Proclamation No. _____ /2022

Ethiopian Digital Identification Proclamation

Whereas the establishment of a reliable Digital Identification System in Ethiopia ensures the resident's right to be identified and enhances the ability to exercise other rights, promotes trust between service providers and consumers, and creates a nationwide enabling environment to ensure transparency, accountability, and efficiency;

Whereas establishing a technologically developed, inter-sectorial, foundational digital identification system, helps to plan national development effectively, achieve economic transformation, ensure good governance, reduce wastage of resources, eliminate redundancy and duplication, ensure inclusion support for effective policy design and execution of developmental plans, ensure fair distribution of resources among residents;

Whereas, deploying a nationwide Digital Identification system, fostering a reliable, accessible, and secure system, promoting the country's social, political, and economic development and predictability; ensuring the overall peace and security of the nation's resident,s and reinforcing the justice system;

Whereas the lack of a digital identification system in the country created a challenge for public and private sector entities from uniquely and reliably identifying individuals; moreover, residents of the country are unable to properly identify themselves and receive service; Likewise, national and regional policy-makers face difficulty to formulate proper development policies due to lack of standardized digital identification system in the country. This gap created by a lack of a robust Identification system is, hence, hampering efficient service delivery and good governance; and there is a need to address these problems by instituting a legal framework;

Whereas it is necessary to establish a legal basis for the use of digital identification in a comprehensive, consistent and reliable method, by establishing a digital identification system for the registration of residents of the country and by retaining the information of the registrants; Properly define the trust framework and legalize the relationship between the various stakeholders of the digital identification system, including the registrant, registrar, relying party, authentication service provider and the Digital Identification Institution;

NOW, THEREFORE, in accordance with article 55(1) of the Constitution of the Federal Democratic Republic of Ethiopia, it is hereby proclaimed as follows.

SECTION ONE
General Provisions

1. Short Title

This proclamation may be cited as "Ethiopian Digital Identification Proclamation Number ……. /2022."

2. Definition

Unless the context requires otherwise, in this proclamation:

1/ "Foundational Identification" means a legal identifier that enables the Resident to access services by making use of his unique identity;

2/ **"Digital Identification System"** means an organized and reliable foundational identification system that provides a Unique Number to each resident by collecting Demographic and Biometric data in a central database.

3/ **"Digital Identification"** means a Foundational Identification with a Unique Number that is issued to a resident that is registered on the Digital Identification System.

4/ **"Minor Digital Identification"** is a type of Digital Identification issued without collecting biometric data to a minor as defined per the guidelines of the Institution.

5/ **"Biometric Data"** means physical attributes that can be computed off of a natural person such as fingerprints, iris, and facial photos used for unique calculation of a person's identity.

6/ **"Demographic Data"** means the non-biometric personal attributes of a resident entered into the Digital Identification System, referred to in Article 7 of this Proclamation.

7/ **"Unique Number"** means a special, and non-repeating number issued to a Registrant by the Digital Identification System after successful registration; and once issued, a unique number is permanent unless in exceptional circumstances defined by the institution.

8/ **"Alias Number"** is a unique number that the resident or the Institution can generate to be securely and privately associated with the unique Digital Identification of the resident.

9/ **"Institution"** means a Digital Identification entity that will implement the Digital Identification System and execute the provisions within this Proclamation.

10/ **"Resident"** means a natural person living in Ethiopia, with or without proof of Ethiopian citizenship, a foreign resident living or working in the territory of Ethiopia in accordance with the country's law.

11/ **"Registrant"** means a resident natural person who receives a Digital Identification after providing his Demographic and Biometric data.

12/ **"Registrar"** means the Digital Identification Institution or a body entrusted by the Institution to collect the individuals' information.

13/ **"Registration"** means the process of enrolling a registrant, through a unique deduplication process of personal data sent by the Registrar to the Digital Identification System.

14/ **"Relying Party"** means a body that authenticates an individual's identity, with the knowledge and consent of the Digital Identification Institution and the individual.

15/ **"Authentication"** means the process of verifying, whether online or offline, the identity of an individual against registered information in the Digital Identification System.

