Arab Regional Fintech Working Group

Digital Identity and e-KYC Guidelines for the Arab Countries

No.
136
2020

صندوق النقد العربي
ARAB MONETARY FUND

أمانة مجلس محافظي المصارف المركزية ومؤسسات النقد العربية

مجلس محافظي المصارف المركزية ومؤسسات النقد العربية
COUNCIL OF ARAB CENTRAL BANKS AND MONETARY AUTHORITIES GOVERNORS

صندوق النقد العربي
ARAB MONETARY FUND

Arab Regional Fintech Working Group

Digital Identity and e-KYC Guidelines for the Arab Region

Arab Monetary Fund
2020

ACKNOWLEDGEMENT

This guidelines document was produced within the Arab Regional Fintech Working Group (WG) mandate, which implies the exchange of knowledge and expertise, strengthening the capacity-building of the Arab regulators, as well as building a network of peer to peer between Arab and international experts from the public and private sectors to promote Fintech industry and the development of innovation. The WG has a comprehensive structure from the different Fintech industry stakeholders, within the Arab region and worldwide, to enhance establishing a proper Fintech ecosystem in the Arab region.

This document was produced by drawing from resources and information channeled by regulatory and supervisory authorities in Arab countries, namely Central Banks, Capital Market Authorities, and Financial Intelligence Units, whose exerted significant effort in responding to the survey conducted from September through November 2019.

The Digital Identity and e-KYC Guidelines in the Arab Region was prepared by Kokila Alagh and Soumya George from KARM Legal Consultants, member of MENA Fintech Association, in collaboration with Nouran Youssef from the Arab Monetary Fund. Moreover, the document has benefited from valuable review, comments and suggestions provided by Harish Natarajan from the World Bank as well as Nadine Chéhade and Policy team from CGAP-WB.

Any queries regarding this report should be addressed to:

Nouran Youssef, DBA

Senior Financial Sector Specialist, Arab Monetary Fund

Economic Department, Financial Sector Development Division

Corniche Street, P.O Box 2818, Abu Dhabi, United Arab Emirates

Tel. +971 2617 1454

E-mail: Economic@amfad.org.ae; FSD@amfad.org.ae,
FintechWG@amf.org.ae; nouran.youssef@amf.org.ae;

Website: www.amf.org.ae

For the document:

Table of Contents

ABBREVIATIONS & KEY DEFINED TERMS

ABBREVIATIONS

ADB	Asian Development Bank
AML	Anti-Money Laundering
ANSI	American National Standard Institute
Basel Committee	Basel Committee on Banking Supervision
BIS	Bureau of Indian Standards
BMGF	Bill and Melinda Gates Foundation
CBCG	Correspondent Banking Coordination Group
CDD	Customer Due-Diligence
CERSAI	Central Registry of Securitization Asset Reconstruction and Security Interest of India
CFT	Counter-Financing of Terrorism
CGAP	Consultative Group to Assist the Poor
CGD	Center for Global Development
CITeR	Center for Identification Technology Research
CNIC	Computerized National Identity Card
DDoS	Distributed denial-of-service
DFS	Digital Financial Services
DFSPs	Digital Financial Service Providers
DIAL	Digital Impact Alliance
Digital ID	Digital Identity
DIN	German Institute of Standardization
Draft FATF Guidance	Draft Guidance on Digital Identity
ECA	United Nations Economic Commission for Africa
e-KYC	Electronic Know Your Customer

FATF	Financial Action Task Force
FDPs	Forcibly Displaced Persons
FI	Financial Institutions
FIU	Financial Intelligence Unit
FSB	The Financial Stability Board
FSPs	Financial Service Providers
GDP	Gross Domestic Product
GDPR	General Data Protection Regulation
GLEIF	Global Legal Entity Identifier Foundation
GPFI	Global Partnership for Financial Inclusion
GSMA	Global System for Mobile communications Association
IBIA	International Biometrics and Identification Association
ID	Identification
ID4D	Identification for Development
IEC	International Electrotechnical Commission
IOM	International Organization for Migration
ISO	International Organization for Standardization
ITU	International Telecommunication Union
ITU-T	ITU's Telecommunication Standardization Sector
KYC	Know Your Customer
LEI	Legal Entity Identifier
MFA	Multi-Factor Authentication
ML	Money Laundering
MSMEs	Micro Small and Medium-sized enterprises

