National ID
ብሔራዊ መታወቂያ

Ethiopian
National ID Program

Working
Protocol

March, 2023

Contents

1. Overview

In today's world, there is a growing recognition of the importance of identification for sustainable development in a country. Ethiopia is no exception. Although the concept and usage of manual identification is in practice, electronic identification presents significant opportunities for Ethiopia to transform towards a digital economy. Pertinent to recent goals on digital transformation, with the capability of ensuring unique identity and online authentication/identification, Ethiopia strives to join and integrate with the global economic ecosystem. In recent years in Africa, we have seen large implementations of National ID systems in countries such as South Africa, Kenya, Nigeria, Rwanda, Uganda, and very recently in Morocco.

Agenda 2063 of the African Union Commission (AUC) commits to transform the continent by ensuring irreversible universal advancement across the continent to improve the condition of African people. Furthermore, Sustainable Development Goals (SDG) 2030 particularly Goal 9 asserts the development of quality, reliable, sustainable, and resilient infrastructure, including regional and trans-border infrastructure to support economic development and human wellbeing, with a focus on affordable and equitable public service access for all. SDG target 16.9 also asserts the importance of legal identity to promote just, peaceful, and inclusive societies, which calls for "providing legal identity for all, including birth registration by 2030". This requires a unique identity management system to ensure equity and inclusion, and ensure no one is left unserved.

The Ethiopian National ID Program (NID Program) which has been reorganized under the FDRE Prime Minister Office to lead and manage the establishment of the national identification platform and service covering all parts of the country for eligible residents. The NID Program leads the process of establishing digital identification service pertinent to international standards, principles, and guidelines[1].

This protocol document is prepared to serve as a guideline for ID related operations including enrollment, authentication, privacy, and other safeguards until such time as the ID Law is put into effect and permanent ID authority replaces the work of the NID Program.

[1] NID Policy, Principles and Governance Document: https://id.et/wp-content/uploads/2021/12/Policy-and-Governance-Ethiopian-ID_Dec_2021_V1.3.pdf

2. Program Objectives

With an inclusive and trusted proof of identity, people will have the assurance for all rights and services such as owning property, a bank account and credit, safety net support, benefits such as social security, legal protection, and other state provided services and benefits.

- The standards and technologies will enable seamless information integration at the regional and international levels and empower residents by providing them with genuine and trustworthy credentials recognized by the international community.

The scope of the NID program is to provide a foundational digital identification for all residents in the nation.

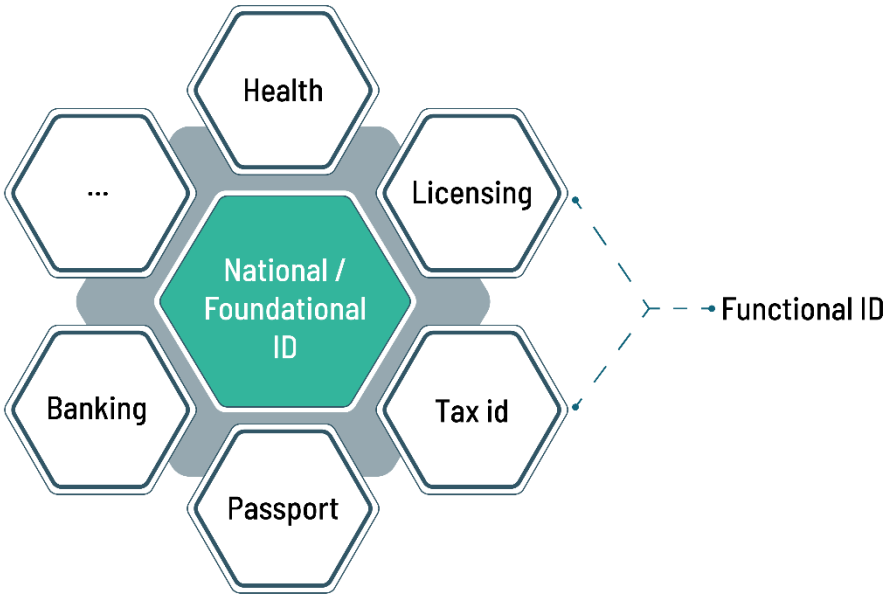

Figure 1: Foundational ID in an operational context

3. Program Components

The following list shows the expected major components of the NID Program:

NID Program Components	
Legal Framework	**Prepare The Legal Enabling Environment**
	Approve NID proclamation
	Approve the Data Privacy and Protection Law
	• Draft NID Regulation • Draft NID Directives • and other working procedure manuals
	Recognize Other Relevant technology and Cyber related Laws,Policies and strategies
The Fayda IDMS	**Prepare NID (FaydaSys) Platform system**
	Prepare Deployment Software Tools
	Make Lab level Test
	Plan for progressive scaleup
	Technical and Operational Capacity Building
Rollout (Registration, Authentication, and Integration)	**Common**
	Logistics (Procurement Plan)
	Personnel
	Use Case Prioritization and Planning
	Finance Allocation
	Pilot Rollout
	Registration and Authentication
	Plan for the long term (Ecosystem, Business Model)
	Evaluation and Refinement
	National Rollout
	Prepare hardware and software procurement plan
	Infrastructure
	Software
	Registration Kits
	Data exchange Standards and protocols in place
	Integration Tested and Stabilized

	National Rollout
Design and Implement A Business Model	Research on the Best Model
	Design of the Ecosystem Approach
	Defining Permanent Roles
	Defining Operational Directives and Procedures
	Defining Financial Model
Transition to a Permanent Entity	
	Establishing the Permanent Entity
	Transition

4. Timeline

This protocol will be in effect during the Pilot's entire lifecycle and until:

(1) A National ID Authority is established based on ID proclamation, Council of Ministers regulation and the NID program ends its mandate, and

(2) Entry into force of the NID and Data Protection Proclamation, NID Regulation or Directives.

For the avoidance of doubt, the provisions of this Protocol related to personal data collection and processing will be of no further effect when the NID and Data Protection Proclamation and NID Regulation are adopted, which NID Proclamation, DPP and NID Regulation will then govern collection and processing of personal data. Likewise, remaining provisions of this Protocol related to the National ID institution, attributes of the NID System or other ID-related issues will be of no further effect when the National ID Proclamation, Regulation and Directives are adopted.

5. Working Protocol

It is the commitment of the GoE to follow international guidelines and principles of identification, typically the principles of ID4D. The NID Program is working on establishing a legal framework and enabling environment for the operationalization of the program and to establish trust and public confidence in the program and eventual system. Accordingly, drafts are prepared for the most essential legal documents for

approval by law makers. However, due to current national context and the procedural nature of the approval process, the program intends to release a working protocol that can work in lieu of the draft legislations in the pipeline.

I. Privacy and Minimal Data Collection

This entire program aims to design and implement a foundational ID system for Ethiopia at the national level. For all intents and purposes, "National ID" shall mean Foundational Digital ID. From this program's perspective, the term "National ID" is synonymous to the term "Foundational ID" for communication and reporting purposes.

Only those demographic and biometric data necessary for establishing uniqueness will be collected. All demographic data collected, stored in the NID database and/or published in the ID credential focuses on minimal data required to identify an individual, namely "Full Name", "Gender", "Current Address" and "Date of Birth". As of current operation, the biometric data should include ten fingerprints, dual iris and ICAO compatible facial images as per Fayda specifications.[2]. However, for minors below the age of four no biometric data should be collected to give digital ID. all other demographic data are optional, including citizenship information. Moreover, sensitive, or unnecessary data such as an individual's religion or ethnicity, birthplace or other similar data will NOT be collected.

Other optional fields including phone number, postal address and email are taken for further interaction and notification purposes. Consent from individuals to participate in the pilot will be obtained by using the following statement:

> *"You are hereby informed that your personal information is being collected for the purpose of being included in a national ID database for issuing a personal digital identification. This information may be shared or otherwise automatically processed only in connection with that purpose. Third parties will not have access to this data without your consent. You have the right to inspect your data, audit its history and correct any errors by contacting us on www.id.et"*

A log of all individuals who are so informed will be maintained where the register of other data collected in connection with this program is maintained.

[2] For more on the biometric specifications, refer to the Annex on the Biometric Kit specifications on id.et/nidspecifications

II. Inclusion

To remove barriers to inclusion and following the international guidelines, the National Foundational ID service will be available to all citizens and non-citizens (legal residents) who can provide any type of acceptable evidence including an appropriate witness/es that can attest about the individual's identity called Introducer. The introducer practice has already been in use for the Kebele-ID although it has mainly been practiced by citizens.

