



AMAN &
PARTNERS

LEGAL UPDATE

ISSUE 10

LEGAL RECOGNITION OF ELECTRONIC SIGNATURE IN ETHIOPIA

SEPTEMBER 2023



BOWMANS
ALLIANCE FIRM

ELECTRONIC SIGNATURE IN ETHIOPIA

The use of electronic modalities for the purpose of facilitating transactions is rapidly growing in Ethiopia. With a view to regulating this progress, the Ethiopian government has been adopting policies and legislations, including the Proclamation to regulate Electronic Signature No. 1072/2018 [“E - signature Proclamation”] issued in 2018.

This legal update outlines selected legal developments and implications as covered in the E-signature Proclamation with a particular focus on: (i) meaning of E-signature and scope of the E-signature Proclamation; and (ii) the legal recognition of E-signature.

MEANING OF E-SIGNATURE AND SCOPE OF THE E-SIGNATURE PROCLAMATION

DEFINITION

The term “Electronic Signature” is defined as information affixed or logically associated to an electronic message that may be used to identify the signatory as well as the signatory’s approval of the information contained in the electronic message. As such, E-signature includes but is not limited to affixing a scanned signature, email communications including typed name or clicking to agree on Terms and Conditions.

The E-signature Proclamation also defines the term, “Digital Signature”. Unlike the broader definition of Electronic Signature, the term “Digital Signature” is described as a type of specific E-signature (a particular system) capable to provide reliable digital signature and encryption services called asymmetric cryptosystem. The asymmetric cryptosystem is required to fulfill four specific requirements related to identifying the signatory and linking the signature with the signatory. These requirements are: (i) unique link to the signatory; (ii) capability to identify the signatory; (iii) creation of the signature using a private key that the signatory has a sole control; and (iv) detectability of signature or ability to identify subsequent changes. These requirements are intended towards enabling verification for parties’ identity, authentication of messages and ensuring non-repudiation.

SCOPE OF THE E-SIGNATURE PROCLAMATION

The scope of application of the E-signature Proclamation extends to any electronic message exchange unless governed by other laws on electronic message. The term “Electronic Message” is defined under the E-signature Proclamation as information generated, sent, received, or stored by electronic means.

The E-signature Proclamation recognizes actors in the implementation of E-signature, including the Root Certificate Authority, the Certificate Service Provider, Subscriber and Relying Parties. In this regard, it empowers the Information Network Security Agency (INSA) as the Root Certificate Authority.



As a Root Certificate Authority, the INSA is mandated to ensure the trustworthiness and overall security of the cryptosystem; issue licenses to certificate providers and monitor their activities; and formulate working procedures for certificate providers. However, up until date, INSA has not fully commenced its operations as per this Proclamation and neither has it registered nor issued certificate for any Service Provider in Ethiopia. The powers, responsibilities and duties of actors incorporated in the E-signature Proclamation will be discussed in our future legal update.

LEGAL RECOGNITION OF ELECTRONIC SIGNATURE

The E-signature Proclamation prescribes that in any legal proceeding, neither an electronic message nor an electronic signature shall be denied legal effect, validity or admissibility as evidence on the ground that it is in electronic form. The E-signature Proclamation deems the requirement of a signature as being fulfilled when a reliable E-signature is used. In this regard, there are two circumstances in which the requirement for a reliable E-signature is deemed to have been fulfilled:

- (a) the appropriateness for the purpose the message is generated; agreement entered between the parties regarding electronic signature; or considering other conditions such as nature, extent and type of transaction; or
- (b) Digital signature supported by a valid certificate from the Root Certificate Authority. Thus, while a digital signature is automatically regarded as a reliable signature, any other type of E-signature should meet the requirements under (a) above to be regarded as reliable one.

The E-signature Proclamation, in the context of civil proceedings, gives a legal presumption to a message with a reliable electronic signature, as to the link of an electronic signature with the signatory; signatory's intention to approve the electronic message; and non-alteration of the E-signature. However, the Proclamation provides that such presumption may be proved otherwise.

CONCLUDING REMARKS

In light of the recognition of E-signature under Ethiopian law, the signing of an agreement in an electronic form does not result in the invalidation of such agreement by the mere fact that it is signed electronically. That said, the recognition of E-signature does not exclude legal requirements under other laws such as requirements for witness, formality or signing of documents before relevant authorities. Regardless of the enactment of the E-signature Proclamation, the practical challenges arising from the implementation of this legal instrument have not been tested sufficiently. Moreover, delay in the commencement of operations by the Root Certificate Authority creates further uncertainty on the practical implementation of the E-signature Proclamation in general and the application of digital signature in particular.



AMAN & PARTNERS LEGAL SERVICE LLP

info@aaclo.com | www.aaclo.com

Disclaimer

The information contained in this legal update is only for general information purposes. Nothing herein shall be considered and relied upon as a legal advice or a substitute thereto.

© Aman & Partners LLP. All Rights Reserved 2023