NADRA	National Database and Registration Authority
NGO	Non-Governmental Organizations
NIST	United States National Institute of Standards and Technology
ODIHR	OSCE Office for Democratic Institutions and Human Rights
OTP	One Time Password
OSCE	Organization for Security and Co-operation
PIN	Personal Identification Number
PSA	Pakistani Standards Authority
SIA	Secure Identity Alliance
SIM	Subscriber Identification Module
SMEs	Small and Medium-sized Enterprises
SMS	Short Message Service
UIDAI	Unique Identification Authority of India
UN	United Nations
UNDP	United Nations Development Programme
UNICEF	The United Nations International Children's Emergency Fund
UN SDG	United Nations Sustainable Development Goals

KEY DEFINITIONS

These definitions are based on the definitions used by World Bank in its paper and the Draft FATF Guidance.

"Assurance Levels" or "Levels of Assurance"	Refers to the level of trustworthiness, or confidence in the reliability of each of the three stages of the Digital ID process
"Attributes"	A named quality or characteristic inherent in or ascribed to someone or something. In identification systems, common personal identity attributes include name, age, sex, place of birth, address, fingerprints, a photo, a signature, an identity number, date and place of registration, etc
"Authentication"	Something that establishes that the claimant (customer) who asserts his or her identity to obtain access to the customer's account is the same person whose identity was obtained, verified, and credentialed during on-boarding.
"Authenticator"	Something the claimant possesses and controls that is used to authenticate (confirm) that the claimant is the individual to whom a credential was issued, and therefore (depending on the strength of the authentication component of the digital identity system) is (to varying degrees of likelihood, specified by the authentication assurance level) the actual subscriber and account holder
"Digital ID"	A set of electronically captured and stored attributes and/or credentials that uniquely identify a person
"Digital ID system"	Systems that cover the process of identity proofing/enrolment and authentication. Identity proofing and enrolment can be either digital or physical (documentary), or a combination thereof.
"Identity"	A set of attributes that uniquely identify a person.
"Identification"	The process of establishing, determining, or recognizing a person's identity.
"Interoperability"	Means that an individual's digital identity credentials can be used to prove official identity for new customer relationships at unrelated private sector or government entities, without their having to obtain and verify personally identifiable information (PII) and conduct customer identification/verification each time
"Verification"	Means the part of identity proofing and involves confirming that the validated identity relates to the individual (applicant) being identity-proofed

EXECUTIVE SUMMARY

Presently, an estimated one billion people globally do not have access to an officially recognizable identity and most of these people reside in developing economies. Absence of a trustworthy identification acts as one of the biggest barriers in accessing a wide range of socio-political and economic rights and is a roadblock in achieving the financial inclusion goals. Further, with most transactions moving digital, legacy identification systems (based on physical documents and processes) themselves become a limitation. Technology provides opportunities to reconsider existing systems and build the infrastructure necessary to balance market integrity, financial inclusion and economic growth, while also meeting international financial standards like the UN SDG Goals and FATF recommendations. Financial services can leverage Digital ID systems to increase efficiency, enhance effectiveness and identify new ways of providing services to customers. The analysis is supported by the 'G20 High-Level Principles of Digital Financial Inclusion' and the 'Principles on Identification for Sustainable Development' developed by the World Bank Group.

Digital Identity is a "*compilation of electronically captured and stored attributes of a uniquely identifiable persona that can be linked to a physical person*." The attributes can be divided into various categories including birth related information (place of birth, date of birth *etc*), descriptive information (height, weight, physical traits *etc*), personal identifiers (like social security number) and biometric data (fingerprint, DNA, iris scan *etc*). Identity systems may fall into one of the two major categories: ***foundational*** (created for general public administration and identification) or ***functional*** (created in response to a demand for a particular service or transaction). Specifically, in the case of financial services, irrespective of the nature of identity used as a reliable source of identification, it is necessary that the identity system is legal, unique and digital.