- Inclusion Principles:
  - Leave no one behind
  - Ensure universal access for individuals, free from discrimination.
  - Remove barriers to access.

III. Authentication Mechanisms and Standards

The owner of the identity data is the individual and will have the right to manage how it should be used at the individual level. Accordingly, all rules set forth on the annexed draft ID proclamation will be complied with during the pilot. All tests will be performed by using a formal consent from every registrant that participates during the pilot period.

IV. Usage of Credentials

Different forms of credentials may be issued for registered individuals that can allow both online and offline authentication. Until such time as defined by Law, the ID credentials issued by NIDP shall only be applicable to the purposes for which the ID is issued and its scope will be limited to provision of services for the particular relying party that has signed an agreement with the NID Program[3]. Hence, all identity credentials issued by NID Program while this Protocol Document is valid, i.e., until such time as ID Regulation comes into force to establish an ID authority, will not have a legal role to play as a foundational ID but a functional one to serve the aforementioned list of use-cases. Accordingly, the credentials are not mandatory and a prerequisite for different types of functional services currently provided using the Kebele ID.

V. Vendor Neutrality and Open Source

The program focuses on vendor neutrality and remaining in technology ownership of the core ID platform. This arrangement ensures individual data remains secure under NID Program, also known as the "Data Controller" and not the vendors or other third parties. The hardware vendors as well as ABIS and other

[3] For a list of services that are in active agreement with NIDP offering enrollment and authentication, visit https://id.et/services/

software vendors should be interchangeable, and the platform will remain independent of a specific type of hardware technology or software license. Customization work conducted on the Fayda (MOSIP) platform may or may not be shared back with the open-source MOSIP community at the discretion of the NID Program.

VI. Security in Design

This platform gives the highest priority for security as a platform that holds sensitive data, and it provides the basis for many other functional services across the nation. Communication between any endpoints, including enrollment stations, supervisor and admin portals, authentication stations, resident service portals and backup sites are all end-to-end encrypted. This offers individuals, service providers and authentication parties the trust and confidence that their personal data and interaction is secure, tamper-free and not accessible without their knowledge and active consent.

- Design Principles:
    - Establish a trusted – unique, secure, and accurate – identity.
    - Create and responsive and interoperable platform (flexible and scalable)
    - Use open standards and prevent vendor technology lock-in.
    - Protect privacy and agency through system design.
    - Plan for financial and operational sustainability

VII. Grievance redressal and management

- All individuals enrolled on NID system will have the right to inspect their personal data and audit its history on the platform provided by NID (www.id.et)
- An internal grievance redressal committee will be established through the ID Proclamation, Directive to be issued by the institution and this Protocol document.
- If individuals encounter any errors or problems in their personal data, they can contact NID Program through digital means on www.id.et, via a toll-free call center on 9188 or by personally going to any of the designated enrollment centers.
- Any other grievances or complaints can be reported on site during the enrollment processes or directly to NID via the above-mentioned mechanisms. A complaints officer will log the grievance report and a redressal workflow will be initiated.

VIII. Communications

- NID prioritizes transparency and as such all non-personal or non-sensitive data, including activities of the program, anonymous statistical data, audit reports and other findings will be publicly published.

IX. Governance

- Governance principles are:
    - Oversight, Security and Accountability.
    - Safeguard data privacy, security, and user rights through a comprehensive legal and regulatory framework.
    - Establish clear institutional mandates with transparency and accountability.
    - Enforce legal and trust frameworks through independent oversight and in compliance with UN and international laws, guidelines and principles.

X. Relationship with Relying Parties

The pilot and the subsequent country rollout will depend on relying parties to scale its reach. The strategy[4] that will be followed towards the successful completion of the batch registration will primarily focus on functional use-cases that offer the individual the benefit of ID supported trustworthy services.

The pilot will be operational and will involve different organizations which include local authorities (regions, zones/sub-cities, and woredas). Furthermore, a selected use case can imply the direct participation of different organizations. As an example, the selected PSNP (Productive Safety Net Program) use case will require the direct involvement of three ministries (Ministry of Agriculture, Ministry of Urban Development and Construction and Ministry of Labor and Social Affairs) as well as the Federal Urban Job Creation and Food Security Agency which the program has already began contacting.