16/ **"Authentication Service Provider"** means a body that responds to a request for authentication at the inquiry of a Relying Party for Personal Data.

17/ **"Personal Data"** means the collected information referred to in Article 7 of this Proclamation to the digital identification system, including biometric data.

18/ "**Sensitive Personal Data**" means data on a natural person:

a) racial or ethnic origins;
b) genetic data;
c) physical or mental health or condition;
d) sexual life;
e) political opinions;
f) religious beliefs or other beliefs of a similar nature;
g) the commission or alleged commission of an offense;

h) any proceedings for an offense committed or alleged to have been committed, the disposal of such proceedings, or the sentence of any court in the proceedings;
i) any other personal data as the Institution or other authorized entities may determine to be sensitive personal data.

19/ "Consent" means permission given by a registrant in writing, in a digital format, verbally, or in any other clear, unambiguous manner, for their Personal Data to be processed for known purposes, based on the registrant's free will.

20/ "Digital Identification Credential'' means a physical or digital documentary evidence containing Personal Data and either the Unique Identification Number or Alias Number;

21/ "Region" means a region established in accordance with Article 47 of the Constitution of the Federal Democratic Republic of Ethiopia and for the purpose of this proclamation, it includes Addis Ababa City Administration and Dire Dawa City Administration.

22/ "Government" means the government of the Federal Democratic Republic of Ethiopia; and for the purpose of this proclamation, it includes regional administrations.

23/ "Person" means any natural or juridical person.

24/ In this proclamation, any phrase expressed with a masculine gender includes the feminine gender as well.

3. Scope of Application

This proclamation shall apply to any person in Ethiopia.

4. The Ethiopian Digital Identification Institution

1/ The Council of Ministers will designate, by a Regulation, Institution to implement the powers and responsibilities of the Digital Identification System as stipulated in this Proclamation.

2/ Without prejudice to the duties and responsibilities to be provided by the regulation to be decided by the Council of Ministers, the Institution shall perform the following duties and responsibilities:

a) To establish and organize a Digital Identification System to serve as a primary Foundational Identity of any resident.
b) To collect Biometric Data for the purpose of issuing a Digital Identification service is solely given to the Institution or a body authorized by the Institution.
c) To issue Digital Identification and other credentials in an all-inclusive manner to all residents who completed registration by providing Personal Data as per this Proclamation.
d) To organize the Digital Identification System to serve as the foundation for government-issued resident identification credentials and for other authorized service providers.
e) Ensure data accuracy, safety, and privacy of registrants; establish a system that ensures that Personal Data within the Digital Identification System shall be used only for the stated purpose under this Proclamation.
f) Shall be organized to enable the government to make sound policy decisions by establishing a well-established demographic system with organized information about residents of the country.
g) Serve as Authentication Service Provider required for Authentication services of socio-economic sectors.
h) Shall be organized to develop a proper governance and revenue structure as necessary to provide best-in-class services.
i) Shall integrate with various entities and digital platforms to provide data sharing and exchange services.

j) Promoting research and development activities in biometrics and related fields, especially on the Digital Identification System;

SECTION TWO
Digital Identification System Principles, Enrollment and Service Provision

5. Principles

Digital Identification System shall abide by the following principles:

1/ The Digital Identification System shall be inclusive, free from discrimination, accessible and with minimal barriers to entry and use.

2/ The Digital Identification System shall be trusted, private and secure by design, responsive, interoperable across sectors and boundaries, ensure data and system sovereignty, vendor neutral and planned for financial and operational sustainability.

3/ The Digital Identification System shall respect the privacy and security of personal data, maintain the system's cyber security and safeguard people's Digital Identification rights through a comprehensive legal and regulatory framework, establish clear and institutional mandates and accountability, establish independent and neutral grievance redressal and adjudication provisions.

4/ Any Personal Data entered into the Digital Identification System shall follow the principle of data minimization, whereby no extra data should be collected nor entered into the system other than those necessary for Digital Identification.

5/ Relying Parties that establish digital schemes to identify their customers have to comply with the Digital Identification System and the legal framework thereof.