The FATF Draft Guidance on Digital Identity (November 2019) identified that to be considered a 'Digital Identity' certain components of the identity lifecycle would have to be mandatorily digital. The lifecycle of identity systems includes three major components:

TABLE 1- Digital ID Components

Component One: Identity proofing and enrolment (with initial binding/credentialing)	Process involves collecting, validating and verifying the identity information of an individual, enrolling the individual with an identity account and connecting (or binding) the individual's unique identity to authenticators possessed and controlled by this person	Mandatorily Digital
Component Two: Authentication	Establishes that the claimant is the same person who has been identity proofed, enrolled, and credentialed (e.g., is the on-boarded customer). Authentication itself could be undertaken utilizing attributes which the person either 'has', 'knows' or 'is'.	Mandatorily Digital
Component Three: Portable Identity	Means that an individual's Digital ID credentials can be used to prove official identity for new customer relationships, without their having to obtain and verify	Optional

	personally identifiable information and conduct customer identification and verification each time	

Though Digital ID can pave way to eliminate financial exclusion and have a wide range of benefits, it also brings to fore a set of new risks, which are solely related to the technology being used including risks from cybersecurity and data theft. In the light of the risks associated with identity theft, the importance of technical standards and frameworks cannot be harped upon. The FATF Recommendations oblige FIs to conduct CDD using "*reliable*" information. Therefore, a Digital ID system which complies with the required assurance levels and interoperability standards should be deemed to be a contingent requirement for such information to fulfill the '*reliability'* test. Various international organizations and agencies are involved in developing standards. However, examples like the eIDAS Regulation are a great example for intergovernmental efforts in this respect.

The FATF Recommendations have obligated FIs to adopt a 'risk-based' AML principle while undertaking CDD. The 'risk-based' principle requires assessment of the risks associated with illicit activities (such as money laundering and terrorist financing). To achieve this objective, FIs are required to implement control measures reasonably deploy corresponding resources to limit or control the effects of such risks, as and when they occur. KYC is an inherent part of the CDD process and may be undertaken through:

- Tiered CDD models (with basic CDD, simplified CDD or enhanced CDD being used based on the risks associated with the CDD); and
- e-KYC models that allow approved entities to query a national identity system to authenticate or verify customers' identities and, in some cases, to retrieve basic attributes about them, which attributes may be stored electronically or digitally.

Developments in technology have brought about various technology solutions, often referred to as '*KYC utilities*' which act as a single repository of customer identity data which is utilized for facilitating easier KYC process. By pooling resources, reducing duplicative efforts, and digitizing processes through KYC utilities, FSPs can shorten the time required for identity checks and verification, reduce CDD compliance costs and potentially improve the quality and reliability of customer data. Governments, may either develop such technologies and repositories themselves or consider the use of specialized private sector players as well as the co-operation of financial service providers for developing such a central repository.

With the intention of understanding the development of Digital ID and e-KYC programmes among the Arab countries, a questionnaire was circulated to the Central Banks of the Arab Countries. Based on the findings of the survey, it is noted that Digital ID system are still in nascent stages, though there are systems in most countries for a government issued national identity system. Most countries are still following physical KYC structure with face-to-face interactions (or equivalent) and physical documents being the basis for client on-boarding and verification models. Bahrain and UAE appear to be the frontrunners in the implementation of an e-KYC model. Based on the findings of the survey, a **range of action items have been proposed to Arab Countries:**

- Establishment of a unique, legal, interoperable, Digital ID with an 'identity first' focus that collects minimal information for creation of an identity
- Support the Digital ID framework by adoption of policies, rules and regulations addressing the risks or concerns associated with the use of Digital ID
- Establish a 'risk-based' CDD regime which balances between the AML/CFT objective and financial inclusion objectives
- Prioritize integrity of user data and facilitate processes and procedures for minimalistic sharing of the information during CDD
- Create benchmarks and standards for use of any 'non-government' backed identity systems
- Ensure complete, accurate and better integrated databases that can be utilized for customer identification and verification purposes
- Implement a strong governance model to manage the Digital ID and CDD regime
- Provide regulatory clarity, remove barriers and foster enabling regulatory environment for innovation which may provide newer solutions for CDD.
- Collaborate with regional and international bodies and regulators
- Formulate transnational frameworks for interoperability and levels of assurance being implemented across Arab countries.

This report is divided into four broad sections.

- The first section reviews the role and need for Digital ID : This section focusses on the importance thereof along with the principles, the international developments, characteristics, technological requirements, levels of assurance, benefits and risks of Digital ID.
- In the second section, the paper studies the need to have a reliable identity system for the purposes of conducting CDD. This section discusses how on the benefits of utilizing KYC utilities for the purposes of conducting CDD. The significance of 'risk-based' AML and a tiered CDD structure is discussed in depth.
- The third section evaluates the developments surrounding Digital ID in India, Estonia and Nigeria.
- The final section gauges the developments surrounding Digital ID and e-KYC among the Arab countries based on the findings of the survey.

