



GLOBAL STANDARDS  
PROPORTIONALITY (GSP)  
WORKING GROUP

# POLICY MODEL FOR DIGITAL IDENTITY AND ELECTRONIC KNOW YOUR CUSTOMER (E-KYC)



# CONTENTS

---

CONTEXT AND BACKGROUND	3
OBJECTIVE	3
SCOPE AND APPLICATION	3
READING INSTRUCTIONS	4
<b>PART I: POLICY AND REGULATORY FRAMEWORK FOR IMPLEMENTING DIGITAL ID AND E-KYC</b>	<b>6</b>
I: Laws and regulations on digital ID and e-KYC	
II: Laws and regulations on data protection and privacy	
III: Governance and institutional structures	
IV: Financial inclusion strategies	
V: Gender-inclusive strategies	
<b>PART II. POLICY CONSIDERATIONS FOR DESIGNING THE PLATFORM AND BUILDING THE DIGITAL ID SYSTEM AND THE TECHNOLOGY INFRASTRUCTURE</b>	<b>14</b>
I: Designing the system	
II: Onboarding and registration procedures	
III: System capabilities	
IV: Data management	
V: User services	
<b>I: POLICY AND REGULATORY FRAMEWORK FOR IMPLEMENTING DIGITAL ID AND E-KYC</b>	<b>19</b>
I: e-KYC and authentication framework	
II: Access and interoperability for third party stakeholders	
II: Last-mile infrastructure	
II: Use cases	
V: Exception handling and grievance resolution	
<b>ANNEXURE 1: AFI MEMBER COUNTRIES DIGITAL ID AND E-KYC POLICY PRACTICES</b>	<b>23</b>
<b>ANNEXURE 2: REFERENCES</b>	<b>25</b>

---

## CONTEXT AND BACKGROUND

Countries across the world have been upgrading their public infrastructure for better service delivery in the digital era. One of the key developments in many countries is the implementation of a digital identity (ID) system. A major use case for digital ID has been electronic know your customer (e-KYC) processes, leveraging the digital ID system. The advantages of this range from increased efficiency, cost savings, and accelerated financial inclusion in many countries. This is evident in the experience of several AFI member countries.

As countries build the infrastructure and a robust regulatory and policy environment to enable digital ID and e-KYC development, it is imperative to keep the approach user-centric. The AFI Global Standards Proportionality Working Group (GSPWG) has codified best practices from AFI member countries and other global experiences into this policy model. The policy model builds on the recognition by AFI members of digital ID as a key pillar of an overall Inclusive FinTech policy framework, as enshrined in the Sochi Accord on FinTech for Financial Inclusion endorsed by the membership in 2018.

---

### OBJECTIVE

The policy model provides guidance to countries looking to develop or improve their digital ID systems and leverage them for e-KYC. The aim is to enable them to build robust, interoperable, inclusive, and sustainable systems thus contributing to the achievement of financial inclusion goals and inclusive financial integrity.

---

## SCOPE AND APPLICATION

The policy model builds a framework that draws on the approaches used by AFI member countries for developing a policy and regulatory environment to enable digital ID and e-KYC; design and build the infrastructure and technical features of the system; and leverage the digital ID for e-KYC processes. Financial inclusion of women and other disadvantaged groups such as youth, the elderly, persons with disabilities, and forcibly displaced persons are common themes throughout the model. Principles have been formulated to address the specific needs of these groups.

These principles highlight key practical and operational aspects that must be considered while developing a digital ID system and utilizing it for e-KYC. They are based on best practices and experiences of AFI member countries as well as service providers and technical knowledge partners. While the policy model can be used as a standalone guide, it should be noted that technology, industry practices, and use cases are rapidly evolving, and that policy approaches need to be adaptable to such developments. The policy model will be regularly reviewed and updated in order to take these developments into account.

## READING INSTRUCTIONS

The policy model's core topics are interconnected. Please read the entire document holistically.

### OVERVIEW OF KEY CONCEPTS AND DEFINITIONS

#### ACCESS TO THE DIGITAL ID SYSTEM (CLARIFICATION OF AUTHENTICATION, E-KYC)

For the purposes of this Model, access refers to being an authorized system user or administrator being able to authenticate a person's identity based on one or more factors or being able to complete an e-KYC transaction by authenticating and viewing or receiving user data required for KYC compliance.

#### ANTI-MONEY LAUNDERING AND COUNTERING THE FINANCING OF TERRORISM (AML/CFT)

These refer to policies, laws and regulations for maintaining the integrity of the financial system by deterring and preventing the use of the financial system for money laundering, terrorism financing, and other such illicit activities.

#### AUTHENTICATION

This refers to the process of checking whether a person who claims an identity is the rightful owner of that identity based on one or more factors (something they have, know, or are) previously provided with the KYC information.

#### CREDENTIALS

A credential is any document, object, or data structure that can digitally affirm the identity of an individual through some method of authentication in an identity system.<sup>1</sup> There are several kinds of factors that can be used as identity credentials, such as smartcards, biometrics, passwords, one-time passwords (OTPs).

#### DEDUPLICATION

Deduplication refers to eliminating duplicate or redundant information. In the case of a digital ID system, it is the process of checking for duplicate entries, usually through a biometric matching process, to ensure unique additions are made.

#### DIGITAL IDENTITY (ID)

Digital ID refers to any digitalized or digital identity document that is provided or issued by governments, it could also include forms of digital ID that are provided in partnership with the private sector or other authorized entities, such as the United Nations High Commissioner for Refugees, but which are linked to a person's "official" or "legal" identity and recognized by the government for official purposes.<sup>2</sup>

#### DIGITAL ID SYSTEM

This is a system for the process of identity proofing and enrolment, and authentication. Identity proofing and enrolment can be done with either digital or physical documentation or a combination of both. However, binding, credentialing, authentication, and portability or federation must be digital.<sup>3</sup>

#### ELECTRONIC KNOW YOUR CUSTOMER (E-KYC)

e-KYC refers to the process of electronically verifying the credentials of a customer in line with KYC processes of the country with respect to risk-based approaches. For example, this may include biometric and/or video identification as recommended by the Financial Action Task Force (FATF) in its digital ID guidance (2020).

#### FINANCIAL ACTION TASK FORCE

The FATF is an intergovernmental and standard setting body responsible for establishing and promoting international standards to combat money laundering, the financing of terrorism, and proliferation financing.

#### FOUNDATIONAL IDENTITY

Foundational IDs are multipurpose IDs, such as a national ID and a civil registry, that provide identification for the general population.

#### FUNCTIONAL IDENTITY

Functional IDs manage identification, authentication, and authorization for specific sectors or use-cases, such as voting, taxation, and social protection.<sup>4</sup>

1 World Bank. 2019. ID4D Practitioner' Guide: Version 1.0 (October 2019). Washington, DC: World Bank. Available at: <http://documents1.worldbank.org/curated/en/248371559325561562/pdf/ID4D-Practitioner-s-Guide.pdf>

2 Ibid.

3 FATF (2020), Guidance on Digital ID, FATF, Paris. Available at: <http://www.fatf-gafi.org/media/fatf/documents/recommendations/Guidance-on-Digital-Identity.pdf>

4 World Bank. 2019. ID4D Practitioner's Guide: Version 1.0 (October 2019). Available at: <http://documents1.worldbank.org/curated/en/248371559325561562/pdf/ID4D-Practitioner-s-Guide.pdf>

**IDENTITY PROOFING/VERIFICATION**

This is a process for establishing or determining a person's identity by collecting and proofing relevant identity information.