XI. Permanent Independent Entity

As depicted on the NID Program's component and progress model (section 2.1 and figure 2), it should be noted that the government, and the NID Program thereof, is in the process of passing the ID Law that establishes a permanent independent ID authority. This Protocol Document shall serve as a guiding principle

[4] Look at id.et/strategy for the latest on the NIDP strategy.

for procedural decision and adjudication until a Digital Identification Institution is formally established. KYC as a service is identified as a sustainable revenue generation mechanism for this institution. NID program is working towards realizing a wholly government owned public enterprise or a share company whose shareholders are other public enterprises.

XII. Supervision

Since the NID Program is a nationwide service, it falls under Federal Government jurisdiction. However, as a regulatory organ, the National ID Authority may be subject to the supervision of the highest law-making entity – the House of Peoples' Representatives. Other overarching legal provisions such as the Ethiopian Personal Data Protection, cyber security, and cybercrime laws as well as accountability to any judicial jurisdictions are to be respected.

XIII. Procedures for Penalties and Legal Measures

An internal tribunal will be established to adjudicate reported cases of fraud or illegal activities within the scope of NID Program. This internal tribunal will be composed of legal, technical, and administrative personnel. Decisions will be made based on internal procedures, ID laws, this protocol document and applicable legislations and appropriate administrative measures taken against the offending entities.

Any other proven misuse, fraud or legally accountable cases that need to be administered through currently operational Civil or Criminal Codes, including those who are found to commit intentional fraud, identity theft and other illegal activities will be reported by the NID Program to the appropriate bodies.

6. Annex I: Digital ID Draft Proclamation

Proclamation No. _____ /2023

Ethiopian Digital Identification Proclamation

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

Whereas, establishing a technologically developed, cross sectoral foundational digital identification system, helps to plan national development effectively, create economic transformation, ensure good governance, reduce wastage of resources, eliminate redundancy and ensures inclusiveness when policies are designed, and development plans are executed;

Whereas, establishing a nationwide Digital Identification system is important to establish a reliable, accessible and secured system, and to promote the country's social, political and economic development and predictability, to ensure the overall peace and security of residents and reinforcing the justice system.

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 ……./2023."**

2. **Definition**

   Unless the context requires otherwise in this proclamation:

   1. **"Foundational Identification"** means a legal identification that enables Residents to access services basing on 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 and through the Unique Number it is used to get service to be provided with foundational Identifications.

   4. **"Minor Digital Identification"** is a Digital Identification issued without collecting biometric data to a minor as defined by 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 photo 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 8 of this Proclamation.

   7. **"Unique Number"** means a special, and non-repeating number issued to a Registrant by the Digital Identification System after a successful registration of biometric and demographic information; and once issued it is permanent unless

in exceptional circumstances decided by the institution.

8. **“Alias Number”** is a number generated from the identification system 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, or it may be an office structured in a Governmental office relevant to the task.

10. **“Resident”** means a natural person living in Ethiopia fulfilling the requirement of residence indicated under article 174 and 175 of the civil code, and includes a person with or without a proof of Ethiopian citizenship and a foreign resident living or working in the territory of Ethiopia by getting resident permit from the relevant authority.

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 person entrusted by the Institution to collect the registrants’ 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 person 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 person that gives authentication service at the request of a Relying Party for Digital Identification information .

17. **“Personal Data”** means Biometric Data and Demographic Data indicated under article 8 of this proclamation, collected with the Digital identification system.

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. political opinion;
    e. religious beliefs or other beliefs of a similar nature;
    f. the commission or alleged commission of an offense;
    g. 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;
    h. 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 Regions.
23. **“Person”** means any natural or juridical person.
24. In this proclamation, any phrase expressed with a masculine gender includes the

feminine gender.

3. **Scope of Application**

This proclamation shall be applicable on any person found in Ethiopia.

4. **The Ethiopian Digital Identification Institution**

1. The Council of Ministers may establish, by a Regulation, the Institution to implement the powers and responsibilities of the Digital Identification System as stipulated in this Proclamation or it may be structured in Governmental office relevant to the task as the case may be.

2. The Institution shall have the following objectives: -

    a. To establish and organize a Digital Identification System to serve as a primary Foundational Identity of any resident;
    b. Lead and coordinate the task of collection of Biometric and demographic Data for the purpose of issuing a Foundational Identification service.
    c. Issue, lead and coordinate the issuing task of Digital Identification.
    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. 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 organize a system that can manage the demographic data of the residents of the country to enable the government to make sound policy decisions; and
    g. Establish a system to provide Authentication services necessary to social, economic and political sectors.