6/ Being a holder of Digital Identification or receiving the authentication service thereof, shall not by itself, confer any right of, or be proof of, citizenship or domicile in respect to a Registrant.

7/ When any resident applies for registration, the Institution has the responsibility to ensure that the applicant has not previously received a Digital Identification.

6. Registration System

The Registrar shall verify and register the personal data of the registrant using identification documents, and other documents acceptable by the Institution or witnesses.

7. Personal Data

1/ The Digital Identification System shall consist of demographic information and Biometric Data for each Registrant.

2/ Every Registrant shall provide personal information including:

a) First Name, Father's Name, Grandfather's Name, or when the three names are not available or applicable, the Institution may collect other arrangements of legal names;
b) Date of birth: day, month, and year;
c) Gender;
d) Domicile Address;

3/ In addition to the information listed under Sub-article 2, with the exception of Sensitive Personal Data, additional personal data may be collected including, but not limited to:

a) Nationality

b) Phone number
c) Email address
d) Postal Address

4/ Pursuant to article 6 of this Proclamation, if the Registrant fails to submit the required proof of identity, he may present an individual witness who:
   a) Have a Unique Number, or
   b) Is a prospective registrant pursuant to Article 6 of this article, that submitted his biometrics into the Digital Identification system and can provide an identity document;

5/ Biometric Data
   a) Every Registrant must have his Biometric Data collected.
   b) Without prejudice to the sub-sub article (a) of this sub-article, an exception to some components of the Biometric Data requirement may be granted if the Registrar attests that one or more physical disabilities bar a registrant from submitting his biometrics facial photograph will, however, be mandatory in all circumstances.
   c) The institution will devise a mechanism to ensure accessibility of service for individuals who are unable to be present at the Registrar due to serious health problems.
   d) Biometric Data shall be recaptured at certain time intervals as set by the Institution.

8. Issuance of Digital Identification for Minors

A minor, whose cutoff age will be determined by the institution's directive, may obtain a valid Minor Digital Identification without giving biometric data through a parent, caretaker, or legal guardian who has already registered in the Digital Identification System.

9. Unique Number Issuance

1/ Upon collection of personal data as described under Article 7, the Institution shall issue each Registrant a Unique Number that uniquely differentiates that person from others.

2/ The Unique Number shall be generated by electronic means, in a confidential manner, and shall preserve the security of the personal information behind it.

3/ One Unique Number shall be given to one registrant and shall remain immutable, irrevocable and permanent.

4/ Without prejudice to the unique number referred to in sub-article 2 of this Article, the Digital Identification System shall generate Alias Number or numbers with a set validity period meant to shield the privacy of the unique number based on the assessment of the Institution, the request of the Registrant, or a Relying Party, allowing the Registrant to receive authentication service similar to what the Unique Number enables.

5/ The unique number described in Sub Article 2 of this article is immutable, but for the registrant's privacy, but for Digital Identification Credentials an Alias Number can be equally valid.

6/ Any Registrant who has lost their Unique Number may appear in person at the Institution or a delegated body to recover it.

7/ Without prejudice to sub-article 4 of this Article, after the death of the registrant, the Digital Identification Institution has to ensure that the Digital Identification cannot be used for authentication even though the unique number remains immutable;

8/ Without prejudice to this article, Sub Article 3, an individual's digital identification may be locked or disabled as per his request or by a court order. The detailed procedure shall be determined by a directive.

10. Digital Identification Credential

1/ The Digital Identification Credential issued by the Institution or by other authorized entities may display the following personal data:

a) All the information listed in this proclamation article 7, Sub Article 2;
b) Photograph referred to in article 7 Sub Article 5 (b);
c) Unique or Alias Number.
d) Date of issuance and date of expiry of the Digital Identification Credential;
e) Any other information collected in accordance with article 7 of this Proclamation and subsequent decisions of the Institution and deemed relevant for the Credentials.

2/ The Digital Identification Credential must be renewed upon the recapture of biometric data; however, if the renewal date of the Digital Identification Credential is expired, it shall not be used for authentication services.