The process of showcasing the fundamentals of Digital ID, lessons learnt from previous experience globally and the developments locally has helped the authors identify specific action items for the Arab nations to consider and adopt.

1. Introduction

Traditionally, identification of a person is based on physical interactions and/or through identification systems followed by the government of the country. An identity system enables a person to prove that '*you are who you say you are*' and this ability is fundamental for their active participation in political, social and economic life.

It is estimated that approximately one billion people globally do not have access to an officially recognizable identity and most of these people reside in developing economies.[1] In the absence of a trustworthy identification mechanism, an individual may be unable to exercise or access the range of human rights or basic entitlements available to them under national and international laws. Lack of an acceptable identity is of concern for marginalized individuals, which includes displaced or stateless people and other vulnerable groups. Even in case that person provides an identification document, it is pertinent that adequate processes are adopted or followed to minimise the risk of false identification. The relevance of such processes and procedures, whether manual or digital, cannot be disregarded in case of financial services.

The primary responsibility to implement the registration and recognition of legal identity is vested with national governments[2]. Globally, regulators recognise that an implementation of a unified, legal, Digital ID would be a 'game-changer' in achieving the financial inclusion objective.

2. Importance of Digital Identity

Identity is a fundamental requirement for most transactions that occur today. Legacy systems utilised identity systems based on physical documents or processes. Physical identity systems were structured for face-to-face transactions. Some of the inherent characteristics of physical identity systems end up acting as a limitation of their use in the digital world. The major characteristics of physical identity documents are as follows[3]:

- *Document based* – It effectively depends on access or possession to the physical documents like passport, driver's license and similar identity documents, even if such documents may not have to be submitted in originals. A proof of identity that is based on possession of physical document may not require demonstration of a link between an individual and the documents, enabling use of an entity's credentials by a different user.

[1] Vyjayanti Desai. Anna Diofasi, Jing Lu, "*The global identification challenge: Who are the 1 billion people without proof of identity?*" (World Bank, April 2018) available at https://blogs.worldbank.org/voices/global-identification-challenge-who-are-1-billion-people-without-proof-identity accessed on October 20, 2019. Also, refer to the World Bank Group's Identification for Development (ID4D) initiative, "*The Global ID4D Dataset*" last updated June 25, 2018 available at https://datacatalog.worldbank.org/dataset/identification-development-global-dataset accessed on October 20, 2019.

[2] Target 16.9 UN SDG

[3] World Economic Forum, "*A Blueprint for Digital Identity: The role of financial institutions in building Digital Identity"*, (2016) available at http://www3.weforum.org/docs/WEF_A_Blueprint_for_Digital_Identity.pdf , accessed on November 19, 2019.

- *Siloed:* Identity data is held in discrete places that are not interconnected and cannot be aggregated by the entity nor be connected to other applications.
- *Inflexible:* Identity attributes are collected based on the standardized set of information required for a purpose and such information may not be easily adapted.

The inherent features of physical identity systems would act as limitations for their use for conducting CDD on a digital platform. These concerns are effectively resolved through the development of Digital ID systems that store identity attributes uniquely in a digital or electronic system. However, Digital ID systems bring with them a separate set of concerns or risks (some of which are elaborated subsequently in this report). If appropriately designed, managed and governed in compliance with national and international standards and best practices Digital ID acts as an efficient and effective system capable of handling complex transactions and increased volumes.

Technology provides opportunities to reconsider existing systems and build the infrastructure necessary to balance market integrity, financial inclusion and economic growth, while also meeting international financial standards, including the Basel Committee, FATF, the FSB and the UN SDG. These aspects are discussed below.

2.1 Preservation and maintenance of Market Integrity

In the digital world, guaranteeing that transactions are undertaken in safe and secure manner is one of the biggest challenges. Customer identification along with anti-money laundering and counterterrorism financing are the cornerstones of ensuring integrity and fairness in the markets. From a risk management perspective performing and verifying customer identity and conducting CDD both at the time of customer on-boarding and on an ongoing basis, are fundamental components for maintaining market integrity.

From a business standpoint, knowledge of the identity of the client is indispensable for the financial providers since it equips them in shielding themselves against fraud and crime. An identity system goes a long way towards providing the services based on the customer's needs, often assisting the FSP in:

(a) satisfying the client's financial needs; and
(b) verifying the suitability of financial product for a client.