SECTION TWO
Digital Identification System Objectives, Principles, Enrollment and Service Provision

5. **Objectives**

The Digital Identification system shall have the following objectives: -

1. Contribute to the respect of human rights and improvement of good governance by enabling residents to be easily authenticated when moving from place to place in any part of the country;
2. Improve trust between service providers and service recievers and prevent illegal activities by creating Digital Identification System that helps to identify those who want to get service easily;
3. By establishing nationwide Digital Identification System minimizing resistiveness and as a result minimizing wastage and improving inclusiveness when national policies, strategies and plans are drafted and developmental activities are implemented; and
4. By establishing a system that enables the collection of demographic and biometric data of residents, serving as a source of identification for other governmental and non-governmental bodies, strengthening other service focused identification systems to transfer them to digital identification systems.

6. **Principles**

Digital Identification System shall abide by the following principles:

1. Principle of Inclusiveness

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

2. Principle of infallibly

a. 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.

b. 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 procedure.

3. The Principle of Data minimization

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.

4. The principle of Alienability

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

7. **The right to get digital identification and the responsibilities of the institution or registrant**

1. Any person who is registered for digital identification by giving his biometric and demographic data shall have the right to get digital identification.
2. When any Resident applies for registration, the Institution has the responsibility to ensure that the applicant has not previously received a Digital Identification.
3. The Institution or Registrar shall verify and register the personal data of the Registrant using identification documents, other documents acceptable by the Institution or witnesses, the details shall be decided by directive to be enacted by the Institution.

8. **Personal Data Registration system**

1. The Digital Identification System shall consist of Demographic and Biometric Data for each Registrant.
2. Without prejudice to sub-article 1 of this article, Digital Identification System shall consists of the following Demographic Data: -
    a) First name, father's name, grandfather's name, or when there is no legal name organized in the way, the Institution may collect other arrangements of legal names or the name of the registrant which is known by the local community;
    b) Nationality.
    c) Date of birth: day, month and year.
    d) Gender.
    e) 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) Phone number
    b) Email address
    c) Postal Address
4. When the Registrant fails to submit the required proof of identity listed under article 7 of this Proclamation and wants to be registered through witness, the witness: -
    a) should have a Unique Number, or
    b) should be a person registered in a Digital Identification System.
5. Registration of Biometric Data
    a. Without prejudice to sub article (1) of this article, if it is confirmed by the Registrar that the Registrant cannot give biometric data because of disability or any other reason, digital identification may be provided by registering facial photograph.

b. The Registrar may register Registrants who cannot come to the registration place because of health or any other reason, at their place or any other convenient place, the details of implementation can be decided through a directive to be enacted by the institution.

6. Personal Data shall be renewed at the time interval to be decided by directive to be issued by the institution.

9. **Circumstances where children's get Digital Identification**

Notwithstanding article 7 sub-article 1 and article 8 sub article 1 of this proclamation, to register minors it is sufficient to register the demographic data of the minor through a parent, caretaker, legal guardian or anyone who is registered in the Digital Identification System and can take the responsibility for the registration of the minor.

10. **About Unique Number**

1. Upon collection of Personal Data as described under Article 8 and populating the data to the system, 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 thereof.
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 to the Registrant 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, however, for the purpose of protecting the Registrant's privacy the number on the Digital Identification Credentials and the number used in other circumstances can be changed by an Alias Number.
6. Any Registrant who has lost their Unique Number may appear in person at the Institution or a delegated body to recover it subject to fee.

7. Without prejudice to sub-article 4 of this Article, after the death of the Registrant, the 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 requested by the Registrant or by a court order. The detailed procedure shall be determined by a directive.

11. **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 8, Sub Article 2;
        b) Photograph referred to in article 8 Sub Article 5 (b);
        c) Unique or Alias Number; \Date of issuance and date of
        d) expiry of the Digital Identification Credential.
        e) Any other information collected in accordance with article 8 of this proclamation and subsequent decisions of the Institution and deemed relevant for the Credentials.
    2. The renewal period of Digital Identification Credential must be the same with the renewal period of Personal Data; however, if the renewal date of the Digital Identification Credential is expired, it is prohibited to give services using this Digital Identification Credentials.
    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 Institution or other body permitted by the Institution, shall verify that Digital Identification Credentials issued and the identity of the Registrant, prior to renewing or issuing Digital Identification Credentials respectively.
    5. A Registrant whose Digital Identification Credential is lost or damaged can apply for a replacement and may take another 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.