**INCLUSIVE FINANCIAL INTEGRITY**

This refers to a successful alignment of financial inclusion and AML/CFT or financial integrity policy objectives. This is essentially attained when a country has both implemented global financial integrity standards and also expanded access to, and usage of, quality formal financial services. A clear national vision, effective coordination of public and private stakeholders, and integration of AML/CFT and financial inclusion processes at the national level are key factors to achieving inclusive financial integrity.

**PRINCIPLE OF PROPORTIONALITY**

For the purposes of the policy model, the principle of proportionality advocates that countries should collect adequate data that are relevant for the optimal operation of the digital ID system. Excess information should not be collected.

**SENSITIVE DATA**

This data comprises biographic information, the collection of which is particularly sensitive because the information could be used for profiling or discriminate against an individual or put their security at serious risk. The fields of biographic information should therefore not be made easily available to third parties or placed in the public domain. They include, but are not limited to, data on racial or ethnic origin, political opinions, religious beliefs, sexual orientation, and so on.<sup>5</sup>

**USER**


This refers to the individual who is onboarded to the digital ID system and who provides identity information for the various use cases.

---

<sup>5</sup> Ibid.

This policy model has been developed around  
**THREE POLICY CONSIDERATIONS:**

**1**  
POLICY AND REGULATORY FRAMEWORK FOR IMPLEMENTING DIGITAL ID AND E-KYC



See page 6

**2**  
POLICY CONSIDERATIONS FOR DESIGNING THE PLATFORM AND BUILDING THE DIGITAL ID SYSTEM AND THE TECHNOLOGY INFRASTRUCTURE



See page 14

**3**  
POLICY CONSIDERATIONS TO IMPLEMENT KEY PROCESSES AND USE CASES LEVERAGING THE DIGITAL ID FOR E-KYC



See page 19

# PART 1: POLICY AND REGULATORY FRAMEWORK FOR IMPLEMENTING DIGITAL ID AND E-KYC

This section details the framework to build an enabling regulatory environment to foster the most effective use of digital ID and e-KYC. Overarching laws on data protection and governance are also detailed, along with strategies for financial inclusion and gender considerations.



## I: LAWS AND REGULATIONS ON DIGITAL ID AND E-KYC

REGULATORY CATEGORY	GUIDING PRINCIPLE	RATIONALE
<b>DIGITAL ID AND E-KYC LAWS, REGULATIONS, AND POLICIES</b>	<p>Enact specific foundational laws in the country governing the following key aspects:</p> <ol style="list-style-type: none"> <li>AML/CFT and risk-based, tiered KYC</li> <li>Identity documents and digital ID<sup>6</sup></li> <li>Data protection and privacy</li> <li>Cybersecurity</li> </ol> <p>Additional to or integrated into foundational laws:</p> <ol style="list-style-type: none"> <li>e-KYC</li> </ol> <p>It is not necessary to enact specific laws in the country governing digital ID and e-KYC. It is sufficient that they are included in the regulatory framework.</p>	<p>To provide clarity in the application of the law, rule, or directive around the use and management of ID and its various applications. It helps in the following ways:</p> <ul style="list-style-type: none"> <li>&gt; Increased compliance and informed decision making for stakeholders</li> <li>&gt; Reduced risk to privacy and fraud</li> <li>&gt; Social and economic benefits for both public and the private sector</li> </ul>
<b>CONTENT AND SCOPE OF LAWS, REGULATIONS, AND POLICIES</b>	<p>Laws, regulations, and guidelines should be drafted before the implementation of a national digital ID program or e-KYC to foster an enabling environment within the legal and regulatory boundaries.</p> <p>Key aspects that should be part of the regulatory framework for a country can include:<sup>7</sup></p> <ol style="list-style-type: none"> <li>Objective and scope of use of the digital ID, including use cases of digital ID such as e-KYC</li> <li>Data points to be collected and credentials to be issued</li> <li>Background and rationale</li> <li>Validity and renewal process</li> </ol>	<p>Enabling policies and frameworks detailing the use and scope of digital IDs will help stakeholders to take concrete steps towards building a wide range of aspects around digital ID, such as governance, policy, operation, technology, and law, etc.</p> <p>Clearly specifying what data is to be collected will ensure consumer protection and mitigate regulatory arbitrage.</p> <p>Clear guidelines also foster cooperation and coordination among various stakeholders. It helps them understand what the ID infrastructure allows, what are the limitations and opportunities, what needs to be changed, who gets impacted, and how.</p>

6 Digital ID systems are those that use digital technology throughout the identity life cycle, including for data capture, validation, storage, and transfer; credential management; and identity verification and authentication. See, World Bank. 2019. ID4D Practitioner’s Guide: Version 1.0 (October 2019). Available at: <http://documents1.worldbank.org/curated/en/248371559325561562/pdf/ID4D-Practitioner-s-Guide.pdf>

7 This list is not exhaustive. More elements can be added based on country context and requirements.

REGULATORY CATEGORY	GUIDING PRINCIPLE	RATIONALE
<b>CONTENT AND SCOPE OF LAWS, REGULATIONS, AND POLICIES</b>	<ul style="list-style-type: none"> <li>e. Details and restrictions on the processing of data</li> <li>f. Details on consent mechanism/architecture, with provisions to revoke consent</li> <li>g. Restrictions on sharing information, including access and permissions to third parties</li> <li>h. Data integration and interoperability</li> <li>i. Details on data storage and management, including disaster recovery and business continuity plans</li> <li>j. Security and confidentiality of information</li> <li>k. Governance and institutional structures governing the digital ID and e-KYC</li> <li>l. Roles, responsibilities, and accountability of the entities in charge and users/participants</li> <li>m. Offenses and penalties</li> <li>n. Grievance mechanisms and escalation</li> <li>o. Procedures for updating information</li> <li>p. Special measures for women and other disadvantaged groups such as youth, the elderly and persons with disabilities, and specific amendments to existing laws to integrate forcibly displaced populations</li> <li>q. Audits and reviews</li> <li>r. Use of digital signature</li> </ul> <p>Laws should be adaptable and consistent with other, related laws in the respective jurisdictions in order to make them more effective.</p>	
<i>continued</i>		
<b>GLOBAL STANDARD REFERENCES FOR KYC</b>	<p>Consult and ensure adherence to the FATF Standards and related guidance<sup>8</sup> in formulating the AML/CFT, KYC and e-KYC<sup>9</sup> policies. This includes the FATF Guidance on Digital ID.<sup>10</sup></p> <p>Ensure performance, and/or outcomes-based criteria when establishing the required attributes, evidence, and processes for proving official identity for customer due diligence.</p>	<p>To build a robust KYC framework with maximum scope for the stakeholders. Following the FATF Recommendations and guidance helps in keeping pace with developing rules and regulations. However, it is important that AML/CFT, KYC and e-KYC policies are carefully contextualized to the country’s unique context and ML/TF risks.</p>

8 FATF. 2012-2021. International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation. Available at: <https://www.fatf-gafi.org/publications/fatfrecommendations/documents/fatf-recommendations.html>

9 There is no international standard on e-KYC. However it is addressed to an extent in: FATF. 2020. Guidance on Digital Identity. Available at: <http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/Guidance-on-Digital-Identity-report.pdf>