A Digital ID system is most beneficial for the users permitting them to undertake most transactions without being physically present, wherever so allowed by law.

However, to build trust in a Digital ID system, it is vital that the data collected from the users is protected. The design of the system must embed the principles of confidentiality and integrity of data and the system. The Digital ID system must have an in-built governance model and ensure that the use of the data is in compliance with confidentiality and integrity principles. The sanctity and accuracy of the data – which is confirmed through a thorough verification and due-diligence

aids in increasing the confidence and trust in the system and reduces the likelihood of any criminal or terrorist abuse

2.2 The balancing the objectives of financial inclusion and economic growth.

The uptake of mobile phones and access to the internet is a key enabler in achieving financial inclusion The core objective of e-KYC is to make opening of account easy and cost-effective for individuals and SMEs, and allow resources to be focused on high-risk customers to support financial inclusion. For instance, as per the 2018 '*State of Aadhaar's'* report, in India, since the implementation Aadhaar, 84% people have used Aadhaar as a proof of identity to open bank accounts.[4]

The availability of a reliable, digitally authenticated identity system can strongly support financial competitiveness. Some of the key aspects of a Digital ID that may facilitate financial competitiveness is:

- Biometrics-linked Digital ID may make it easier for the unbanked to obtain financial accounts by simplifying the documentation requirements required at account opening;
- It may help the FIs to comply with the customer identification and verification components of CDD.
- It may also provide more cost-effective ways of onboarding new customers, which could potentially be conducted by agents. Agents can use Digital ID to reliably record customer's identity and proof of validation which can be verified and used to feed the information from the Digital ID system for the required CDD checks.

TABLE 2- Biometric Identification

Biometric Identification
Digital biometric identification involves comparing a template generated from a live biometric sample to a previously stored biometric in order to determine the probability that they are a match. For example, a fingerprint biometric is a representation of multiple points on the fingerprint, and the relative positions of those points. A biometric comprising 20 or more points would be viewed as good quality, whereas one with just four or five would be viewed as inadequate. It is hence a profile creation and similar patterns can be created for different persons, leading to false positive
One-to-one (1:1) matching is a comparison against a single template and is typically used for authentication and verification. One to-many (1:N) matching is a comparison against all or a subset of templates stored in a database, and can be used for identification (e.g., a criminal record search) or deduplication (i.e., ensuring that each individual exists only once in the database). In principle, 1:N deduplication allows identity providers to establish statistical uniqueness in a population. However, biometrics do pose certain concerns. Firstly, to undertake 1:N matching, a national database of biometrics is a pre-requisite. Also, physical factors, personal and cultural sensitivities can also affect the usability of some biometrics. Nonetheless, once identification is complete, biometrics may be extremely useful for authentication process, which follows 1:1 matching.

[4] Ronald Abraham, et al, "*State of Aadhaar Report 2016-2017*", (May 2017) available at https://static1.squarespace.com/static/5b7cc54eec4eb7d25f7af2be/t/5bc5357e652dea4073286a35/1539650996433/State-of-Aadhaar-Ch3-Legal.pdf , accessed on November 19, 2019.

2.3 Compliance with international financial standards, i.e. UN SDG, the Basel Committee, FATF and FSB.

Financial technology and in particular "regulatory technology" present opportunities to reconsider existing systems and to build the necessary infrastructure to balance market integrity, financial inclusion, and economic growth, while at the same time meeting commitments to international financial standards including those set by the FATF, Basel Committee, FSB and the UN. These institutions and regulatory bodies recognize that high levels of financial exclusion are a threat to the financial integrity of economies.

The expansion of identity programs is a specific target of the UN Sustainable Development Goals, calling for UN Member States to "*provide legal identity for all, including birth registration*" by 2030.[5] The World Bank's ID4D program is also playing a leading role in global efforts to stimulate the introduction of reliable, unique identity. The ID4D program recognizes that identity document is key to the pursuit of development goals across a wide range of sectors, with healthcare, education and financial services among the best-known examples.

