somewhat different.

[1] Adam Mambi, *ICT Law Book: A Source Book for Information & Communication Technologies and Cyber-Crime* (Dar es salaam: Mkuki na Nyota Publishers, 2010) 103-105; Ubena John, 'E-documents & E-signatures in Tanzania: Their Role, Status, and the Future', in Kelvin Joseph Bwalya and Saul F.C. Zulu, (eds), *A handbook of Research on e-Government in Emerging Economies: Adoption, E-Participation, and Legal Frameworks*, Vol.1 (Hershey, PA, USA, IGI, 201), pp. 90-122.

[2] See ss 6-7 ETA providing for validity of electronic signatures in Tanzania.

[3] Stephen Mason and Timothy S. Reiniger, '"Trust" Between Machines? Establishing Identity Between Humans and Software Code, or whether You Know it is a Dog, and if so, which Dog?', *Computer and Telecommunications Law Review*, 2015, Volume 21, Issue 5, pp. 135-148.

[4] Andrew Murray, *Information Technology Law* (Oxford, OUP, 2011), p. 428; for a comprehensive list of the functions of a signature, see Stephen Mason, Chapter 7 'Electronic signatures' in Stephen Mason and Daniel Seng, editors, *Electronic Evidence and Electronic Signatures* (5th edn, Institute of Advanced Legal Studies for the SAS Humanities Digital Library, School of Advanced Study, University of London, 2021), 7.11-7.19, open access at https://humanities-digital-library.org/index.php/hdl/catalog/book/electronic-evidence-and-electronic-signatures.

Defining the electronic signature

Section 3 of ETA provides:

> 'electronic signature' 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.

Section 7 of ETA provides that an electronic signature is secure if it:

> (a) is unique for the purpose for which it is used;
>
> (b) can be used to identify the person who signs off the electronic communication;
>
> (c) is created and affixed to the electronic communication by the signer;
>
> (d) is under control of the person who signs; and
>
> (e) is created and linked to the electronic communication to which it relates in a manner such that any changes in the electronic communication would be revealed.[5]

Beside the statutory definition of an electronic signature, there are several legal scholars who have attempted to define the term 'electronic signature' and identify the purposes of a signature. According to Professor Chris Reed, the electronic signature serves three purposes: the identity of the signatory; the intention to make a signature; and that the signatory adopts the contents of the document.[6] Mason outlines a number of aspects of the signature, including the purpose and functions, considered dictionary definitions,[7] discusses the difference between the manuscript (handwritten) signature and a digital signature and explains what a digital signature is.[8] The oft-cited example of an ideal electronic signature is the digital signature within the framework of a PKI, because the PKI involves trusted third parties.

At this juncture, it is noteworthy that the term 'digital signature' is used interchangeably with 'electronic signature'.[9] Any form of electronic signature is capable of being binding, but some forms of electronic signature do not have the same status in law in some jurisdictions.[10] The digital signature can achieve technical efficacy in security, confidentiality, and integrity. It is used to secure databanks, online shops, critical infrastructure, and such like. Electronic signatures take various forms, such as a name typed at the foot of an email, a sound, clicking 'OK', or the accept button on a web page signifying assent to the terms and conditions on that page.[11] Other forms of signature include biometric measurements, such as the scanned retina, fingerprint, and DNA samples.[12] The use of the

---

[5] ETA s7.

[6] Chris Reed, 'What is a signature?', (2000) 3 Journal of Information, Law and Technology (JILT), at https://warwick.ac.uk/fac/soc/law/elj/jilt/2000_3/reed/.

[7] Mason, Chapter 7 'Electronic signatures', 7.1-710.

[8] Mason, Chapter 7 'Electronic signatures', 7.30, a full technical overview of how a digital signature works is set out at 7.203-7.227.

[9] Mason, Chapter 7 'Electronic signatures', 7.30-7.32.

[10] Anna Nordén, 'Electronic signatures in a legal context', in Cecilia Magnusson Sjöberg, editor, *IT Law for IT Professionals – an introduction* (Studentlitteratur AB; 2005) pp. 152-154; Ubena John, 'E-documents & E-signatures in Tanzania: Their Role, Status, and the Future', p 104; Stephen Mason, 'The practical issues in using electronic signatures in different jurisdictions', *Computer and Telecommunications Law Review, 2021, Volume 27, Issue 6, pp. 165-179*.

[11] By way of example, see the USA case of *Moore v Microsoft Corporation*, 293 A.D.2d 587, 741 N.Y.S.2d 91 (N.Y. App. Div. 2002); see also *eBay International AG v Creative Festival Entertainment Pty Ltd* (2006) 170 FCR 450 (Australian Federal Court held that the act of clicking acceptance of terms and conditions appearing in a website is as good as signing of a contract in writing); Stephen Mason *Electronic Signatures in Law* (4th edn, Institute of Advanced Legal Studies for the SAS Humanities Digital Library, School of Advanced Study, University of London, 2016), 3.10, currently available online at https://ials.sas.ac.uk/digital/humanities-digital-library/observing-law-ials-open-book-service-law/electronic-signatures; Cecilia Magnusson Sjöberg and Anna Nordén, 'Managing Electronic Signatures – Current challenges' in Peter Wahlgren, editor, *IT Law* Volume 47 (Stockholm Institute for Scandinavian Law, 2004), pp 81-95; Anna Nordén, 'Electronic signatures in a legal context', pp. 149-183.

[12] See Mason, Chapter 7 'Electronic Signatures', for a complete list and relevant case law.

fingerprint – especially a thumb print – as a signature is common in Tanzania, and individuals without a handwritten signature and who file their pleadings will sign them by affixing their thumb prints to the documents in proceedings.

Development of the electronic signature law in Tanzania

Prior to the enactment of the ETA in 2015, the electronic signature lacked legal recognition in Tanzania. The legislature subsequently took cognizance of the development in electronic commerce and electronic government services. In 2015, it enacted the ETA to provide for a range of issues, including the legal validity of electronic transactions, electronic contracts, electronic signatures, and the admissibility of electronic evidence. Despite these developments, trust in electronic transactions was difficult to achieve without the parties identifying or knowing their counterparties in online transactions.

The attributes of the secure electronic signature set out above are commendable. However, the law has not defined the rights, duties and liabilities of the parties creating, using, or relying on electronic signatures. To address this shortcoming, Tanzania intended to implement PKI signatures as mandated by the ETA.[13] The ETA embodies provisions for the regulation of cryptographic and certification services.[14] Digital authentication is undertaken by the electronic Government Authority (eGA) on behalf of public entities via PKI and the Digital Signature Management System as mandated by the e-Government Act, No 10 of 2019.[15] These provisions confirm that the Tanzania preference is for a PKI.[16] The law further states, at s6(1), that 'where a law requires the signature of a person to be entered, that requirement shall be met by a secure electronic signature made under this Act.'