10 Ibid.

REGULATORY CATEGORY	GUIDING PRINCIPLE	RATIONALE
<b>RISK-BASED TIERED KYC</b>	<p>Conduct regular national, sectoral, and institutional-level risk assessments which should serve as a basis for the development of risk-based tiered KYC. This will help to identify any financial exclusion challenges faced by any category of the population which may necessitate proportionate or bespoke KYC requirements to avoid unduly restricting of access to low-risk products and services.</p> <p>A risk-based approach should ensure that KYC requirements which are applied are proportionate to the assessed level of risk, including consideration of reduced requirements where risks are assessed to be lower. Effective implementation of the risk-based approach to customer due diligence should support financial inclusion objectives. Risk assessments can be done on multiple levels:</p> <ul style="list-style-type: none"> <li>&gt; Customer/Country/Geography</li> <li>&gt; Products/Services/Transactions/ Channels</li> </ul> <p>Determine a relevant timetable to conduct subsequent risk assessments.</p>	<p>To determine the level of risk that financial services providers are exposed to when catering to different categories of the population. This is an important step to ensure that financial services and products are developed for the most disadvantaged and will not impede their access and usage as well as to maintain an up-to-date understanding of ML/TF risks in the country.</p> <p>A risk-based approach will ensure that measures taken to prevent or mitigate money laundering, terrorism financing, and proliferation financing are commensurate to the risks identified. Regular national, sectoral or institutional-level risk assessments are needed to ensure updated practices and mitigation of new risks.</p>
<b>E-KYC</b>	<p>Develop a clear policy and implementation plan for e-KYC, leveraging foundational ID such as national ID or functional IDs with wide penetration.</p> <p>Ensure the e-KYC system accommodates risk-based tiered KYC practices.</p> <p><i>(For more specific details please refer to Section III)</i></p>	<p>Authentication and verification of identity through e-KYC processes have shown a high level of savings in countries both in terms of time and cost, for financial services providers. It will also foster financial inclusion for women by eliminating gender-specific challenges (need to travel to transaction points, being accompanied by a male companion, etc.).</p>
<b>SUPPORT IMPLEMENTATION</b>	<p>Issue guidance to all relevant stakeholders on the interpretation of different laws and regulations. More specifically, financial institutions, including but not limited to banking companies, insurance companies, brokers, etc, and intermediaries. Guidance should ensure clarity and clear steps for the implementation of concepts related to compliance and regulating cross-border transactions due to foreign jurisdictions.</p> <p>Central banks and relevant authorities should study developments in AML/CFT locally, regionally and globally in order to provide guidance to accountable institutions to remain compliant at all times and document and share the interpretations of FATF Recommendations and related guidance.</p>	<p>To ensure regulatory clarity among financial institutions and to understand their most urgent challenges in complying with AML/CFT regulations. This will facilitate necessary actions and mitigation measures to navigate through such challenges.</p>



REGULATORY CATEGORY	GUIDING PRINCIPLE	RATIONALE
<b>SUPPORT IMPLEMENTATION</b>	<p>This will enable effective implementation and better understanding among financial institutions. Provide assumptions, if any, and a standardized implementation plan to avoid any challenges or discrepancies that may arise.</p> <p>Provide support and promote open dialogue on implementation and address any challenges that may arise post implementation.</p>	
<i>continued</i>		
<b>COLLECTION OF PERSONAL IDENTIFIABLE INFORMATION</b>	<p>Collect the minimum amount of data points from citizens as needed to satisfy KYC requirements and inform customers explicitly about the possible usage of collected data.</p> <p>The personal identifiable information collected should consider the scope and usability of the system and determine through proportionality, what is mandatory.</p> <p>Sensitive information, if collected, should be further classified into tiers to ensure additional privacy and security by limiting full data access to third-party entities.</p>	<p>To respect user privacy and adhere to the principles of proportionality by not collecting more data than is necessary. It helps to:</p> <ul style="list-style-type: none"> <li>&gt; Ensure minimum breach of privacy of users</li> <li>&gt; Realize time and cost savings incurred in collecting and verifying each of the collected data fields</li> <li>&gt; Reduce the risk of leaking sensitive data and surveillance</li> </ul>
<b>VERIFICATION OF DATA AND IDENTITY PROOFING</b>	<p>Verify data collected against independent and reliable data or documents of issuer entities, such as national ID documents.</p> <p>Verification against other civil databases and biometric authentication on the spot are commonly used identity proofing methods. As an exception handling mechanism, consider community proofing strategies for users without documents for low-risk categories.<sup>11</sup></p>	<p>To safeguard against fraud and identity theft where possible.</p>
<b>COLLECTION OF BIOMETRICS</b>	<p>Establish clear policies on the collection of biometric information, its storage, and usage. Determine what biometrics are most useful for the system being developed, keeping in mind the principle of proportionality and utility.</p> <p>Minimum biometrics should be collected to identify an individual uniquely — fingerprints, facial, and iris have proven to show the highest use. Voice can be considered for countries with high feature phone use. Invasive methods such as collecting DNA should go through a complete due diligence process and be compliant with existing data protection and privacy laws.</p>	<p>Biometric collection allows for both identification and authentication. Authentication based on biometric matching is more efficient and accurate. It also helps in the deduplication of identity records.</p>

11 FATF. 2020. Guidance on Digital Identity, p. 38. Available at: <http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/Guidance-on-Digital-Identity-report.pdf>

REGULATORY CATEGORY	GUIDING PRINCIPLE	RATIONALE
UPDATING BIOMETRICS	Draft procedures to update biometric information that is subject to change due to age, occupation, physical or medical conditions. Draw out guidelines for a mandatory update in special cases, such as for children, the elderly and persons with disabilities.	To ensure minimum issues and failures during biometric authentication and verification.
UPDATING USER DATA	<p>Draft guidelines to make corrections, amendments, or deletion of inaccurate information in digital ID.</p> <p>The guidelines should allow flexibility to recognize users by the gender they identify with, rather than the gender assigned to them at birth and update this information.</p>	To preserve data integrity, retain correctness and ensure most recent data is stored and processed.

## II: LAWS ON DATA PROTECTION AND PRIVACY

REGULATORY CATEGORY	GUIDING PRINCIPLE	RATIONALE
DATA PROTECTION AND PRIVACY POLICY	<p>Include key elements of data protection and privacy in the guidelines, directives, and existing laws on the collection, processing, management, and storage of personal data of individuals, such as:</p> <ol style="list-style-type: none"> <li>Mandatory consent for the processing of personal data by assessing the validity of blanket consent compared with transactional consent</li> <li>Details of scenarios of when consent would not be required, e.g. court order</li> <li>Special provisions for children (collecting limited demographic information and that which can be linked to the legal guardian) and disadvantaged groups</li> <li>Privacy by design principles extended to data fiduciaries</li> <li>Classification of sensitive data</li> <li>Deletion of data when purpose of data collection has expired</li> <li>Measures and penalties for mishandling data, including submission of false data by personnel</li> </ol>	A comprehensive data protection and privacy policy is required to govern both the public and private sector as it is challenging for stakeholders to comply with multiple rules and regulations on the use and management of ID.
PRIVACY AUDITS AND ASSESSMENTS	<p>Establish an independent data protection authority that is responsible for ensuring that the treatments of personal data are implemented according to legal provisions and guidelines.</p> <p>Specify the process for conducting privacy risk reviews/assessments of the overall system. Guidelines should state which third parties are authorized to do so as well as the time intervals.</p>	To review policy and procedures on how data is collected, managed, and stored. It will also verify compliance with the guidelines on data protection and privacy, help identify risk and build mitigation strategies.