CDD is most closely associated with the fight against money-laundering, which is essentially the province of the FATF. The mandate of the FATF is to set standards and to promote effective implementation of legal, regulatory and operational measures for combating money laundering and terrorist financing and other related threats to the integrity of the international financial system.[6]

FATF Recommendation on CDD (Recommendation 10) is the most comprehensive and elaborate among the 40 Recommendations. It is based on four pillars, requiring:

- identification and verification of customers,
- identification and verification of beneficial owners,
- understanding the nature and purpose of transactions,
- monitoring the clients and their transactions on an ongoing basis.[7]

Recommendation 10 of FATF Recommendation has highlighted that the "*principle that financial institutions should conduct CDD should be set out in law."* Countries have been granted the choice to determine the means of enforcement . Furthermore, Recommendation 10(a) of the FATF Recommendations noted the significance of using a "*reliable, independent source documents, data or information*" to identify customers and verify the customer identity.

---

[5] UN, "*Transforming our world: the 2030 Agenda for Sustainable Development",* (2015). Available at https://sustainabledevelopment.un.org/post2015/transformingourworld, accessed on November 17, 2019.
[6] FATF, "*International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation",* (FATF, Paris, France in 2012-2019) available at https://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%202012.pdf accessed on November 11, 2019.
[7] Ibid

More recently, FATF has concluded a public consultation on Draft FATF Guidance which explains the manner in which Digital ID systems can be used to conduct CDD and ongoing due diligence. The Draft FATF Guidance provides guidance notes to assist governments, regulated entities and other relevant stakeholders in applying a risk-based approach to the use of Digital ID for CDD.[8]

The Basel Committee strongly supports the adoption and implementation of the FATF recommendations, particularly those relating to banks. It maintains that sound KYC procedures must be viewed as a critical element in the effective management of banking risks. In accordance with Basel Committee's Core Principles for Effective Banking Supervision (2012), all banks are required to "*have adequate policies and processes, including strict customer due diligence (CDD) rules to promote high ethical and professional standards in the banking sector and prevent the bank from being used, intentionally or unintentionally, for criminal activities*"[9]. The afore-mentioned mandate is to be deemed as a part of banks' general obligation to have sound risk management programmes required to be in place to address all kinds of risks, including risks associated with money laundering and financing terrorism. Banks are expected to integrate into their overall risk management structure appropriate steps to identify, assess, monitor, manage and mitigate risks of money laundering and the financing of terrorism with respect to customers, countries and regions, as well as to products, services, transactions and delivery channels on an ongoing basis.

FSB was established to coordinate at the international level, the work of national financial authorities and international standard-setting bodies in order to develop and promote the implementation of effective regulatory, supervisory and other financial sector policies. In 2015, a World Bank survey commissioned by the FSB noted that almost half of the emerging market and developing economies surveyed have experienced a decline in correspondent banking services due to concerns about money laundering and terrorism financing risks in affected jurisdictions, overall risk appetite and lack of profitability. In furtherance thereof, in November 2015, the FSB launched a four-point action plan[10] to assess and address the decline in correspondent banking relationships, coordinated by the CBCG[11]. One of the four areas of the action plan include "*clarifying regulatory expectations, as a matter of priority, including through guidance by the Financial Action Task Force (FATF) and the Basel Committee on Banking Supervision (BCBS)"*[12], thus reiterating the importance of key objectives surrounding customer due-diligence in banking transactions. This requirement was further stressed in the FSB action

[8] FATF, "*Public consultation on FATF draft guidance on digital identity"* available at https://www.fatf-gafi.org/publications/fatfrecommendations/documents/consultation-digital-id-guidance.html accessed on December 9,2019.
[9] See in particular, BCBS 29 in Core Principles for Effective Banking Supervision, September 2012.
[10] FSB , "*Report to the G20 on actions taken to assess and address the decline in correspondent banking",* 2015 available at https://www.fsb.org/2015/11/report-to-the-g20-on-actions-taken-to-assess-and-address-the-decline-in-correspondent-banking/ accessed on November 12, 2019.
[11] The CBCG's membership comprises senior representatives from international organizations and standard setters and national authorities in the FSB and its Regional Consultative Groups.
[12] The other action items include: (a) examining the dimensions and implications of the issue; (b) Domestic capacity-building in jurisdictions that are home to affected respondent banks; and (c) Strengthening tools for due diligence by correspondent banks.

plan released in May 2019[13], wherein it was suggested that technical solutions such as KYC Utilities may be relied upon for the purposes of undertaking CDD.