Having depicted the development of the electronic signature agenda in Tanzania, it is worthwhile to elaborate the approaches in respect of electronic signature laws adopted in other jurisdictions, albeit briefly.

Approaches to electronic signatures law

This section makes a short comparison to the development of the law of electronic signatures within Australia and South Africa. The electronic signature laws in these countries seem to have been influenced by UNCITRAL Model law on Electronic Commerce. The three types of approach that jurisdictions have taken to electronic signatures are briefly explained.[17] They are prescriptive, minimalistic, and two-tier.

Prescriptive approach

The prescriptive approach to electronic signatures specifies the particular type of electronic signature technology to be adopted. It is strict and inflexible. This approach may act to stifle innovation because other types of electronic signature technology are excluded. The jurisdictions that have opted for the prescriptive approach are Brazil, Indonesia, Israel, Peru, Philippines, Russia, Turkey, and Uruguay.[18] The prescriptive approach stipulates the purpose of the electronic signature, but also specifies the technology for a signature to be legally valid. Some jurisdictions adopted this approach, but later revised the legislation.[19]

---

[13] See Ministry of Works, Transport and Communication, Consultancy report dated 20 February 2017 in respect of Tender No. ME.006/RCIP/2015-2016/HQ/C/03 Business, Functional, Non-Functional Requirements and System Design Specification for the Tanzania National Public Key Infrastructure includes policy, legislative and regulation requirements. Herein referred to as the NPKI consultancy report (on file with the author). See also International Competitive Selection Tender from the Tanzania Communications Regulatory Authority available at https://www.tcra.go.tz/uploads/documents/sw-1619170675-PROVISION%20OF%20CONSULTANCY%20SERVICES%20FOR%20IMPLEMENTATION%20OF%20NATIONAL%20PUBLIC%20KEY%20INFRASTRUCTURE%20(NPKI)%20IN%20TANZANIA.pdf.

[14] ETA ss33-36.

[15] The e-Government Act s5.

[16] India took the prescriptive approach and preferred the PKI model, but the law was amended to provide for all forms of electronic signature: Mason, *Electronic Signatures in Law*, 3.3.

[17] For details on the approach to electronic signature law from various jurisdictions see Mason, *Electronic Signatures in Law*, 3.2-3.21.

[18] See CERTIPHI, electronic signatures, https://www.certiphi.com/resource-center/compliance-services/electronic-signatures/; Mason, *Electronic Signatures in Law*, 3.3.

[19] India is a good example.

Minimalistic approach

The minimalistic approach permits the use of any form of electronic signature. All types of electronic signature are legally recognized. The countries that have preferred the minimalistic approach include Australia, Canada, New Zealand, Thailand, and USA.[20] The advantage of the minimalistic approach is that it promotes innovation. The merit of the minimalistic approach is simplicity. Any type of electronic signature is legally recognized. In so doing the market is left to supply any signature technology. Nevertheless, besides other deficiencies, the minimalistic approach has left room for signatures of poor quality to be used and hence they may be easily forged, although it must be noted that, given the millions of contracts entered into remotely across the world every day, there are very few cases of forgery.[21]

Two-tier approach

The two-tier approach is a hybrid model in which most types of signature technology will be legally recognized. The legislation generally provides for a certain class of approved electronic signature technologies that may be used.[22] The EU has indicated it prefers the qualified electronic signature (digital signature) over other types of electronic signatures. Tanzania has similarly expressed preference for the secure electronic signature over other types of electronic signature. The two-tier approached has been adopted in the EU, China, Japan, South Africa, and Tanzania. The advantage of this approach is that the law recognizes any type of electronic signature. The legislation also tends to include attributes linked to an electronic signature that are considered to be reliable or secure.[23] The problem is that not every signature is reliable or secure. ETA section 6(1) provides that where the law requires a signature to be appended, such requirement shall be met by entering or using a secure electronic signature as defined under section 7. Regardless, many Tanzanians use simple electronic signatures such as the name at the foot of email, and a scanned version of handwritten signature. This is probably because buying and constantly paying to up-date a PKI digital signature is expensive and complex to install and use.

Australia

Although Australia adopted the minimalistic approach to electronic signatures, the Gatekeeper Public Key Infrastructure Framework issued by the Digital Transformation Office (DTO) suggests that some Australian government agencies preferred to use the PKI signature. The Gatekeeper PKI Framework is a guide issued to assist those who are using or relying on a signature affixed within a PKI to authenticate online transactions. It helps the parties (accreditation authority, registration authority, certification authorities, key issuers, certificate holders, users or relying parties) involved in the PKI signature cycle to understand the technical and legal requirements. Moreover, it helps them appreciate their roles, rights, duties, and liabilities. The use of the PKI signature is not mandatory in Australia.[24] Parties are free to choose any electronic signature technology that meets the attributes set out in the Electronic Transactions Act.[25] Nonetheless, when government agencies or other organisations use the PKI (including a digital certificate to authenticate the signing party), Gatekeeper accredited service providers must be used.[26] Unlike South Africa, where the South Africa Accreditation Authority (SAAA) accredits both private and government electronic signature service providers, in Australia, the Gatekeeper PKI Framework is for government agencies that use PKI signatures. Section 2 of the Gatekeeper PKI Framework provides:

> The Gatekeeper PKI Framework is a whole-of-government suite of policies, standards and procedures that governs the use of PKI in Government for the authentication of individuals, organisations, and non-person entities (NPE) – such as devices, applications, or computing components.

---

[20] CERTIPHI, electronic signatures, https://www.certiphi.com/resource-center/compliance-services/electronic-signatures/; Mason, *Electronic Signatures in Law*, 3.8.

[21] Mason, Chapter 7 'Electronic signatures', 7.35-7.37, 7.227.

[22] CERTIPHI, electronic signatures, https://www.certiphi.com/resource-center/compliance-services/electronic-signatures/; Mason, *Electronic Signatures in Law*, 3.15; Article 7 of UNCITRAL Model Law on Electronic Commerce also adopted a two-tier approach to electronic signature; Article 6(3) of UNCITRAL Model Law on Electronic Signature echoes the foregoing law.

[23] This has been done in South Africa and Tanzania.

[24] Section 5.4 of Gatekeeper PKI Framework.

[25] Electronic Transactions Act 1999 (Cth), s10(1).

[26] See Section 5.4 of Gatekeeper PKI Framework.