3/ Without prejudice to the provisions of Article 4 sub article (2) paragraph (c) of this Proclamation, digital Identification Credentials may be issued by the Institution or by other bodies mandated by the Institution.

4/ The Registrar that issues or renews the Digital Identification Credential shall update and re-verify the Registrant's Personal Data.

5/ A Registrant whose Digital Identification Credential is lost or damaged can apply for a replacement and may take a new credential based on procedures put in place by the Institution.

6/ Any person who finds a lost physical Digital Identification Credential shall return it to the Institution or to a nearby police station.

11. Language

1/ Personal Data recorded into the Digital Identification System and displayed on Digital Identification Credentials shall be in the working language of the Federal Government or the working language of the Regional Government where Registration is taking place and in English.

2/ Without prejudice Sub-Article 1 of this Article, Personal Data may be recorded and Digital Identification Credential printed in additional local language as per the directives of the institution.

12. Change of Information of Digital Identification

It is the Registrant's responsibility to notify the Institution of the changes or amendments to his Personal Data after Registration.

SECTION THREE
Relying Parties and Authentication Service

13. Relying Parties

1/ Subject to the provisions of Article 5 sub-article 7 of this proclamation, any Relying Party reserves the legal right to render digital identification a mandatory requirement to offer their services upon the approval of its concerned regulator.

2/ Relying parties may receive a Registrant's Personal Data from the Institution or other Authentication Service Providers authorized by the Institution, upon receiving the consent of the Registrant.

3/ Any Registrant that needs to access services based on the Digital Identification System has the right to receive Authentication Services to get that service.

4/ Relying parties have to receive authorization to access the data for the purpose of electronically identifying their customers from the Institution before they can provide an Authentication Service based on the Digital Identification System.

5/ In exceptional cases where the Digital Identification Authentication Service is not properly functioning, the Relying Party reserves the right to use other authentication mechanisms to deliver services.

6/ The duration of the retention period for Personal Data by a Relying Party shall be specified by a directive of the Digital Identification Institution.

14. Authentication Service Provision and Usage

1/ Digital identification is legal and sufficient evidence to authenticate a person's identity;

2/ The Institution and other authorized Identification Providers can provide authentication services.

3/ Any Registrant that wants to receive Authentication Service has to have a Digital Identification or a Digital Identification Credential with its unique number.

4/ Authentication Service Providers shall provide the minimal necessary level of personal data based on the needs of the relying party as authorized by the Institution.

5/ Authentication Service Providers, as well as relying parties, should ensure the safety and security of the Personal Data they received from the Digital Identification System.

SECTION FOUR

Personal Data Management, Protection, Security, and Grievance Redressal

15. Personal Data Management

1/ The Digital Identification System shall be a reliable and robust system to securely and safely administer Personal Data.

2/ The Digital Identification System is tasked with maintaining Personal Data quality over time, including the responsibility of updating, re-verifying, renewing, temporarily locking, and/or revoking digital identification information.

16. Data Fraud or Error

1/ When an issued Digital Identification is confirmed to be fraudulent, the Institution may take corrective actions against the personal data, lock the digital identification from further misuse or take legal action.

2/ Whenever the Institution verifies that there is erroneous Personal Data entered into the system intentionally or by negligence, it has the responsibility to rectify the error while maintaining the irrevocable nature of the Unique Number.

17. Handling and Security of Personal Data

1/ The Institution shall employ strong administrative, legal, procedural, and technical safeguards to ensure the protection of Personal Data from either natural or man-made disasters, electronic attacks, theft, destruction, and other similar losses.

2/ Personal Data collected for the Digital Identification System must be organized in a convenient manner for access by any relying party or identity provider and stored securely in a database managed by the Institution;

18. Protection of Personal Data

1/ The owner of any Personal Data collected for the Digital Identification System is the Registrant. Any authentication processes under the Digital Identification System shall be done with the consent of the Registrant.

2/ The Institution shall maintain the confidentiality of Personal Data in the course of collecting, authenticating, storing and processing the same.