3. Governing Principles – The Principles on Identification for Sustainable Development & G-20 High Level Principles for Digital Financial Inclusion

3.1 The Principles on Identification for Sustainable Development

Given the critical role of identification for development, the UN Member States have adopted UN SDG *"to provide legal identity for all, including birth registration* by 2030[14]. These principles are derived from and reinforced by international practice and are extensively agreed upon at international and national levels. To reinforce the Target 16.9 of the UN SDG, eminent international organizations[15] endorsed certain 'shared principles' to recognize strong identification systems to support development and the achievement of the Sustainable Development Goals. The shared common principles[16] are fundamental in maximizing the benefits of identification systems for sustainable development while mitigating risks.

TABLE 3- Inclusion Principle – Identification for Sustainable Development

Principle 1: Inclusion: Universal Coverage and Accessibility	
Ensuring universal coverage for individuals from birth to death, free from discrimination.	**Removing barriers to access and usage and disparities in the availability of information and technology.**

Countries are required to afford all its 'residents' the opportunity to procure a legal identity for themselves in accordance with the principles set out in international law and their own legislative frameworks.[17] The primary pre-requisite for ensuring that this principle is adequately achieved would include the commitment by countries to universal birth registration for all individuals born on national territory – being adopted or implemented without any discrimination. This right should be universal without any limitation to the citizens of a nation.[18]

---

[13] FSB, "*FSB Action Plan to Assess and Address the Decline in Correspondent Banking: Progress Report*" , May 2019 at https://www.fsb.org/wp-content/uploads/P290519-1.pdf accessed on December 22, 2019

[14] Target 16.9, UN SDG

15 Endorsing organizations include ADB, BMGF, CGD, DIAL, IOM, Mastercard, OSCE ODIHR, Plan International, SIA, the GSMA, UNHCR, The UN Refugee Agency, UNICEF, UNDP, ECA and the World Bank Group.

[16] UN High Commissioner for Refugees (UNHCR), "*Principles on Identification for Sustainable Development: Toward the Digital Age"*, (February 2017), available at: https://www.refworld.org/docid/59db4aaa4.html accessed 6 November 2019.

[17] States have the sovereign right to determine eligibility for citizenship in accordance with international law. While proof of citizenship will be limited to citizens, States should provide legal identification to all person's resident on their territory, including birth registration. They should also provide proof of citizenship to all persons entitled to it without discrimination of any kind.

[18] For example, Article 7 of the Convention on the Rights of the Child (CRC) states: "*The child shall be registered immediately after birth and shall have the right from birth to a name, the right to acquire a nationality and, as far as possible, the right to know and be cared for by his or her parents*." The CRC has been ratified by every member state of the UN except for the United States, which has signed but not ratified the treaty.

The identification framework which surpasses the various barriers during the enrolment and use thereafter would be a key component for the achieving financial inclusion objectives. There are many different barriers to the adoption of identity systems, for example:

- Socio-cultural barriers such as the culture of distrust, the loss of anonymity, religious or cultural practices hindering the collection of data;
- potential economic barriers such as increased transaction costs or the high investment costs associated;
- technical barriers such as the information technology disparities, existing proprietary standards, the lack of interoperability, inherent drawbacks of the technology itself (example would be concerns surrounding biometric accuracy) and the legacy problems.
- organizational & procedural barriers such as the lack of internal capacity of some government departments,
- legal barriers such as the multiplication of legal requirements, of corporate ID policies, and of national laws impacting identity

The identification system would have to be designed with special attention to each of the above barriers. It would have to be ensured that the identity system, would in itself, not act as a tool which results infringement of personal or community rights.

Access to civil registration or registration of birth and death free of charge should be made available to all, including non-imposition of any direct fees or any indirect costs associated with obtaining identification supporting documents. In a world where most services and amenities are being made available digitally or electronically, the lack of connectivity or a mere preliminary understanding of technology, would also result in denial of identification service. Nations should direct joint efforts to formalize procedures that support the provision of both online and offline infrastructure to provide “last-mile” access and connectivity, particularly for those in remote locations. Countries where a large section of the population has tertiary education also tend to have a population with higher skill levels - confirming that digital literacy cannot be seen separately from traditional literacy at the country level. In other words, individuals with higher levels of education, especially tertiary education or higher, are much more likely to have advanced digital skills.