The Digital Transformation Office is responsible for scrutinizing the application for accreditation of the Gatekeeper of PKI and making recommendations to the Gatekeeper Competent Authority. The latter is responsible for decisions in relation to the accreditation of service providers. Although the Gatekeeper PKI Framework appears to be for government agencies, it applies to organisations that choose to obtain and maintain gatekeeper's accreditation.[27]

Under Section 10(1)(a) and (b) of the Electronic Transactions Act 1999, an electronic signature is legally recognized in Australia if it has the following attributes:

> …(a) in all cases—a method is used to identify the person and to indicate the person's intention in respect of the information communicated; and (b) in all cases—the method used was either: (i) as reliable as appropriate for the purpose for which the electronic communication was generated or communicated, in the light of all the circumstances, including any relevant agreement; or (ii) proven in fact to have fulfilled the functions described in paragraph (a), by itself or together with further evidence…

These attributes apply to any electronic signature regardless of its underlying technology.

In the three countries (Tanzania, Australia, and South Africa), a notable similarity is that all have electronic signature laws that have been highly influenced by the UNCITRAL Model Law on Electronic Commerce. Principles such as functional equivalence found in this Model Law have found their way into the electronic signature laws of these jurisdictions. Also, South Africa and Tanzania have provisions that stipulate the attributes of electronic signature to be secure or reliable. These match the attributes set under Article 7 of the UNCITRAL Model Law on Electronic Commerce.

While Australia has adopted the minimalistic approach, South Africa and Tanzania have opted for the two-tier approach. This might be because the two-tier approach is not only found in the UNCITRAL Model Law on Electronic Commerce, but it is also found in the Southern African Development Community (SADC) Model law.[28]

Because electronic signatures comprise many types, their qualities vary. Many jurisdictions give a higher value to an electronic signature that has the capability of achieving confidentiality, integrity, authenticity, and identifying the signatory. It is for this reason that Tanzania adopted the secure electronic signature (in EU parlance[29]) that in practice, and according to the government plan, is the public key infrastructure (PKI) signature.[30]

South Africa

In South Africa, a PKI has been implemented via the Electronic Communications and Transactions Act.[31] Under that law, the advanced electronic signature (AES) is defined, in section 1, as 'an electronic signature which results from a process which has been accredited by the Authority as provided for in section 37'. Where the law requires a transaction to be endorsed by signature, that requirement is met only if the AES is used.[32] The AES underlying framework is the use of PKI. In South Africa accredited authentication and certification products and certification services also known as PKI or AES services are carried out by two accredited agencies: Law Trust Party Services (Pty) Limited and the South African Post Office Limited (SAPO).[33] The latter is a government agency accredited by the South Africa Accreditation Authority (SAAA) to provide cryptography and certification services. The SAPO first launched its Trust Centre, which is a digital signature and authentication hub, in July 2013.[34] Its Trust Centre is AES Class 4 Certificate and related certificates are compatible with all applications that support the use of the X.509

[27] Section 2 of Gatekeeper PKI Framework.
[28] https://www.itu.int/en/ITU-D/Projects/ITU-EC-ACP/HIPSSA/Documents/FINAL%20DOCUMENTS/FINAL%20DOCS%20ENGLISH/sadc_model_law_e-transactions.pdf .
[29] 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, OJ L 257, 28.8.2014, p. 73-114, for which see Article 26 Requirements for advanced electronic signatures (eIDAS).
[30] Section 7 of ETA.
[31] Act No. 25 of 2002 (ECTA).
[32] See ECTA s13(1).
[33] South Africa Accreditation Authority (SAAA), accredited authentication and certification products and certification services, at http://www.saaa.gov.za/index.php/accreditation.html.
[34] There is a link to the SAPO Trust Centre from the South Africa Accreditation Authority, although the link does not appear to be working.

digital certificate.[35] The other provider, LAWTRUST, is a private company accredited by the SAAA to offer digital authentication services.[36] The LAWTRUST AES product is based on a (claimed) high assurance digital certificate, compatible with products or services that support the X.509 digital certificate.[37]

Recent cases in South Africa regarding electronic signatures[38] include *Spring Forest Trading 599 CC v Wilberry (Pty) Ltd t/a Ecowash.*[39] The issue in this case was whether the names of the parties at the bottom or foot of each email constituted the required consensual cancellation of the agreement. It was held the names at the foot of the emails constituted a signature and was binding. Cachalia JA giving judgment for the court said, at [28] that

> The typewritten names of the parties at the foot of the emails, which were used to identify the users, constitute 'data' that is logically associated with the data in the body of the emails, as envisaged in the definition of an 'electronic signature'. They therefore satisfy the requirement of a signature and had the effect of authenticating the information contained in the emails.

Global & Local Investment Advisors (Pty) Ltd v Nickolaus Ludick Fouché,[40] involved emails sent fraudulently to a bank authorising the transfer of funds. The issue for determination was whether a series of fraudulent emails bound *Fouché*. The court held, at [16], that '[The emails] were not written nor sent by the person they purported to originate from. They are fraudulent as they were written and dispatched by person or persons without the authority to do so. They are not binding on Mr Fouché' – hence the typed signature was a forgery and could not be relied upon. The case of *First Rand Bank t/a Wesbank v Molamuagae*,[41] was an action against Andrew Molamuagae for the cancellation of an instalment sale agreement and the repossession of a vehicle which Molamuagae purchased under the contract. The contract, called an 'iContract', was signed by Molamuagae online with a personal information number, which had been sent to his cellular telephone number, together with his identity number. One of the issues before the court was whether the electronic signature complied with the Electronic Communications and Transactions Act 2002 (ECTA). Senyatsi AJ said that it did, at [43]: 'The NCA [National Credit Act 2005] does not provide for the form that the signature to the instalment sale agreement needs to take. As a result, it is quite possible to sign the agreement electronically and in compliance with the ECTA.' It followed that the instalment sale agreement had been concluded by the parties.