3/ Data collected for the Digital Identification System shall be done in accordance with the principles set out in Article 5 sub-article 4 of this Proclamation; No information shall be collected for the Digital Identification System other than those necessary to identify residents.

4/ Any person, or law enforcement body may not collect, disclose, distribute, print, use, transfer a copy to a third party or publicly disclose information without the Registrant's consent.

5/ It is prohibited to disclose, transfer or modify the Personal Data of any Registrant, collected under the Digital Identification System, in accordance with the rules and regulations without the Registrant's consent.

6/ Notwithstanding the provisions of sub-article 5 of this article, the data may be disclosed or transferred to the relevant legal entity authorized by law or by court order.

7/ The Institution may generate anonymous statistical reports to share with authorized third parties in accordance with the procedures of the Institution.

8/ Personal Data transmitted to a Relying Party from a Digital Identification system database can be used only for that particular service for which it was requested; Relying Parties may store this information in their own database and use it only for their own use, without violating its original purpose.

9/ Without prejudice to Sub Article 7 of this Article, misuse of Personal Data by any party, for purposes other than they were designed for, is prohibited.

10/ During registration, a standard consent form prepared by the Institution, should be issued by the Registrar. This form should describe the Registrant's rights and obligations and shall be completed and signed by the Registrant as proof of consent.

11/ Subject to the provisions of sub-article 9 of this Article, for cases where the registrant brings a witness, the witness requires a secondary form stating their voluntary consent, their rights, and obligations, with either their Unique Number or proof of Digital Identification registration and proof of identity, must be provided, signed and completed on the form.

19. Grievance and Complaint Redressal

1/ The Institution shall establish a complaint handling department and notify such establishments its customers.

2/ Any person against whom Digital Identification service is provided and a decision is made have the right to lodge a complaint to the Institution.

3/ Any complaints and grievances that may be encountered in the course of service provision of the Institution shall be solved in accordance with the grievance redressal process and through the Institution's complaint filing and redressal directive.

4/ A party who is dissatisfied with the decisions of the Institution may file a petition to the pertinent court requesting judicial review of the decisions.

SECTION FIVE
Miscellaneous Provisions

20. Duty to Cooperate

Any person has the obligation to cooperate so that the Proclamation shall attain its purpose.

21. Repealed Laws

No law or customary practice, inconsistent with the provisions of this proclamation shall be applicable with respect to matters provided for by this Proclamation.

22. Power to Issue Regulation and Directive

1/ The Council of Ministers may issue regulations that are necessary to enforce this Proclamation.

2/ The Institution may issue necessary directives to enforce this Proclamation and the enforcing Regulations, including but not limited to the following issues:

a) Re-registration penalty;
b) Usage of Alias number for the protection of the individual's data privacy
c) Biometric data content and related detail procedures that issue each individual a unique identification number that reliably distinguishes their identity
d) Digital Identification procedures for registration, verification, use, administration, and other services delegation procedure to relying parties, registrars, identification providers, etc…
e) Issuance of Unique Identification for minors, lower age limit, and age verification due diligence;
f) Collection of biometric data exceptions when proven that one or more biometric data could not be collected due to proven disability;
g) Issuance of a special Digital Identification by receiving a medical certificate from individuals with special health needs that require special support to collect their biometric data;
h) The validity period for biometric data;
i) Reporting and announcement of changes and modifications to contents of Digital Identification System and personal data;
j) Detail mechanisms for grievance and complaint redressal related to the digital identification system;
k) Authorization to issue or print Digital Identification Credentials, detail personal data to be printed and its validity period;
l) Directives of conditions of proof of domicile to address inclusion;
m) Legal procedures to correct issues of duplication, erroneous entry and fraud;
n) Procedures to accept witnesses and documentation submitted as proof of identification and address;
o) Data Sharing, exchange and authentication with concerned bodies and digital systems.
p) The duration of the retention period for Personal Data by a Relying Party;

23. Effective date

This proclamation shall enter into force on the date of its publication in the Federal Negarit Gazeta.

Done at Addis Ababa, this ____ day of ____ / 20202

Sahlework Zewdie

President of the Federal

Democratic Republic of Ethiopia