### III: GOVERNANCE AND INSTITUTIONAL STRUCTURES

REGULATORY CATEGORY	GUIDING PRINCIPLE	RATIONALE
<b>ENFORCEMENT AND GOVERNANCE STRUCTURES</b>	<p>Establish an independent entity in charge of planning, management, and administration of the digital ID. The entity should have powers to enforce and assign responsibility based on the rules and regulations drawn out in the laws. A board consisting of representatives from key financial regulatory institutions, financial intelligence unit, and relevant ministries such as IT, communications, justice, and social protection should be created to oversee activities of this independent entity.</p> <p>To ensure stakeholder cooperation, collaboration and harmonization in the implementation of digital ID, the independent body should also have jurisdiction and oversight of other third-party entities that use the ID data to ensure no misuse occurs.</p> <p>Build the capacity of actors in the ecosystem to highlight the principles of cooperation in the implementation of the ID system, the adoption of effective e-KYC by FSPs, and proper oversight and supervision. Implementing partners should also promote digital literacy and make their customers aware of the need, uses and benefits of the ID before its launch.</p>	<p>To promote efficiency, accountability, transparency and prevent exclusion and misuse.</p>
<b>FOSTERING INNOVATION</b>	<p>Promote initiatives in the country to foster innovations related to digital ID. Regulatory sandboxes, innovation hubs or test and learn approaches have been successful in offering an enabling environment for innovations related to:</p> <ol style="list-style-type: none"> <li>a. Cost-effective ways to deliver services through technology-enabled channels</li> <li>b. Remote onboarding and e-KYC by leveraging digital ID for different services and products</li> <li>c. Alternative credit rating options for people with no formal credit score, particularly women entrepreneurs</li> <li>d. Emerging technology</li> </ol> <p>Consider regional sandboxes to create a more sustainable working model through joint funding and sharing of technical knowledge.</p> <p>The sandbox can be used for innovations across sectors and use cases. This environment can be specifically used for innovations to accelerate financial inclusion specifically for disadvantaged groups while also innovating new products and services for existing customers.</p>	<p>Approaches to foster innovation such as regulatory sandboxes, innovation hubs or test and learn approaches provide the right environment for oversight, visibility, and supervision by regulators while also allowing innovation by the private sector of efficient solutions and interesting use cases.</p>

## IV: FINANCIAL INCLUSION STRATEGIES

REGULATORY CATEGORY	GUIDING PRINCIPLE	RATIONALE
<b>NATIONAL STRATEGIES FOR FINANCIAL INCLUSION</b>	<p>Clearly integrate digital ID and e-KYC development in national policies, strategies and initiatives to accelerate financial inclusion, including:</p> <ul style="list-style-type: none"> <li>a. National Financial Inclusion Strategy (NFIS)<sup>12</sup></li> <li>b. National Financial Education or Literacy Strategy</li> <li>c. A coordination structure to drive national financial inclusion efforts which should be led by the central bank and/or ministry of finance comprised of relevant stakeholders such as the ministries of finance, IT, communications, social protection, education, women and others. The structure can have working groups for different NFIS pillars and comprising private sector, civil society, development and humanitarian groups.</li> <li>d. Specific adjustments for onboarding to the digital ID system for disadvantaged populations,<sup>13</sup> such as doorstep onboarding, alternative documents, and community proofing, e.g. an endorsement by a qualified intermediary or entity such as UNHCR</li> <li>e. Introduction of specific products and services targeted at disadvantaged groups, including the elderly and persons with disabilities, such as low-risk products and services, government-backed low-cost insurance, no-frills bank accounts with no maintenance charges, low-interest credit for low-income groups and women, etc.</li> <li>f. Financial awareness and literacy projects</li> </ul>	<p>To ensure that design and implementation of digital ID and e-KYC contribute to the advancement of financial inclusion in a coherent, coordinated and focused manner, towards granting greater access to and usage of quality, affordable financial services specifically for the unserved and underserved population.</p>
<b>IMPLEMENTATION OF NATIONAL FINANCIAL INCLUSION STRATEGIES</b>	<p>Leverage on the national coordination structure for financial inclusion to build a collaborative effort for NFIS implementation led by government agencies, established by law or decree, and involving private sector and civil society stakeholders. The coordination structure will ensure sound multi-stakeholder coordination, distribution of responsibility, and effective accountability.</p> <p>Implementation of NFIS should be aligned with national financial education, financial literacy and consumer protection policies and strategies.</p> <p>Implementation can be expedited by using "mission mode" projects with clearly defined objectives and timelines for quick results. Countries with digital ID can leverage the ID for efficient onboarding and e-KYC.</p>	<p>To ensure the achievement of national financial inclusion goals, including through attaining buy-in from different key stakeholders and ministries, as well as the committed resources and budget to implement policy actions and undertake the activities.</p>

<sup>12</sup> Alliance for Financial Inclusion, 2020. Policy Model for National Financial Inclusion Strategy. Available at: <https://www.afi-global.org/publications/policy-model-for-national-financial-inclusion-strategy/>

<sup>13</sup> Disadvantaged population groups include the economically disadvantaged, youth, the elderly, persons with disabilities, forcibly displaced persons, racial and ethnic minorities, children from low-income groups, and others that the country might have explicitly defined.

**V: GENDER-INCLUSIVE STRATEGIES**

REGULATORY CATEGORY	GUIDING PRINCIPLE	RATIONALE
<b>GENDER-INCLUSIVE PROCESSES</b>	<p>Strategize and initiate a thorough analysis of the policies and digital ID system to ensure gender inclusivity throughout the lifecycle<sup>14</sup> of the digital ID.</p> <p>Some key considerations are offline solutions and mobile or women-only registration days and promoting gender-sensitive interfaces. Collaboration and cooperation of public and private institutions specializing in women's affairs would support the development of a focused gender-inclusive strategy.</p>	To ensure there is no exclusion in the digital ID system due to additional barriers faced by women.
<b>COLLECTION OF SEX AND AGE-DISAGGREGATED DATA</b>	<p>Promote the collection, tracking, analysis and monitoring of sex and age-disaggregated data. Determine the frequency and sources (supply side and demand side) of collection.</p> <p>Consider allowing access and dissemination of the data to other public entities that might benefit from this information.</p>	To ensure data is collected for better policy and strategic decision making

## PART II: POLICY CONSIDERATIONS FOR DESIGNING THE PLATFORM AND BUILDING THE DIGITAL ID SYSTEM AND THE TECHNOLOGY INFRASTRUCTURE

This section details the principles and considerations for designing and building the digital ID system, the technology infrastructure as well as the supporting architecture. These principles draw from, among others, those for data management and user services which are also key considerations for the digital ID system.



