

Six Key Points on the Electronic Signature Law in Ethiopia

Description

By Yenatfanta Bekele

Introduction

Our society is dynamic through time. The way of our life evolved through many phases. Importance of law is that it also evolves or changes as we do. Contemporary world is being depended on digital platforms. Most of our activities are intertwined with the internet and digitalization including contracts.^[1] Thus laws that can be applicable to such issues are undeniably important. Most countries have such laws. Ethiopia enacted Electronic Signature Proclamation No. 1072/2018 in December 2018 G.C. the reasons are it has become necessary to provide legal recognition to the exchange of electronic messages and determine the rights and obligations of participating parties as provided in the preamble.

Definition of Electronic Signature

The definition of electronic signature contains almost the same elements in different jurisdictions or states. In the U.S.A it is defined as: "an electronic sound, symbol or process that is attached to or logically associated with a record and executed or adopted by a person with the intent to sign the record".^[2] In Ethiopia it is defined as information in electronic form, affixed to or logically associated with, an electronic message, which may be used to identify the signatory in relation to the electronic message and to indicate the signatory's approval of the information contained in the electronic message.^[3] Simply electronic signature means digital way of signature of electronic message that verifies the intention and acceptance of a certain message with intention to do so. There is also digital signature which is a type of electronic signature that uses asymmetric cryptosystem and is uniquely linked to the signatory; is capable of identifying the signatory; is created using a private key that the signatory has sole control; and is linked to the electronic message to which it relates in such a manner that any subsequent change of the electronic message or the signature is detectable as indicated under article 2(5).

Scope of the Law

As per to article 3 of proclamation No. 1072/2018; this specific law concerning electronic signature applies to any electronic message. In other word any messages or documents that are agreed upon by parties will be under the jurisdiction of law. Additionally any law or regulation or directive which is not consistent on matters covered and ruled by this proclamation will not be applicable according to article 53. Thus this law applies to any messages that are electronically signed but does not imply to documents but messages only. In the following paragraph I will try to highlight some of the issues concerned electronic signature based on proclamation No. 1072/2018.

Legality of Electronic Signature

Before the enactment of this proclamation laws, regulations and practices that mandatorily require handwritten signatures and documents.^[4] The enactment of Proclamation No.1072/2018 changed this requirement and broadened the acceptance of electronic signatures of messages in legal aspects according to article 5. Thus where any law requires that information shall be in writing, such requirement shall be deemed to have been satisfied if such information is rendered or made available in an electronic form and accessible so as to be usable for subsequent reference as per to article 5(2). Accordingly, the law presumes that the electronic signature is the signature of the subscriber; the electronic signature was affixed by that person with the intention of approving the electronic message; and the electronic message and the signature has not been altered since the specific point in time to which the electronic signature was affixed as per to article 7. However, this presumption rebuttable as the law allows if the contrary can be proven and this is also applicable to digital signature as per to article 8.

Authority and Certificate Providers

In order for this proclamation to be applied a government authority that executes it must exist. Thus article 9 provides that the Information Network Security Agency (INSA) shall act as the Root Certificate Authority pursuant to the mandate given to it in its establishment Proclamation. The certified certification will be effective for 5 year unless it is canceled or revoked or returned or terminated as per to the proclamation. Not just domestic certificate providers but also foreign certificate providers can be recognized as long as they comply as per to this law's requirements as provided under article 20. INSA has different powers and duties concerning the certificate. Generally, INSA has the power and responsibilities to issue license to certificate providers and monitor their activities and operations ensure the trustworthiness and the overall security of the crypto system; issue working procedures and standards that certificate providers shall follow as per to article 10.

Mainly, INSA has the power to suspend, cancel revoke that was issued before which is provided from article 14 up to 16. There are different reasons that are provided in order one's certificate to be suspended, cancelled or revoked. To list out some of them, for instance; INSA has the power to suspend to examine the occurrence of any of the grounds, which are stated under sub article of Article 15 of this proclamation that result cancelation of certificate provider licenses; or when the Root Certificate Authority considers that the grounds are not suffice to revoke the certificate provider license but defects are required to be corrected within a specified time and other. It also has the power to revoke certificate if the certificate provider breaches the provisions of this Proclamation or regulations and directives issued under this proclamation; it is proved that the license has been given based on falsified information; and other reasons.

In order for recognition there are some requirements that must be fulfilled. Any person may apply to acquire certificate upon satisfying requirements provided under this Proclamation and regulation and directives issued in accordance with this Proclamation and detailed terms and conditions set by the certificate provider. There are different obligations rested upon certificate provider. These responsibilities are to provide a time stamp service declaration that confirms the correct date and time of an act to a specific electronic message, digital signature or authenticity of a certificate; to provide encryption service in accordance with the requirements set by the Root Certificate Authority; to use trustworthy system; to have financial capacity to publish and inform the policy; and to keep custody of information for 2 years and with confidentiality unless agreed otherwise as described from articles 23

up to 29.

Subscribers

Not just the above persons but also subscribers are also provided with obligation as per to article 44. As the rest Root Certificate and certificate provider's subscribers have responsibilities and right. Subscribers have the obligation to provide accurate information; obligation to safeguard private key; obligation to request suspension or revocation of certificate and acceptance of certificate.

Dispute Remedy

Different persons as natural and legal persons are involved in the application of this proclamation. These are Root Certificate Authority, certificate providers, and subscriber or the users. Any kind of dispute may arise between two of these persons. Thus the law provides different settlement institutions. If a dispute arise between Root Certificate Authority and certificate providers can bring the case to National Crypto Council. If one of the parties needs to take appeal reasoning the decision can take their case to Federal High Court^[5]. On the other hand, if the dispute is between certificate providers, and subscriber or the users the dispute shall be settled by Root Certificate Authority. If any of the party need to take an appeal to Federal High Court.^[6]

Conclusion

As contemporary world is being depended on digital platforms and electronic connection, this way of life needed to be regulated which led the Ethiopian government to enact proclamation on electronic signature while broadening the protection of people in their changing world. The law regulates different issues that are concerned with electronic signature starting with requirements to be mate; and regulating how the electronic messages should be protected relaying on a set of responsibilities in order to protect the subscribers. It lays down different responsibilities and protection toward the Root Certificate Authority, Certificate provider and subscriber. Providing and mandating responsibilities towards one of these persons in return protect the rest. Thus the fact that the law has already regulated electronic signature is appropriate and timely.

[1]Eyasu Mekonen, Ethiopia enacted a new electronic signature law
<http://www.flslegalservices.com/2019/12/04/ethiopia-enacted-a-new-electronic-signature-law/#:~:text=The%20law%20stipulates%20that%20no,it%20is%20in%20electronic%20form.>

[2]The Electronic Signatures in Global and National

Commerce Act, <https://www.fdic.gov/regulations/compliance/manual/10/x-3.1.pdf> , March 1, 2001

[3] Electronic Signature Proclamation No. 1072/2018, 24th Year No.25 February 16, 2018 Art 2(6)

[4]Wossenyeleh Tigu and Abraham Arega, Regulation of E-signature in Ethiopia
www.mtalawoffice.com/legal-updates/entry/regulation-of-e-signature-in-ethiopia/#:~:text=In%20Ethiopia%2C%20there%20has%20been,the%20Electronic%20Signature%20Procl
. December, 2018.

[5] Proclamation No. 1072/2018 Art, 50

[6] Id Art, 51

Category

1. Blog Posts

Date Created

June 18, 2020

Author

dmethiol_admin

Dagnachew & Mahlet Law Firm LLP