Public Key Infrastructure signature

The PKI involves trusted third parties in the creation and management of keys and certificates for the purposes of a digital signature. The signature interface uses a pair of keys: one private and another public.[42] The latter may be kept public whereas the former is kept secret (private). Public key encryption uses two different keys, each of which will decrypt documents encrypted by the other key. This means the private key can be kept secret, while the other is made public.[43]

With a PKI signature, the rights, duties/obligations and liabilities and other PKI specific issues of certification and supervision are defined in the ETA in Part VI and Part VII. The PKI signature is required to have the following

[35] SAAA, accredited authentication and certification products and certification services, at http://www.saaa.gov.za/index.php/accredited-authentication-and-certification-products-services.html.
[36] LAWtrust, PKI, at https://www.lawtrust.co.za/solutions/pki.
[37] SAAA, accredited authentication and certification products and certification services, at http://www.saaa.gov.za/index.php/accredited-authentication-and-certification-products-services.html. See also SAPO Trust Centre at https://docplayer.net/96041888-The-sapo-trust-centre.html; X.509 at https://en.wikipedia.org/wiki/X.509.
[38] See Mason, 'Electronic signatures', Chapter 7 for earlier cases from South Africa.
[39] (725/13) [2014] ZASCA 178; 2015 (2) SA 118 (SCA) (21 November 2014); mentioned by Mason, Chapter 7 'Electronic signatures', 7.129.
[40] (71/2019) [2019] ZASCA 08; 2021 (1) SA 371 (SCA) (18 March 2020).
[41] (24558/2016) [2018] ZAGPPHC 762 (26 February 2018).
[42] Anna Nordén, 'Electronic signatures in a legal context', at pp. 156-157; John, 'E-documents & E-signatures in Tanzania: Their Role, Status, and the Future', p 105.
[43] Chris Reed, 'What is a Signature?' 2000(3); for a comprehensive explanation of how PKI works, including the risks, see Mason, Chapter 7 'Electronic signatures', 7.203-7.277.

attributes: to ensure confidentiality, integrity, authenticity and identify the signatory.[44] Other scholars have added non-repudiation as another attribute,[45] although, as Mason indicates, non-repudiation is impossible.[46]

Existing laws that address the issues of PKI electronic signatures

Tanzania has several relevant items of legislation and regulations that affect the legal position of PKI electronic signatures. They include the ETA and the Electronic Transactions (Cryptographic and Certification Services Providers) Regulations 2016 (G.N. No. 228), the Electronic Transactions (Cryptographic and Certification Services Providers) Regulations 2016 (G.N. No. 224), Electronic and Postal Communications Act of 2010 and the Electronic and Postal Communications (Computer Emergency Response Team) Regulations 2018 (G.N. No. 60); The Tanzania Communications Regulatory Authority Act 2003; and the Evidence Act (Chapter 6).[47] Each are examined below.

Electronic Transactions Act

The Electronic Transactions Act, Act No. 13 of 2015 (ETA) is the first Act to provide for the validity, admissibility and enforceability of electronic signatures in Tanzania.[48] The ETA provides for a secure electronic signature and its functions, together with the regulation of Cryptographic and Certification Services.[49] The ETA provides a definition of the electronic signature;[50] the legal recognition of an electronic signature;[51] the secure electronic signature, its attributes and application;[52] the liability of the relying party;[53] the use of electronic signatures in electronic record keeping;[54] the use of an electronic signature for the purposes of notarisation, acknowledgement, and certification;[55] the regulation of cryptographic and certification services,[56] and the admissibility and authenticity of evidence in electronic form.[57]

The following Ministries are responsible for information and communications technology: the Ministry of Works, Transport and Communication, the Tanzania Communications Regulatory Authority (TCRA), the Bank of Tanzania (BoT), and the Electronic Government Authority (eGA). These government institutions are also involved in regulating electronic signatures. The ETA mandates the Minister responsible for ICT to select and designate a regulator of cryptographic and certification services[58] and approves policies and regulations for cryptographic and Certification Services Providers[59] and putting the NPKI into operation. The law also stipulates the functions of the regulator of cryptographic and certification services, including, among other things, the licensing of electronic signature services and issuing of digital certificates.[60]

The Tanzania Communications Regulatory Authority (TCRA) is the regulator of cryptographic and certification services. The communication sector is vast, which means the TCRA might have difficulties undertaking its duties. Ideally, the regulation of electronic signatures should have been left to another institution. Nevertheless, there are other institutions playing a role in regulating electronic signatures not set out in legislation. They do so by virtue of their position. These institutions are the BoT, eGA, National Identity Agency (NIDA), and private commercial banks. The BoT regulates commercial banks, the eGA approves and monitors development of all electronic government projects, and the NIDA issues National Identities both manual and electronic. In so far as the regulation of electronic

[44] ETA s7.
[45] Anna Nordén, 'Electronic signatures in a legal context', pp. 156-157.
[46] Mason, Chapter 7 'Electronic signatures', 7.286-7.297.
[47] [Cap 6 R.E. 2019].
[48] ETA s6.
[49] ETA ss33-36.
[50] ETA s3.
[51] ETA s6.
[52] ETA s7 and s8.
[53] ETA s12.
[54] ETA s9.
[55] ETA s10.
[56] ETA ss33-36.
[57] ETA ss18 and 46; the Evidence Act [Cap. 6 R.E. 2019] (TEA) s64A.
[58] ETA s13(4).
[59] ETA s33.
[60] ETA s34; ETA Regulations (G.N. No. 228 of 2016).

signatures is concerned (with exception of the eGA managing the government's digital authentication framework[61]), the powers and functions of these institutions in the electronic signature cycle are not clearly articulated in legislation. Hence the rights and duties of the parties involved may be contractual. For example, the issuance of a PIN for bank cards that can be used in ATMs remains a contractual arrangement between a bank and its customer.

Despite the above legal framework, there is uncertainty. While the parties to a contract are free to use the electronic signature of their choice unless the law prescribes otherwise,[62] this freedom of choice is qualified with the preference for the secure electronic signature.[63] Interestingly, provisions for secure electronic signatures may also be regarded as non-discriminatory, for it merely sets out what attributes an electronic signature needs if it is to be considered secure.[64] Thus, any electronic signature is legally recognized providing it meets the attributes set out in ETA s7.

Forms of electronic signature other than PKI signatures

Despite the ETA recognizing PKI electronic signatures, the implementation of the intimated PKI electronic signatures regime in Tanzania has not been realized. There is no PKI infrastructure in place. That is not to say people are not using electronic signatures. As mentioned above, other forms of electronic signature are used in sending text messages, sending email, using the PIN to take out money from an ATM.[65] Further, it must be emphasised that the definition of an electronic signature is very wide, and includes all forms of electronic signature, not just digital signatures using a PKI, as discussed below.

Clearly, commercial organisations incorporate security features when dealing with customers. For instance, where a bank offers electronic banking services to its customers, the bank issues the customer with a username and password to obtain access to online services. This process differs from one bank and another. When a customer logs onto their electronic banking platform, some banks will send a notification to their mobile telephone that the account is being viewed. During this interaction by the software, the browser and the Internet Protocol address will be recorded by the bank (unless the customer uses a VPN or other mechanism to make it appear that they are obtaining access to the account from another country).[66] Additionally, a bank receives a code to his mobile telephone or email address instantly which must be used within a short period of time to authenticate the customer before approving or confirming the funds transfer.