### I: DESIGNING THE ID SYSTEM

REGULATORY CATEGORY	GUIDING PRINCIPLE	RATIONALE
<b>TYPE AND FEATURES OF DIGITAL ID</b>	<p>Clearly define the type of digital ID<sup>15</sup> (foundational or functional) which is being implemented in the country. The decision should be based on a thorough examination of the needs and objectives of the identity program and after several rounds of discussions with all relevant stakeholders.</p> <p>The key parameters to be considered are:</p> <ol style="list-style-type: none"> <li>Availability of a foundational ID system and infrastructure on which the digital ID can build on</li> <li>Its scalability and plans to leverage the ID</li> <li>Cost implications (including analysis of human resources and infrastructure, digital device ownership)<sup>16</sup> as well as incentives such as enabling tax regimes and cost sharing</li> <li>Implementation and roll-out plans will affect the nature of the ID and the decision to use a current functional ID and convert it to a foundational ID</li> <li>Mandatory registration or optional for some, and any prerequisites such as age, citizenship</li> </ol>	<p>To make the best use of the available resources, including budget, human resources, existing databases, and technology. To help the public and private sector demonstrate the kind of services (health, financial, social security, etc) that can be accessed using the ID.</p>

<sup>15</sup> Foundational ID are multipurpose IDs, such as national ID and civil registries that provide identification for the general population. Functional IDs manage identification, authentication, and authorization for specific sectors or use cases, such as voting, taxation, and social protections. See, World Bank. 2019. ID4D Practitioner's Guide: Version 1.0 (October 2019). Available at: <https://id4d.worldbank.org/guide/types-id-systems>.

<sup>16</sup> World Bank. 2018. Understanding Cost Drivers of Identification Systems). Available at: <https://documents1.worldbank.org/curated/en/702641544730830097/pdf/Understanding-Cost-Drivers-of-Identification-Systems.pdf>

REGULATORY CATEGORY	GUIDING PRINCIPLE	RATIONALE
<b>ADHERENCE TO INTERNATIONAL STANDARDS</b>	<p>Consult international standards on identity design and development and follow recommendations for privacy. Some key principles can be found in the following:</p> <ul style="list-style-type: none"> <li>a. World Bank: Principles of Identification</li> <li>b. ID4D: Technical Standards for Digital Identification</li> <li>c. Privacy by design</li> <li>d. FATF Guidance on Digital Identity Guidelines</li> <li>e. G20</li> <li>f. ISO</li> <li>g. Good ID</li> <li>h. International Association of Privacy Professionals</li> <li>i. ISO 27001:2013 on Information Security</li> </ul> <p>Key strategic decisions can be taken based on other country experiences, insights, and challenges but ensuring country context and requirements are central to the design.</p>	<p>To ascertain development is based on best practices and learnings from other jurisdictions and to ensure that the most appropriate design elements are considered carefully.</p>
<b>ISSUANCE OF CREDENTIALS</b>	<p>Evaluate in the country context which credentials are most appropriate for the use of the general population. Consider factors such as functionality, user preferences, and safety. Examples include, but are not limited to:</p> <ul style="list-style-type: none"> <li>a. Physical (cards)</li> <li>b. Digital (e-cards, ID number)</li> <li>c. Additional factors (PIN, password, OTP)</li> <li>d. QR code</li> </ul> <p>Physical cards provide a sense of safety, smart cards offer various functionalities, digital credentials are more lucrative but might pose an additional barrier for users without access to technology and in low connectivity areas.</p> <p>Ensure that chosen credentials are inclusive and do not impede the use of the digital ID for some sectors of the population. Digital IDs that would require a smartphone or similar device ownership would disadvantage some population group, such as women in certain countries who might not have access or agency to use a smartphone. Issuance of more than one credential will help solve these challenges.</p>	<p>To promote equal use of the digital ID and the associated services, while ensuring no additional barrier to use is created for any category of users.</p>

## II: ONBOARDING AND REGISTRATION PROCEDURES

REGULATORY CATEGORY	GUIDING PRINCIPLE	RATIONALE
<b>REQUIREMENTS FOR ONBOARDING</b>	<p>Issue guidelines on the requirements and process for onboarding for different categories of residents (citizen, foreigner, asylum seeker, gender). Establish clear and easy to attain minimum requirements for onboarding to the platform/identity system based on the objectives of the system. Ensure the minimum requirements set do not further impede some sections of society from being onboarded to the system.</p> <p>Consider the country context and the use of the digital ID to decide whether the onboarding should be push-based (automatic onboarding of all citizens) or pull-based (citizens need to explicitly apply). For foundational IDs that are leveraged for e-KYC practices, onboarding should cover a majority of the adult population.</p> <p>Countries with trusted digital databases that already cover some portion of the population can adopt a push-based full digital approach for onboarding. However, the registration process could be initiated for the unidentified population if there are gaps in coverage of the digital databases.</p> <p>Countries that prefer to build the database from the ground up to avoid using a database with discrepancies can use a pull-based approach.</p>	<p>To ensure wide and inclusive coverage of the digital ID and easy onboarding for all citizens and users.</p>
<b>ACCESS POINTS FOR USERS</b>	<p>Develop guidelines based on country requirements on access points for users to interact with the digital ID platform and for e-KYC services. These points can be used for onboarding, verification, authentication, and other services as required and have a robust monitoring system to promote the integrity of the registration process.</p> <p>Guidelines should ensure proper geographic coverage and adjustments to cater to disadvantaged groups of the population.</p> <p>Access points can be a government-run center, a separate chain of registration centers, or kiosks managed by other stakeholders but monitored by the government, or remote. Leverage private sector players for better reach and efficiency. Consider collaboration with digital access points for banking that might already be an established network.</p>	<p>To ensure easy access points for users to register and interact with the digital ID system, building their trust and willingness to use the ID for various other use cases.</p>
<b>DIRECT COSTS TO THE USER</b>	<p>Issue guidelines and enforce the same to ensure minimal or no direct costs for the citizens or users to be onboarded to the digital ID system or to use e-KYC facilities. Minimal cost to users will encourage use. Costs if any, should be levied in case of lost credentials (cards) that require re-issue.</p>	<p>One of the main objectives of leveraging a digital ID system is to reduce the cost and time spent for users. Additional costs to use this system will reduce their willingness to participate.</p>



## III: SYSTEM CAPABILITIES

REGULATORY CATEGORY	GUIDING PRINCIPLE	RATIONALE
<b>TECHNICAL STANDARDS</b>	<p>Define specific technical standards to be followed in developing the ID platform and database. Technical standards can be set using references of other digital ID and e-KYC practices and guidance from standards-setting bodies.<sup>17</sup> In addition to technical standards, the system needs to ensure the following key aspects:</p> <ol style="list-style-type: none"> <li>a. Robustness and high functionality</li> <li>b. Customizability and configurability</li> <li>c. Privacy embedded into the design.<sup>18</sup></li> <li>d. Standards for collecting, storing, and sharing the data with third parties, when allowed</li> <li>e. Real-time access to data for e-KYC and other use cases</li> <li>f. Additional infrastructure to support application programming interfaces (API) for the digital ID for e-KYC and authentication procedures, and to streamline the accessing of data for productive use.</li> </ol> <p>Consider open-source options for technology development to prevent vendor lock-in, and for economic development. Decisions on centralized or decentralized ID should take into consideration the infrastructure and needs of the country.</p>	<p>To help assess the country's available technology infrastructure and make further amendments in line with international standards. It will also ensure standards for digital ID and e-KYC meet the desired performance targets. API infrastructure will provide convenient mechanisms for stakeholders to verify and authenticate using the digital ID database.</p>
<b>TECHNICAL FEATURES OF THE SYSTEM</b>	<p>Provide guidance on the technical features that should be programmed into the system to ensure efficiency. Some key features that will help improve the system capabilities are:</p> <ol style="list-style-type: none"> <li>a. Automated and dynamic deduplication</li> <li>b. Checks for fraud and embedded anti-fraud processes</li> <li>c. Separate databases for biometric and demographic data</li> <li>d. Real-time linkages with birth and death registers for automatic updates</li> <li>e. Support multiple biometric authentication mechanisms</li> <li>f. Offline authentication and onboarding</li> <li>g. Exception management procedures</li> <li>h. Consent management architecture</li> <li>i. Linkages with other ID systems to promote different use cases, such as driver's license, social security, tax identification system, national health system, etc.</li> </ol>	<p>To ensure the system is following global best practices and is constantly updated and maintained.</p>
<b>TECHNICAL AUDITS AND ASSESSMENTS</b>	<p>Issue guidelines and enforce periodic reviews of the underlying technology for efficiency, innovation, and cost-effectiveness.</p>	<p>To ensure timely upgrades and adherence to evolving industry standards and best practices.</p>