12. **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, the working language of the Regional Government where Registration is takes place and as per the directive to be issued by the Institution in English.
    2. Without prejudice Sub-Article 1 of this Article, Personal Data to be recorded in Digital Identification System and Digital Identification Credential printed in additional local language as per the directives to be approved by the institution.

13. **Change, Destruction or Misplacement of Information of Digital Identification**

    1. When there is change in the information registered in the digital identification system, the Registrant shall report to the Registrar or the body which gives the digital identification.
    2. The Institution or Registrant, when data collected by Digital Identification Systems are misplaced or destroyed, may inform the Registrant to give the data.

SECTION THREE
Digital identifications Relying Parties and Authentication Service

14. **Relying Parties**
    1. Any Relying Party reserves the legal right to render digital identification a mandatory requirement to offer their services up on 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 shall receive authorization from the institution before they start giving Authentication service.
5. 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.

15. **Authentication Service Provision and Usage**
    1. Digital Identification may be taken as legal and sufficient evidence to authenticate a person's identity.
    2. Notwithstanding sub article 1 of this article, being a holder of Digital Identification or receiving the authentication service thereof, shall not by itself be proof of citizenship or domicile in respect to a Registrant.
    3. The Institution and other authorized Identification Providers can provide authentication services.
    4. Any Registrant that wants to receive Authentication Service has to have a Digital Identification or a Digital Identification Credential with its unique number.
    5. 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.
    6. 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, Protection, Security, management and Grievance Redressal

16. **Protection and Security 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 of 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 transferred 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 data 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 10 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.

12. 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.
13. Personal Data collected for the Digital Identification System must be organized in a convenient manner for access by any Relying Party or Authentication Service Provider and stored securely in a database managed by the Institution.

17. **Personal Data Management**
    1. The Institution shall establish a reliable and robust Digital Identification System that can maintain Personal Data securely and safely.
    2. The Institution shall have the responsibility of maintaining Personal Data quality from time to time and shall fulfill the responsibilities of updating, re-verifying, renewing, temporarily locking and/or revoking digital identification information.

18. **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 to prevent 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.

19. **Grievance and Complaint Redressal**
    1. The Institution shall establish a complaint handling department and notify

such establishments to its customers.

2. Any person to whom Digital Identification service is provided and a decision is made has 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 for the attainment of the purposes of the Proclamation.

21. **Criminal liability**

1. Anyone who refuses to take digital identification as a legal identification or objects to give services rendered after verifying identity with digital identification provided by the relevant authority based on this proclamation, regulation and directives to be issued following this proclamation, shall be punished with a fine from birr ten thousand (10,000) to birr one hundred thousand (100,000).
2. Anyone who collects more data than needed to get digital identification in violation of article 16(3), (4) or (5) of this proclamation shall be punished with a fine from birr ten thousand (10,000) to birr one hundred thousand (100,000).
3. Any person who gives data collected for digital identification to a third party in violation of article 16(9) of this proclamation shall be punished in accordance with the circumstance of the case from 1 year to 5 year or to 8 years rigorous imprisonment.
4. If the crime indicated under sub article 1 and 2 of this article are committed

by a juridical person, it shall be punished with a fine from birr one hundred thousand (100,000) to birr five hundred thousand (500,000).

5. If the crime indicated under sub article 3 of this article is committed by a juridical person, it shall be punished with a fine from birr three hundred thousand (300,000) to birr eight hundred thousand (800,000).
6. If the crime indicated under sub article 3 of this article is committed negligently, the punishment shall be from 6 month to 1 year simple imprisonment or with a fine punishment from birr ten thousand (10,000) to birr seventy thousand (70,000).

22. **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.

23. **Transitory provisions**

Notwithstanding the provision of article 23 of this proclamation, Digital Identification given before the adoption of this proclamation, shall be considered as given based on this proclamation and continue as legal identification.

24. **Power to Issue Regulation and Directive**

1. The Council of Ministers may issue regulations necessary to implement this Proclamation.
2. The Institution may issue necessary directives to implement this Proclamation and regulations issued following this proclamation.

25. **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 ____ / 2023.
Sahlework Zewdie

President of the Federal
Democratic Republic of Ethiopia