The electronic signature at the bottom of an email is used widely. There are instances where a signature applied via text message may be valid, for example, in a loan agreement over text message, where the court in China held that the data exchanged via mobile telephones in text messages can be admitted in evidence.[67] In other jurisdictions this has extended to torts such as defamation. The latter was the dispute in *Lazarus Mirisho Mafie and M/S Shidolya Tours and Safaris v. Odilo Gasper Kilenga alias Moiso Gasper*[68] where an email was admitted as evidence to prove that a defamatory email was from the defendant. The court also examined whether an email address may be used to prove that it was indeed the defendant who sent the defamatory email.

ATM cases in Tanzania

There have been a few cases where people have relied on the PIN in an ATM as evidence, in disputes brought before the courts. That extends to where the PIN for use in an ATM or mobile banking such as SIM Banking or an M-PESA

[61] The e-Government Act s5.
[62] ETA s6(3).
[63] ETA s7.
[64] Thanks to Stephen Mason for this observation.
[65] For cases where the PIN is compromised or money fraudulently withdrawn from ATMs, see *National Microfinance Bank (PLC) v Delphina Ikanda Mama*, Civil Appeal No.149 of 2017, High Court of Tanzania, Dar es salaam District Registry at Dar es salaam (unreported); *Mwanswa Jones' case*.
[66] See, for instance, https://en.wikipedia.org/wiki/Internet_geolocation and https://en.wikipedia.org/wiki/Geo-blocking .
[67] *Yang Chunning v. Han Ying*. (2005) hai min chu zi NO.4670, Beijing Hai Dian District People's Court. See case translation and commentary in *Digital Evidence and Electronic Signature Law Review*, 5 (2008), pp. 103–5; see Mason, *Electronic Signatures in Law*, Chapter 3 'The practical issues in using electronic signatures', at 125.
[68] Commercial Case No. 10 of 2008, High Court of Tanzania Commercial Division at Arusha (Unreported).

account have been compromised and money has been fraudulently withdrawn, for which see *National Microfinance Bank Ltd v Michael Obey Daud*.[69]

The more frequent issues before the court are customer protection, customer negligence in handling the PIN, the bank breaching fiduciary duty, weak security of the system, vulnerabilities of the mobile banking system, etc.[70] Surprisingly, the reliability of the PIN is not examined. The customer trusts the system without having knowledge about the system itself.[71] A bank might claim that the customer divulged the PIN to third parties. If proved, the bank will not be liable. But where the customer proves he or she did not authorise a third party to obtain access to his or her account, the bank may be liable.[72] The customer has a duty to notify the bank once the PIN is compromised. What is gathered from the relationship between banker and customer in electronic banking is that it relies on trust and this may include trust that the software and the machine are working correctly.[73]

Assessing the evidence where an electronic signature is in dispute can be of significant concern. For instance, some judges may tend to believe the assurance given by a witness for the bank in the absence of any evidence.[74] The bank customer may be accused of negligence that he or she has shared his PIN with a third party who in turn obtained access to his or her bank account.[75] This conclusion is reached in ignorance of the fact that the software may have its inherent problems or may be accessed without the knowledge of the customer.[76] The possession of an ATM card and PIN is not conclusive evidence that a thief cannot obtain access to the customer's bank account and withdraw cash.[77] It is suggested that the advice offered by the Supreme Court of Lithuania in their sage judgment in the case of *Ž.Š. v Lietuvos taupomasis bankas* is of great value in aiding judges in assessing the evidence, as set out at page 259:[78]

> … in the event of a dispute between the bank and the card holder concerning the use of PIN code (electronic signature), the bank must provide the probative evidence regarding the particular actions or inaction of the card holder that would prove the use of the PIN code (electronic signature) with the card holder's knowledge

[69] Civil Appeal No.51 of 2020, High Court of Tanzania at Mwanza (unreported) available at https://tanzlii.org/tz/judgment/high-court-tanzania/2021/3154.

[70] See Ubena John and Caroline Mutalemwa, 'Are the customers' rights protected against fraud in mobile banking in Tanzania: a review of laws and practice', Institute of Judicial Administration Law Journal (forthcoming 2022).

[71] Mason and Reiniger, '"Trust" Between Machines? Establishing Identity Between Humans and Software Code, or whether You Know it is a Dog, and if so which Dog?', p. 135.

[72] See *Vodacom (T) Limited and NMB v Mwanswa Jonas* Consolidated Civil Appeals No. 1 and No. 2 of 2016, High Court of Tanzania at Mbeya (unreported).

[73] For history of trust in machines see Richard Warner and Robert H. Sloan, "Vulnerable Software: Product-Risk Norms and the Problem of Unauthorized Access" (2012) 45 *Journal of Law, Technology & Policy* 45; see also Mason and Reiniger, '"Trust" Between Machines? Establishing Identity Between Humans and Software Code, or whether You Know it is a Dog, and if so which Dog?', p. 135.

[74] Maryke Silalahi Nuth, "Unauthorized use of bank cards with or without the PIN: a lost case for the customer?" (2012) 9 *Digital Evidence and Electronic Signature Law Review* 95; see *National Microfinance Bank (PLC) v Delphina Ikanda Mama*, Civil Appeal No.149 of 2017, High Court of Tanzania, Dar es salaam District Registry at Dar es salaam (unreported).

[75] *National Microfinance Bank (PLC) v Delphina Ikanda Mama*, Civil Appeal No.149 of 2017, High Court of Tanzania, Dar es salaam District Registry at Dar es salaam (unreported).

[76] Stephen Mason, "Debit cards, ATMs and negligence of the bank and customer" (2012) 27(3) *Butterworths Journal of International Banking and Financial Law* 163; Stephen Mason, "Electronic banking and how courts approach the evidence" (2013) 29(2) *Computer Law and Security Review* 144; Mason and Reiniger Esq., '"Trust" Between Machines? Establishing Identity Between Humans and Software Code, or whether You Know it is a Dog, and if so which Dog?', p. 135.

[77] There seems to be a wrong assumption in some cases (*NMB v Michael Obey Daud HC*, Civil Appeal No.51 of 2020, HCT Mwanza (unreported) and *NMB v Delphina Ikanda Mama* Civil Appeal No.149 of 2017, High Court of Tanzania, Dar es salaam District Registry at Dar es salaam (unreported)) that it is a bank customer who knew his PIN, which meant that the withdrawal from the ATM could not be done by anybody save by the customer or a person who had been given the PIN by that customer. That was held without a critical analysis being done.