17 World Bank. 2018. ID4D Practitioner's Note. Catalog of Technical Standards for Digital Identification Systems. International Bank for Reconstruction and Development / The World Bank. Available at: <https://olc.worldbank.org/system/files/129743-WP-PUBLIC-ID4D-Catalog-of-Technical-Standards.pdf>

18 Alliance for Financial Inclusion. 2021. Guideline Note on Data Privacy for Digital Financial Services. Available at: <https://www.afi-global.org/publications/guideline-note-on-data-privacy-for-digital-financial-services/>

## IV: DATA MANAGEMENT

REGULATORY CATEGORY	GUIDING PRINCIPLE	RATIONALE
<b>360-DEGREE DATA MANAGEMENT (DATA AT REST, IN USE AND IN MOTION)</b>	<p>Issue and enforce strict data management procedures for all stakeholders involved in the data collection, processing, and storage of user data.</p> <ol style="list-style-type: none"> <li>Tokenization, virtualization, and two-factor authentication when data is being used</li> <li>Physical and technical barriers to access when data is stored and at rest, including authorized access, storage and achieving methods</li> <li>Encryption and secure lines when data is being transmitted</li> </ol> <p>Legally collected data may be used to generate aggregate data or statistical summaries without reference to or identification of any specific individual.</p>	To enforce all the data privacy and security measures and ensure that data management practices protect user data from external attacks.

## V: USER SERVICES

REGULATORY CATEGORY	GUIDING PRINCIPLE	RATIONALE
<b>USER SERVICES</b>	<p>User services should include:</p> <ol style="list-style-type: none"> <li>Ability to provide consent and authorizations for third party use</li> <li>Ability to revoke consent</li> <li>Ability to lock biometrics</li> <li>Visibility and ability to track transactions where personal data was requested and processed</li> <li>Options for portability of information</li> <li>Channel for dispute mechanism and requesting compensation</li> </ol> <p>Guidelines on how users can access such services should be published and circulated to users. Multiple channels should be provided, preferably to ease access, mobile applications; USSD and website access can be considered over manual requests</p> <p>Implementing entities should also devise ways to effectively communicate with users to build awareness of the provisions, consent, rights, services, and use cases for the ID systems. Users should also be informed of channels and devices being used within the ecosystem.</p>	To ensure that the systems built are user-centric and control of data is in the hands of the user.

# PART III: POLICY CONSIDERATIONS TO IMPLEMENT KEY PROCESSES AND USE CASES LEVERAGING THE DIGITAL ID FOR E-KYC

This section highlights one of the key use cases for the digital ID, which is e-KYC and authentication services. It summarizes effective practices implemented by AFI members and globally and details a framework and guiding principles to build robust processes for e-KYC, including access, interoperability, last-mile infrastructure, and exception handling.



## I: E-KYC AND AUTHENTICATION FRAMEWORK

REGULATORY CATEGORY	GUIDING PRINCIPLE	RATIONALE
<b>FRAMEWORK FOR E-KYC IMPLEMENTATION</b>	<p>Provide guidance and build an e-KYC framework by detailing the following key aspects, if applicable:</p> <ul style="list-style-type: none"> <li>a. Scope of simplified and regular e-KYC for different stakeholders based on the risk identified</li> <li>b. Applicability of e-KYC (for people with digital ID and exception measures for those without digital ID)</li> <li>c. Collecting user consent for data processing, storage, and management</li> <li>d. Authorization of third parties for access for legitimate use</li> <li>e. Use of video identification<sup>19</sup></li> </ul>	<p>To clearly define the scope and use of e-KYC services and other operations. This will help build an implementation strategy with clear objectives and targets.</p>
<b>AUTHENTICATION MECHANISM</b>	<p>Consult with relevant stakeholders and technical experts to develop an authentication mechanism that is relevant to the country's context and meets the AML/CFT requirements. The digital ID system can be leveraged to cater to various levels of assurance using both demographic and biometric authentication.</p> <p>Some of the key factors that are used in identity authentication leveraging a digital ID system are:</p> <ul style="list-style-type: none"> <li>a. Possession factors (ID number, QR code) Something that a person demonstrates that they have, such as a physical or virtual card or certificate</li> <li>b. Biometric factors (fingerprint, iris, face)</li> <li>c. Knowledge factors (PIN, OTP, login ID). Something that a person already knows</li> </ul>	<p>To build flexible, secure, and efficient authentication systems with effective recourse measures to verify and authenticate the vulnerable population (individuals whose fingerprints wear out with age or due to certain kinds of professions, persons with disabilities who are not able to authenticate using their iris, etc).</p>

<sup>19</sup> High resolution video transmission allowing for remote identification and verification and proof of “liveness”. See, FATF. 2020. Guidance on Digital Identity. Available at: <http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/Guidance-on-Digital-Identity-report.pdf>

REGULATORY CATEGORY	GUIDING PRINCIPLE	RATIONALE
<b>AUTHENTICATION MECHANISM</b> <i>continued</i>	<p>Establish whether it is decentralized authentication, using last-mile devices such as card readers, or centralized with real-time matching with digital ID database.</p> <p>The authentication mechanism should also ideally be device agnostic and multimodal (i.e., able to use different factors and credentials for verification). Two-factor authentication systems meet higher safety requirements and multimodal systems will offer a built-in exception handling process.</p>	
<b>MATCHING PARAMETERS FOR AUTHENTICATION</b>	<p>Develop appropriate matching parameters based on references and technically accepted limits.</p> <p>Ideally matching parameters for numerical data, such as date of birth, phone numbers, should be 100 percent.</p> <p>Biometric factors can be between 80 and 100 percent to adjust for the quality of scanners and last-mile devices.</p>	<p>Matching parameters define the precision of the system; high levels of matching parameters will help build trust in the system's capabilities.</p> <p>However, this should be weighed against the possibility of increased failure rates to ensure a balanced final metric.</p>

## II: ACCESS AND INTEROPERABILITY FOR THIRD PARTY STAKEHOLDERS

REGULATORY CATEGORY	GUIDING PRINCIPLE	RATIONALE
<b>STREAMLINED PROCEDURES FOR ACCESS AND USAGE</b>	<p>Define a standardized set of rules of engagement for third-party stakeholders who want access to the system. Highlight the minimum requirements and permissions required for access.</p> <p>Detail out the steps and procedures for gaining access and the requirements from the third party, in terms of data protection and security measures, whether access is granted to individual stakeholders through an MoU<sup>20</sup> or through authorized entities.</p>	<p>To promote uniform, fair market access to stakeholders to leverage the system. Ensure standardized documentation such as MoUs, non-disclosure agreements (NDAs) and other contractual agreements.</p>
<b>TIERED ACCESS TO DATA</b>	<p>Define and publish a standardized list of different levels of services using the digital ID, such as authentication and e-KYC (demographic and biometric), and auto-fill user data, among others.</p> <p>This tiered system should be based on principles and level of access rather than based on individual entity needs.</p>	<p>To enable industry players to choose from the set list based on their requirements and help them prepare their internal systems accordingly.</p>
<b>CHANNELS OF ACCESS</b>	<p>Provide clear guidelines on the available channels and mechanisms for accessing the data in the digital ID platform for third parties. Channels can be finalized based on a risk analysis of the various alternatives and their pros and cons.</p> <p>Access can be provided through APIs, web service links, or direct links to the system through authorizations.</p>	<p>Available channels should ensure easy streamlined access for uninterrupted economic use of the data and services.</p>

