KAPLAN&STRATTON NEWSLETTER

LEGAL RECOGNITION OF ELECTRONIC SIGNATURES IN KENYA

Sarah Kiarie-Muia

Partner

Mercy Kirui

Associate

1. Introduction

The Kenya Information and Communications Act, No. 2 of 1998 (**KICA**) recognizes the use of advanced electronic signatures in Kenya as equal to traditional handwritten signatures commonly referred to as wet ink signatures.

The Business Laws Amendment Act, 2020 (which came into force on 18 March 2020) also amended a number of statutes (the Law of Contract Act, the Registration of Documents Act and the Land Registration Act) to recognize the use of advanced electronic signatures.

An **advanced electronic signature** is an electronic signature that meets the following requirements:

(a) is uniquely linked to the signatory;

(b) is capable of identifying the signatory;

(c) is created by means that the signatory can maintain under his sole control; and

(d) is linked to the data to which it relates in such a manner that any subsequent change to the data is detectable.

2. Who can use an electronic signature and what kind of documents can be validly executed?

All documents/instruments except wills and negotiable instruments may be signed using advanced electronic signatures.

There are also no restrictions on the persons that can use an electronic signature and accordingly, natural persons and corporates can validly execute documents using electronic signatures. Companies must however comply with the provisions of the Companies Act, 2015 which provides that a document is validly executed by a company if it is signed on behalf of the company by:

(a) two authorized signatories (i.e. a director or secretary for private companies and in the case of a public company, a director, the secretary or a joint secretary); or

(b) by a director in the presence of a witness who attests the signature; or

(c) a person duly authorised by the company under a power of attorney execute documents on its behalf.

3. Are there any requirements for a valid electronic signature?

The KICA provides that where any law requires a signature of a person, that requirement is met in relation to an electronic message if an advanced electronic signature is used that is as **reliable** as was appropriate for the purpose for which the electronic message was generated or communicated. An advanced electronic signature is considered to be reliable for the purpose of satisfying this requirement if:

(a) it is generated through a signature-creation device (configured software or hardware used to implement the signature-creation data);

(b) the signature creation data are, within the context in which they are used, linked to the signatory and to no other person.**Signature-creation data"** means unique data, such as codes or private cryptographic keys, which are used by the signatory to create an electronic signature;

(c) the signature creation data were, at the time of signing, under the control of the signatory and of no other person;

(d) any alteration to the electronic signature made after the time of signing is detectable; and

(e) where the purpose of the legal requirement for a signature is to provide assurance as to the integrity of the information to which it relates, any alteration made to that information after the time of signing, is detectable.

4. What is the role of certification service providers?

Under the Evidence Act, in order to ascertain whether an electronic signature is that of a person by whom it purports to have been affixed, the court may direct:

(a) that person or the certification service provider to produce the electronic signature certificate; or

(b) any other person to apply the procedure listed on the electronic signature certificate and verify the electronic signature purported to have been affixed by that person.

Accordingly, it would be prudent to have the advanced electronic signature supported by an advanced electronic signature certificate issued by a certification service provider (**CSP**). The certificate supports an advanced electronic signature and confirms the identity or other significant characteristics of the person who holds a particular key pair; identifies the certification provider issuing it; names or identifies the person to whom it was issued; contains the public key of the person to whom it is issued and is signed by a responsible officer of the CSP issuing it.

KICA prohibits persons from operating an electronic certification system without a license and mandates the Communications Authority of Kenya (**CA**) to grant licenses authorizing a

person to provide electronic certification services.

The CA may also recognize foreign CSPs e.g. DocuSign as certification service providers in accordance with the Kenya Information and Communications (Electronic Certification and Domain Name Administration) Regulations 2010. To qualify for such recognition the foreign CSP should:

(a) be duly licensed in its country of operation;

(b) comply with the standards and requirements under KICA and the regulations under it; and

(c) establish a local agent to provide the certification services in Kenya.

On 1 September 2020, the CA issued a public notice requiring foreign certification providers operating in Kenya to apply for recognition of their services within 30 days from the date of the notice. As at the date of this note, we understand from the CA that it has recognized one foreign CSP and licensed one local CSP.

It would therefore be important to confirm that your electronic signature provider is licensed or recognized by the CA as a CSP or has a licensed or recognized CSP for purposes of issuing an electronic signature certificate to support of the validity of your advanced electronic signature in the event that the electronic signature is contested.

5. Conclusion

Kenyan law recognizes electronic signatures as a valid form of execution by all legal persons. However, the law prohibits the use of such signatures in certain instances including in the creation and execution of wills and negotiable instruments.

Further, CSPs must be licensed (in the case of local CSPs) or recognized (in the case of foreign CSPs) by CA in order to operate an electronic certification system in Kenya. The validity of an electronic signature may therefore be in jeopardy if the relevant document was executed by an advanced electronic signature attributed to an unlicensed or unrecognized CSP. To safeguard against this risk, parties should ensure that all advanced electronic signatures are issued by a CSP that is licensed or recognized by the CA.

If you require any further information or clarification on the contents of this note, please contact:

Sarah Kiarie-Muia: SKiarie@kapstrat.com

Mercy Kirui: MChemutai@kapstrat.com