[78] Civil case No. 3K-3-390/2002, Supreme Court of Lithuania, translated by Sergejs Trofimovs, 6 *Digital Evidence and Electronic Signature Law Review* (2009) 255 – 262; see also the helpful advice offered to members of the judiciary in two important papers: Paul Marshall, James Christie, Peter Bernard Ladkin, Bev Littlewood, Stephen Mason, Martin Newby, Jonathan Rogers, Harold Thimbleby and Martyn Thomas CBE, Recommendations for the probity of computer evidence', 18 *Digital Evidence and Electronic Signature Law Review* (2021) pp. 18-26 and Michael Jackson, 'An approach to judging evidence from computers and computer systems' 18 *Digital Evidence and Electronic Signature Law Review* (2021) pp. 50-55.

or due to his negligence or lack of care. The bank also bears the obligation to prove that the original PIN code (electronic signature) was used, i.e. the electronic signature, which identifies the specific person – the bank's client. The sufficient basis of transfer of burden of proof to the card holder may be established only in those cases where the original PIN code is used, and in accordance with the present level of equipment and in accordance with the requirements as to the formation and usage of such a signature, this signature could not have been reproduced without the holder's knowledge or negligence.'

Electronic Transactions (Cryptographic and Certification Service Providers) Regulations

Cryptography and certification are at the core of PKI. It is for this reason the Cryptographic and Certification Services Providers Regulations[79] were promulgated. The regulations regulate cryptographic and certification services in Tanzania, and the Minister responsible for communications is empowered to designate an institution to regulate electronic signatures, especially cryptographic and certification services.[80]

Electronic evidence law

Prior to the enactment of ETA in 2015, the electronic signature lacked statutory legal validity. An electronic signature was inadmissible as evidence and hence unenforceable in the courts of law in Tanzania. The ETA recognized electronic transactions. It also recognized data message as evidence. The ETA amended the Evidence Act [Cap 6 R.E. 2019] to the effect that electronic evidence is admissible in the courts of law in Tanzania.[81] In determining the admissibility and evidential weights of evidence in electronic form, s18(2) of the ETA provides for the following to be considered:

(a) the reliability of the manner in which the data message was generated or communicated;

(b) the reliability of the manner in which the integrity of the data message was maintained;

(c) the manner in which the originator was identified; and

(d) any other factor that may be relevant in assessing the weight of evidence.

Electronic evidence cases in Tanzania

The role of the judiciary towards the change of legal framework on the admissibility of electronic evidence and the issue of authenticity should not be understated. Several cases have been decided by the High Court of Tanzania, which include *Trust Bank Ltd v Le-marsh Enterprises Ltd, Joseph Mbui Magari, Lawrence Macharia*;[82] *Lazarus Mirisho Mafie and M/S Shidolya Tours and Safaris v Odilo Gasper Kilenga alias Moiso Gasper*;[83] *Exim Bank (T) Ltd v Kilimanjaro Coffee Company Limited*;[84] and *William Mungai v Cosatu Chumi*.[85] Some of these cases focused on the issue of the authenticity of the electronic evidence.[86]

Controversies have emerged in the courts as to whether a signature is essential in determining the reliability of data messages as evidence. In *Ami Tanzania Limited v Prosper Joseph Msele*,[87] the Court of Appeal of Tanzania held that a signature is not required under section 18 of ETA to fulfil data message reliability requirements. However, in *Stanley Murithi Mwaura v R*,[88] the Court of Appeal held that the admissibility of electronic evidence depends on fulfilling the requirements[89] of proving the reliability of the data massage as stipulated in s18(2) of the ETA. As held in many cases in the High Court, the reliability of a data message can be proved by showing that the manner through which the

[79] G.N. No. 228 of 2016.
[80] ETA s33.
[81] ETA s46; TEA s64A.
[82] [2002] TLR 144.
[83] Commercial Case No.10 of 2008, HC Commercia Division at Arusha (Unreported).
[84] Commercial Case No. 29 of 2011 (HC Commercial Division at Dar es salaam) (Unreported).
[85] Election Petition No.8 of 2015 (HC at Iringa) (Unreported).
[86] Each of these cases are discussed in Ubena John, 'Legal issues surrounding the admissibility of electronic evidence in Tanzania', 18 *Digital Evidence and Electronic Signature Law Review* (2021) 56-67.
[87] Civil Appeal No. 159 of 2020, Court of Appeal of Tanzania at Dar es salaam (Unreported) (judgment delivered on 11 November 2021).
[88] Criminal Appeal No. 144 of 2019 Court of Appeal of Tanzania at Dar es salaam (Unreported) (decided on 22 November 2021).
[89] Holding that they are 'requirements' may be controversial as these are 'attributes' that ought to be considered.

message was created, stored, or communicated was reliable, or how the originator was identified was reliable. These may be partly achieved by using a digital signature, because it has a capacity to provide for the confidentiality, integrity, and authenticity of the data, although using a digital signature will not provide for absolute certainty, because of the weakness of the IT systems.[90]

Electronic and Postal Communications Act

The Electronic and Postal Communications Act, Act No. 3 of 2010 (EPOCA) provides for the functions of TCRA. It provides for a licensing framework of electronic communications service providers. It also empowers the TCRA to regulate standards and competition in electronic communications. The EPOCA provides for the Computer Emergence Response Team (CERT). The team is charged with a duty to investigate internet security issues in Tanzania, including identifying criminal activities and malicious code.

Tanzania Communications Regulatory Authority Act

The Tanzania Communications Regulatory Authority Act, Act No. 12 of 2003 (TCRA) established the post of Regulator of Communications.[91] The main functions of the TCRA are to regulate the communications sector with the aim of guaranteeing the availability of communications services, interconnection, interoperability, and competition. However, because the TCRA has many duties to perform (under EPOCA, TCRA, CCA, etc.) it is debatable whether it has the capacity to regulate PKI digital signatures effectively under the ETA.[92]

The e-Government Act, 2019

To implement electronic government in Tanzania, the legislature in 2019 enacted the e-Government Act,[93] although the adoption of ICT for the provision of public services started earlier. It was in 2009 that the government issued a circular dated 9 October 2009 on the use of ICT in public services. The circular was issued by the Permanent Secretary, in the Ministry of President's Office – Public Service. It provides, among other things, for the proper and secure use of ICT in government services. There are also the e-Government General Regulations.[94] The overall purpose of the Regulations is to implement electronic government in Tanzania.