REGULATORY CATEGORY	GUIDING PRINCIPLE	RATIONALE
<b>ECONOMIC COST STRUCTURES</b>	<p>Through detailed consultation and pricing strategy discussions, understand the willingness to pay among stakeholders. Different models adopted could be:</p> <ol style="list-style-type: none"> <li>Transaction-based tiered costing structure with a fee depending on the level of access and service provided</li> <li>Subscription-based model charged annually or monthly</li> </ol> <p>Pricing models<sup>21</sup> currently in use are free for public entities, and private entities are charged minimal amounts. A simple authentication leveraging the digital ID system has negligible costs while an e-KYC request with data sharing is slightly higher.</p>	Economic costs for services will encourage adoption among stakeholders and provide some income to the system administrators to ensure the sustainability of the system.
<b>MONITORING AND SUPERVISION OF ACCESS AND USAGE</b>	<p>Provide guidelines to implementing entities on monitoring mechanisms that should be in place for third parties who have access. These mechanisms should be defined in the MoU. Monitoring mechanisms should include regular reports, notifications of any breaches, and details of charges and fines levied. These measures should be agreed upon by implementing entities as well as third party stakeholders.</p>	To ensure data protection practices are also followed by all ecosystem players and penalize any misuse or frauds.

### III: LAST-MILE DEVICES AND INFRASTRUCTURE

REGULATORY CATEGORY	GUIDING PRINCIPLE	RATIONALE
<b>LAST-MILE INFRASTRUCTURE</b>	<p>Establish and publish guidelines or industry standards for devices that are used for last-mile authentication of users, such as biometric scanners and card readers.</p> <p>Consider certification of devices used at the last mile that can ensure standardized technical features, quality, and safety requirements.</p> <p>Standards and guidelines should ensure that only authorized/certified devices are used to access the platform of the digital ID. Serial number tracking or registration to a central authority can be implemented to prevent misuse and provide a way to monitor devices used by last-mile functionaries.</p>	To ensure adherence to safety protocols and data protection and data privacy during data transfer and use.

21 World Bank. 2019. ID4D Practitioner's Note. Identity Authentication and Verification Fees: Overview of Current Practices. Washington, DC: World Bank. Available at: <http://documents1.worldbank.org/curated/en/945201555946417898/pdf/Identity-Authentication-and-Verification-Fees-Overview-of-Current-Practices.pdf>

## IV: USE CASES

REGULATORY CATEGORY	GUIDING PRINCIPLE	RATIONALE
<b>INTEROPERABILITY AND SHARED INFRASTRUCTURE</b>	<p>Engage market participants and other stakeholders to promote discussion and provide guidance on interoperability and use cases that can leverage the built infrastructure.<sup>22</sup></p> <p>Encourage discussions on the policy and regulatory requirements to facilitate interoperability for:</p> <ol style="list-style-type: none"> <li>Delivery of government services</li> <li>Social protection delivery of different departments/ ministries</li> <li>Formal financial institutions</li> <li>FinTechs</li> <li>Non-financial institutions, such as telcos</li> <li>Third-party authorized e-KYC/KYC companies</li> <li>Voting</li> <li>Tax administration</li> <li>Litigation activities</li> </ol>	To ensure sustained use and market efficiency through interoperable services and encourage stakeholders to commit to the shared infrastructure.

## V: EXCEPTION HANDLING AND GRIEVANCE RESOLUTION

REGULATORY CATEGORY	GUIDING PRINCIPLE	RATIONALE
<b>EXCEPTION HANDLING PROCEDURES</b>	<p>Document some of the key challenges that might arise and the exception handling procedures and protocols for the same.</p> <p>Procedures to be undertaken during authentication failures or biometric mismatch, particularly for e-KYC transactions.</p> <p>Alternative procedures in areas with low connectivity or other infrastructural challenges should also be laid out. Options such as offline mode can be considered using a QR code or card readers.</p>	To ensure streamlined, decentralized processes around biometric authentication by removing barriers to technology and literacy.
<b>GRIEVANCE RESOLUTION</b>	<p>Offer a robust grievance resolution infrastructure through multiple channels incorporating both human and technology interfaces. Channels should have easy access, proper feedback loops, and quick resolution times. Provision should also be made for grievances and disputes of user financial institutions.</p> <p>Consideration may be made for service level agreements on handling consumer complaints among key institutions responsible for the digital ID system.</p> <p>Details of grievance resolution mechanisms should be publicly disseminated, and users should be informed during onboarding. Effective channels that should be made available as options to users are a toll-free number, website or email address, or if the system provides users with a mobile application, app based.</p>	To help individuals seek easy redress against any aspect of the identity management (enrollment, authentication failure, biometric mismatch, identity theft, data misuse, etc).

# ANNEXURE 1: AFI MEMBER COUNTRY DIGITAL ID AND E-KYC POLICY PRACTICES

COUNTRY	REPORTED POLICY
BANGLADESH	<p>AML/CFT: <a href="#">(Link)</a></p> <p>e-KYC guidelines: <a href="#">(Link)</a></p> <p>Data protection: Digital Security Act, 2018 <a href="#">(Link)</a></p>
BCEAO	<p>Directive n° 02/2015/CM/UEMOA relative à la lutte contre le blanchiment des capitaux et le financement du terrorisme dans les Etats membres de l'UEMOA <a href="#">(Link)</a></p> <p>CEDEAO : Acte additionnel A/SA.1/01/10 du 16 février 2010 relatif à la protection des données à caractère personnel <a href="#">(Link)</a></p> <p>CEDEAO : Directive C/DIR/1/08111 portant lutte contre la cybercriminalité dans l'espace de la CEDEAO <a href="#">(Link)</a></p>
EL SALVADOR	<p>El Salvador is on the way to build Digital ID, by establishing a preliminary draft of the "SPECIAL LAW FOR THE PREVENTION, CONTROL AND PENALTY OF MONEY LAUNDERING. <a href="#">(Link)</a></p>
GHANA	<p>National Identification Authority Act, 2006 (Act 707), National Identity Register (Amendment) Act 2017 (Act 750)</p> <p>Anti-Money Laundering Act, 2020 (Act 1044)</p> <p>AML/CFT Guidelines for banks and Non-bank Financial Institutions in Ghana, July 2018.</p> <p>Data Protection Act, 2012 (Act 843)</p> <p>Cybersecurity Act, 2020 (Act 1038)</p> <p>Payment Systems and Services Act, 2019 (Act 987)</p> <p>Electronic Transactions Act, 2008 (Act 772)</p>
INDIA	<p>AML/CFT: Master Circular on Know Your Customer (KYC) norms/Anti-Money Laundering (AML) standards/Combating of Financing of Terrorism (CFT)/Obligation of banks under Prevention of Money Laundering Act, (PMLA), 2002 <a href="#">(Link)</a></p> <p>Digital ID: The Aadhaar and Other Laws (Amendment),2019 <a href="#">(Link)</a></p> <p>Data Protection:</p>
MADAGASCAR	<p>AML/CFT: <a href="#">(Link)</a></p> <p>Data protection: Loi n° 2014-038 sur la protection des données à caractère personnel <a href="#">(Link)</a>, An independent data protection authority is established (Commission Malagasy de l'informatique et des libertés ). It is responsible for ensuring that the treatments of personal data are implemented following the provisions of the law.</p> <p>Cyber Security: <a href="#">(Link)</a></p>
MEXICO	<p>Digital identity: Legal framework of the National Registry of Population and Identity) <a href="#">(Link)</a></p> <p>AML/CFT: Article 15 of the credit institutions law <a href="#">(Link)</a></p> <p>Data protection and privacy: Federal Law on the protection of personal data in possession of individuals <a href="#">(Link)</a></p> <p>Cyber Security: General provisions on information security for credit institutions <a href="#">(Link)</a></p>
NAMIBIA	<p>AML/CFT: Financial Intelligence Act, 2012 <a href="#">(Link)</a></p>

COUNTRY	REPORTED POLICY
<b>NIGERIA</b>	<p>AML/CFT Regulations (Amendment Regulation 2019) (<a href="#">Link</a>)</p> <p>Nigeria Data Protection Regulation 2019 (<a href="#">Link</a>)</p> <p>CyberCrimes (Prohibition and Prevention Act) (<a href="#">Link</a>)</p> <p>National Identity Management Commission Act 2007 (<a href="#">Link</a>)</p>
<b>PERU</b>	<p>Digital ID: Supreme Decree N° 029-20221-PCM, Legislative Decree that approves the Digital Government Law (<a href="#">Link</a>) – Spanish</p> <p>Data protection: Law N° 29733 and its Regulation - regulates adequate treatment of data, both by public and private entities (<a href="#">Link</a>)</p> <p>Regulation for cybersecurity (<a href="#">Link</a>) – Spanish</p>
<b>PHILIPPINES</b>	<p>AML/CFT: Republic Act No. 9160, otherwise known as the “Anti-Money Laundering Act of 2001 (<a href="#">Link</a>)</p> <p>Digital ID: PhillID - Republic Act No. 11055 (<a href="#">Link</a>), or the Phillipine Identification System Act, signed by President Rodrigo Roa Duterte on 06 August 2018. It is an act establishing a single national identification system that aims to provide valid proof of identity for Filipino citizens and resident aliens of the Philippines.</p> <p>Data protection: Data Privacy act - Republic Act No. 10173 (<a href="#">Link</a>)</p> <p>Cybersecurity: Cyber Crime Prevention Act of 2012 - Republic Act No. 10175 (<a href="#">Link</a>)</p>
<b>RUSSIA</b>	<p>Data protection and privacy: Federal Law on Personal Data, 2006 (<a href="#">Link</a>)</p> <p>AML/CFT: (<a href="#">Link</a>)</p> <p>Digital ID: Resolution of the Government of the Russian Federation No. 710, 2019 (<a href="#">Link</a>)</p>
<b>SENEGAL</b>	<p>Sénégal : Loi n° 2008-12 du 25 janvier 2008 portant sur la Protection des données à caractère personnel (<a href="#">Link</a>)</p> <p>Sénégal : Loi n° 2008-11 du 25 janvier 2008 portant sur la Cybercriminalité (<a href="#">Link</a>)</p>
<b>SINGAPORE</b>	<p>AML/CFT: Guidelines on prevention of money laundering and countering the finance of terrorism (<a href="#">Link</a>)</p> <p>Digital Identity: (<a href="#">Link</a>)</p> <p>Data Protection Act, 2012 (<a href="#">Link</a>)</p>
<b>ZAMBIA</b>	<p>AML/CFT: The Financial Intelligence Centre Act of 2016 (<a href="#">Link</a>)</p> <p>Data protection: The Data Protection Act, 2021 (<a href="#">Link</a>)</p> <p>Cybersecurity: The Cyber Security and Cyber Crimes Bill (<a href="#">Link</a>)</p>



## ANNEXURE 2: REFERENCES

**1. World Bank. 2019.** ID4D Practitioner's Guide: Version 1.0 (October 2019). Washington, DC: World Bank. Available at: <http://documents1.worldbank.org/curated/en/248371559325561562/pdf/ID4D-Practitioner-s-Guide.pdf>

**2. World Bank. 2018.** ID4D Practitioner's Note. Catalog of Technical Standards for Digital Identification Systems. Washington, DC: International Bank for Reconstruction and Development / The World Bank. Available at: <https://olc.worldbank.org/system/files/129743-WP-PUBLIC-ID4D-Catalog-of-Technical-Standards.pdf>

**3. The Centre for Internet and Society. 2020.** Governing ID: Principles for Evaluation. Available at: [https://digitalid.design/docs/CIS\\_DigitalID\\_EvaluationFrameworkDraft02\\_2020.01.pdf](https://digitalid.design/docs/CIS_DigitalID_EvaluationFrameworkDraft02_2020.01.pdf)

**4. Alliance for Financial Inclusion. 2021.** "Four policies to promote inclusive financial integrity in 2021". Available at: <https://www.afi-global.org/newsroom/blogs/four-policies-to-promote-inclusive-financial-integrity-in-2021/>

**5. Alliance for Financial Inclusion. 2019.** KYC Innovations, Financial Inclusion and Integrity. Available at: [https://www.afi-global.org/wp-content/uploads/publications/2019-03/KYC-Innovations-Financial-Inclusion-Integrity-Selected-AFI-Member-Countries\\_0.pdf](https://www.afi-global.org/wp-content/uploads/publications/2019-03/KYC-Innovations-Financial-Inclusion-Integrity-Selected-AFI-Member-Countries_0.pdf)

**6. Alliance for Financial Inclusion. 2020.** Inclusive Financial Integrity: A Toolkit for Policymakers. Available at: [https://www.afi-global.org/sites/default/files/publications/2020-07/AFI\\_CENFRI\\_toolkit\\_AW\\_digital.pdf](https://www.afi-global.org/sites/default/files/publications/2020-07/AFI_CENFRI_toolkit_AW_digital.pdf)

**7. Alliance for Financial Inclusion. 2021.** Guideline Note on Data Privacy for Digital Financial Services. Available at: [https://www.afi-global.org/wp-content/uploads/2021/02/AFI\\_GN43\\_AW3\\_digital.pdf](https://www.afi-global.org/wp-content/uploads/2021/02/AFI_GN43_AW3_digital.pdf)

**8. FATF. 2020.** Guidance on Digital Identity. FATF, Paris. Available at: <http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/Guidance-on-Digital-Identity-report.pdf>

**9. World Bank. 2018.** G20 Digital Identity Onboarding. Available at [https://www.gpfi.org/sites/gpfi/files/documents/G20\\_Digital\\_Identity\\_Onboarding.pdf](https://www.gpfi.org/sites/gpfi/files/documents/G20_Digital_Identity_Onboarding.pdf)

**Alliance for Financial Inclusion**

AFI, Sasana Kijang, 2, Jalan Dato' Onn, 50480 Kuala Lumpur, Malaysia  
t +60 3 2776 9000 e info@afi-global.org [www.afi-global.org](http://www.afi-global.org)

 Alliance for Financial Inclusion  AFI.History  @NewsAFI  @afinetwork