In 2012 under the Executives Agencies Act of 1997,[95] the Electronic Government Agency (eGA) was established as a semi-autonomous agency. The agency later became the e-Government Authority regulating the development and use of e-government systems. The e-Government Act provides for the authority to coordinate, oversee, and promote e-government initiatives and enforce e-government related policies, laws, regulations, standards, and guidelines in public institutions.[96] Another function of the eGA is to establish and maintain a secure shared government ICT infrastructure and systems.[97] A good example is the development of the e-office, explained below. It further develops mechanisms for the enforcement of ICT Security standards and guidelines, the provision of support for ICT security operations, and implementation of government wide cyber security strategies.[98] The eGA has been instrumental in developing various ICT systems and applications for the government and public services generally. For example, the government mailing system, electronic office (e-office) management system, land use and management system, etc.

The Electronic Government Authority and PKI signature

The above laws and the Electronic Government Authority (eGA) played a significant role in operationalization of digital (PKI) signature in government and public service in Tanzania. In 2016, the eGA was charged with a task to

[90] The weakness of software is discussed in depth, with numerous examples, in Mason, Chapter 5 'The presumption that computers are "reliable"' in Mason and Seng, *Electronic Evidence and Electronic Signatures*, and the proof that digital signatures can be undermined and forged is discussed at 7.254.
[91] TCRA Act, 2003 s4.
[92] ETA s34.
[93] Act No. 10 of 2019.
[94] e-Government General Regulations of 2020, G.N. No. 70 published on 7 February 2020.
[95] [Cap 245 R.E. 2002].
[96] The e-Government Act s5.
[97] The e-Government Act s5.
[98] The e-Government Act s5.

develop the electronic office (e-office) management system.[99] The development of the system was completed in September 2017. This system has minimized the use of paper in government offices. It is now possible to manage files electronically. All government entities are required to use the government mailing system and be connected to the government network – GovNet – to use the e-office management system.[100]

The e-office management system also uses the digital (PKI) signature. The eGA is the Certification Authority.[101] This PKI infrastructure is called the eGov PKI and Digital Signature Management System (DSMS).[102] The users are chief executives and the officers managing government registries. The PKI adopted the X.509 standard.[103] Under the eGA PKI and DSMS, there is registration authority which receives digital certificate requests from a particular government entity. It verifies the identity of the requestor and approves it. Thereafter, the approved request is forwarded to the Certification Authority (eGA).[104]

While the above PKI and DSMS works fine, no guidelines have been issued on the rights, duties and liabilities of parties involved in the PKI cycle. Neither the eGA nor TCRA has issued the certificate practice statement.

Weaknesses in the existing laws

Among the major defects of the current laws relevant to PKI in Tanzania is the failure to address the rights, duties and liabilities of the parties involved in PKI. For instance, the ETA and G.N. No. 228 do not provide for the rights, duties, and liabilities[105] of the main participants in the PKI framework, although it does provide for the liability of the electronic signature on the relying party in s12:

> A person who relies on an electronic signature shall bear the legal consequences 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.

It should be noted that this provision merely reinforces the need for the relying party to satisfy themselves that the signature is of the person who it claims to be. The relying party has always had the burden of proving a signature is not a forgery.

Another weakness is the provision of non-exhaustive elements of PKI in the regulations (G.N. No. 228). Some elements such as registration authority, repository, validation authority, subscriber, certificate policy and subscriber (and relying party) agreement are excluded. Admittedly, these may be included in the certificate policy or certificate practice statement.

The lack of provision for the vetting or verification of PKI signature users is a shortcoming. Although the Electronic and Postal Communications Act[106] requires the registration of SIM cards, there are no requirements for the registration of laptops or desktop computers. Moreover, there is no system for registration of internet users. Similarly, the G.N. No. 228 deals with the registration and licensing of cryptographic and certification service providers and not PKI signature users.

[99] The system website is at http://eoffice.gov.go.tz.
[100] The eGA and Department of Archives and Records, training material on e-office (*Mfumo wa Ofisi Mtandao*), May 2022 (unpublished) (on file with the author).
[101] For details on systems developed by eGA see https://www.ega.go.tz/e-services/government-to-government-g2g.
[102] The eGA and Department of Archives and Records, training material on e-office, May 2022 (unpublished) (on file with the author).
[103] The eGA training material on Digital signatures, (unpublished) (on file with the author).
[104] The eGA training material on Digital signatures, (unpublished) (on file with the author).
[105] These may however be stated in the certificate practice statement.
[106] Act No.3 of 2010.

Moreover, there is a lack of legal provisions to establish an institution to undertake the verification of PKI signature users. Both the TCRA Act and EPOCA are silent on this point. Without verifying a user, there is risk that cybercriminals can use the service.

Furthermore, current agreements between vendors, Certifications Authorities (CAs) and users seem to be self-regulating. They are unregulated by the relevant authorities. Neither the ETA nor the G.N. No. 228 regulates these agreements. It is unclear whether the regulator (TCRA) under G.N. No. 228 is responsible. Without such regulation, the interests of consumers and end users may be at stake. The terms contained in the agreements may be used by the CAs to exempt themselves from liability.

The above discussion makes it clear that the regulations do not include the issues raised. It is possible that these matters might be covered under the provisions of ETA s11, where it provides that before the grant of a licence, the regulator has to approve a certification practice statement – all of the issues raised in the four paragraphs above can (and should be) be covered in the certification practice statement. What seems to be missing is a guide on certificate policies and certificate practice statements, as with the Australian framework. Additionally, although the accreditation process or licensing is covered in the regulations, it remains unclear who has been granted licences or has been accredited to provide cryptographic and certification services. The media outlets, including the TCRA website, are silent on this. Thus, there is no evidence that the PKI framework has been implemented except for the eGA PKI and DSMS that is used as the digital authentication framework in the e-Office Management System.

An additional problem is the lack of a privacy and data protection law in Tanzania. A privacy and data protection law ought to be enacted because the absence of such a law jeopardizes the security of PKI signature users' personal data. Arguably, the cryptographic and certification service providers should be subject to appropriately legal binding requirements regarding privacy and data protection in association with the use of their services and the technologies used. This suggestion is informed by the fact that even the EU eIDAS has recognized the need to embrace and employ data protection rules and principles within the electronic signature framework.[107] Similarly, the Australian Gatekeeper PKI Framework has included a privacy impact assessment component which is drawn from the Privacy Amendment (Enhancing Privacy Protection) Act 2012. The Act sets out standards, rights, and obligations for the handling, holding, accessing and correction of personal information (including sensitive data).[108]

Moreover, there is an absence of an information security policy, although a National Information and Communications Technology Policy does exist.[109] We believe that is not enough. There ought to be a National Information Security Policy that will provide a vision and strategies of the Tanzania government on information security.

There is a need for a clearly established or accredited institution to deal with authentication frameworks. To that end Tanzania may borrow a leaf from other countries such as Australia where the Digital Transformation Office is responsible for regulating all government authentication frameworks,[110] and South Africa's SAPO and LAWTRUST. The tasks of managing the government digital authentication frameworks, including the PKI, has been given to the Electronic Government Authority in accordance with the e-Government Act.[111] There is a need to accredit companies to provide a digital authentication framework for the private sector. There seems to be no encumbrance on this because any private company may apply to TCRA, which is the accreditation entity for issuing a licence to provide cryptography and certification services. Nevertheless, even prior to the implementation of the ETA regulations, private commercial banks, owners of online shops and online marketplaces appear to have offered cryptography and

[107] Article 5 of the eIDAS provides for the application of the Consolidated text: Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance), OJ L 119 4.5.2016, p. 1, Corrigendum, OJ L 127, 23.5.2018, p. 2 ((EU) 2016/679), especially with respect to data processing and protection.

[108] Section 8.2 of Gatekeeper PKI Framework.

[109] https://www.ega.go.tz/uploads/publications/sw-1574848612-SERA%202016.pdf.

[110] Australia DTO manages all government authentication frameworks, at https://www.dta.gov.au/news/dto-now-manage-government-authentication-frameworks.

[111] See The e-Government Act s5.

certification services. But for legal validity, admissibility, and enforceability of electronic signature, regardless as to who manages the authentication framework, the requirements set under ETA must be observed.[112]

Adjusting to PKI

As it has been observed in the discussion above, there are several gaps in the existing laws that support PKI and NPKI. The identified gaps ought to be addressed if the operationalization of NPKI is to be successful. The following laws are recommended to be put in place.

One, the law needs to be enacted to make provision for the rights, duties, obligation, and liabilities of the parties involved in PKI. This may be achieved by amending G.N. No. 228. It is essential for the rights, duties and liabilities of the parties involved in the PKI cycle to be defined. This may also be achieved by a certificate practice statement. Without setting out these rights, duties and liabilities, the NPKI might never be put into operation.[113]

Two, the amendment to G.N. No.228 should, ideally, include the following: registration authority, repository, validation authority, subscriber, certificate policy and subscriber (and relying party) agreement. Moreover, the regulations should be reformed to provide for the registration and digital authentication agencies (Bank of Tanzania and Tanzania Posts Corporation as rightly suggested in the NPKI consultancy report). If that is not viable at the time of writing, then more private companies should be encouraged to apply to TCRA for accreditation or licensing for the provision of digital authentication or cryptography and certification services.

Three, the G.N. No. 228 should further provide for proofing and vetting or verification of PKI signature subscribers and users. The identify verification of electronic signature users is essential. Without such identity proofing, the key holders may not be known.

Four, it is important to amend the Bank of Tanzania Act 2006 and Tanzania Posts Corporation Act.[114] G.N. No. 228 should include legal provisions to establish which institution is to undertake verification or proving identity of PKI signature subscribers. This is like the role of the SAPO Trust Centre in South Africa. In Tanzania, the users' identity verification process may be carried out by the Bank of Tanzania and Tanzania Posts Corporation. If that would have been the case, the laws establishing these institutions ought to have been amended to provide for such a role. While the authentication of digital transactions is an important factor for the prosperity of electronic commerce and electronic government transactions, one may wonder about the readiness of the Tanzania Posts Corporation to assume such a role or whether there should there be new institutions accredited to support implementation of cryptography and certification services. Although there seems to be bias in suggesting the use of Tanzania Posts for this purpose. Tanzania Posts has a vast network and an online shop,[115] which might be useful in establishing these types of service. This would not restrict the adoption of PKI by other organizations. Although the BoT and Tanzania Posts Corporation were considered to be in a better position to manage the government's PKI and Digital Signature Management System (DSMS)[116] it was the eGA that developed and manages it.[117] Additionally, it has developed many other e-government systems. Intriguingly, the eGA is a regulatory authority whose function as the regulator may be reconsidered if it concentrates on developing systems instead of regulating others to develop and use the e-government systems. It is not too late to apportion and align the roles in developing and regulating digital authentication framework for public entities.

Five, the enactment of a Privacy and Protection Act is equally important. A privacy and data protection law should be enacted to secure the privacy and personal data of PKI signature users. This law should aim to impose obligations on cryptographic and certification service providers to adopt strategies to secure the privacy of users. As evidenced in countries such as South Africa, the operation of NPKI involves the massive use of personal data. Thus, a privacy and

[112] ETA s7.

[113] Wikipedia, certificate policy, available at https://en.wikipedia.org/wiki/Certificate_policy; see also RFC 2527; S. Chokhani and W. Ford (November 2003) Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework at https://datatracker.ietf.org/doc/html/rfc3647#page-16. See also section 4.3 of the Gatekeeper PKI Framework.

[114] [Chapter 303 R.E. 2019].

[115] See Tanzania Posts online shop at https://www.postashoptz.post/.

[116] It can safely be stated that eGA took advantage of its mandate given under the e-Government Act s5.

[117] It derived its mandate from the e-Government Act s5.

data protection law if enacted will help to set the parameters on the use of such personal data in the NPKI framework in Tanzania. Although there has been delay in enacting such an act, a Bill has already been drafted. What is unclear though is when it will be enacted into law.

Except for point five, and in alternative to some changes into the laws suggested at points 1-4, it might be possible to adopt a Certification Policy and Certification Practice Statement similar to the Australian Gatekeeper PKI Framework. A similar result can also be achieved via a certification practice statement. Tanzania may draw lessons from the Gatekeeper PKI Framework of Australia. Even though the framework was meant for government agencies, private organisations are not precluded from using it as a model.

Six, the formulation of a National Information Security policy. There ought to be National Information Security Policy that will provide a vision and strategies for the Tanzania government on information security. The cryptographic and certification providers will equally be required to have in place information security documentation which will indicate their risk management approach. The regulator may be empowered to impose a penalty on providers who lack adequate information security documentation. For government entities information security issues have been taken care of by the e-Government Act whose implementation is through the eGA.[118]

Conclusion

This article has examined the implementation of the electronic signature law in Tanzania and identified several gaps in the laws. Suggestions have been made to remedy the lacunae. Changes can be made swiftly via the relevant regulatory authorities – although it will be necessary to provide for greater certainty via changes in the law. The recommendations offered in this article are offered in the diligent hope that those in government acknowledge the need to act, and to act swiftly.

Ubena John is a Judge in the High Court of Tanzania, and senior lecturer at the Faculty of Law, Mzumbe University, Tanzania.

jubena@mzumbe.ac.tz

[118] The e-Government Act s5 & ss36-46.