During the creation of an identity system, special attention is to be given to poverty stricken persons or groups, who may be at risk of exclusion for cultural, political or other reasons (such as women, children, rural populations, ethnic minorities, linguistic and religious groups, migrants, the forcibly displaced, and stateless persons), who may not be able to produce any traditional identity evidence. The Draft FATF Guidance highlights that importance of ‘trusted referees’ in such a scenario. Trusted referees may include notaries, legal guardians, medical professionals, conservators, persons with power of attorney, or some other form of trained and approved or certified individual who may, under national legislations and policies, be authorized to certify the identity of persons.

TABLE 4 - Design Principle – Identification for Sustainable Development

Principle 2: Design: Robust, Secure, Responsive and Sustainable	
Establishing a robust—unique, secure, and accurate—identity.	**Creating a platform that is interoperable and responsive to the needs of various users' responsiveness.**
Using open standards and ensuring vendor and technology neutrality.	**Protecting user privacy and control through system design**
Planning for financial and operational sustainability without compromising accessibility.	

To be treated as a trustworthy identity system, the identity database must act as accurate and up-to-date information that may assist in identification and verification. However, to be used as a source for authentication, the database or identity system should also have adequate safeguards against tampering (alteration or other unauthorized changes to data or credentials), identity theft and other errors. The guidelines provided by the Draft FATF Guidance (discussed below) have provided a framework for determining if a Digital ID system is reliable.

Identification providers should work to ensure that identification and authentication services are flexible, scalable, and meet the needs of individuals, public agencies and private entities. The technological robustness, scalability and interoperability of the system are key to facilitate competition and innovation. Technology neutrality and diversity should be fostered to increase flexibility. A system design that is not fit for any purpose or suitable to meet policy and development objectives should be avoided. The long-term fiscal and operational stability of the system should be considered while planning and developing identification systems.

TABLE 5 - Governance Principle – Identification for Sustainable Development

Principle 3: Governance: Building Trust by Protecting Privacy and User Rights	
Safeguarding data privacy, security, and user rights through a comprehensive legal and regulatory framework	**Establishing clear institutional mandates and accountability**
Enforcing legal and trust frameworks through independent oversight and adjudication of grievances.	

An identity system must be underpinned by legal and regulatory frameworks as well as policies which endorse trust in such system. Stringent rules and procedures targeted at ensuring privacy of end-users, preventing unauthorized access and accountability of the provider are material for improving trust. Individuals should be provided, easy and free access which may allow them to exercise choice and control over their personal data. Member states should be transparent about identity management, develop appropriate resources to raise users' awareness of how their data

will be used, and provide them with tools to manage their privacy. Specifically, clear accountability and transparency around the roles and responsibilities of identity system providers, proper regulatory oversight and a proper mechanism for adjudication of disputes regarding identification and the use of personal data that is not satisfactorily resolved by the providers is a central requirement of any identity system.

3.2 G-20 High Level Principles for Digital Financial Inclusion

The G20 High-Level Principles for Digital Financial Inclusion[19] are a major driving force for the adoption of digital approaches to achieve financial inclusion goals in the G-20 member states. It states: "'*Digital financial inclusion refers broadly to the use of digital financial services to advance financial inclusion. It involves the deployment of digital means to reach financially excluded and underserved populations with a range of formal financial services suited to their needs, delivered responsibly at a cost affordable to customers and sustainable for providers*."[20]

Principle 7 of the G-20 Principles suggests that as a part of its action plan towards digital financial inclusion, countries should "*facilitate access to digital financial services by developing, or encouraging the development of, customer identity systems, products and services that are accessible, affordable, and verifiable and accommodate multiple needs and risk levels for a risk-based approach to customer due diligence."* This principle echoes the need to implement a Digital ID which is "accessible, affordable and verifiable".

4. What is Digital Identity?

Institute of International Finance defines 'Digital Identity' as a "*compilation of electronically captured and stored attributes of a uniquely identifiable persona that can be linked to a physical person*." [21] The definition places heavy reliance on "*attributes*" which may be considered as building blocks of digital identity. Attributes can be divided into various categories including birth related information (place of birth, date of birth *etc*), descriptive information (height, weight, physical traits *etc.*), personal identifiers (like social security number) and biometric data (fingerprint, DNA, iris scan *etc.*)[22].

On the other hand, the Draft FATF Guidance defined Digital ID systems "*as systems that cover the process of identity proofing/enrolment and authentication. Identity proofing and enrolment can be either digital or physical (documentary), or a combination, but binding, credentialing,*

19 These principles rely on the explanation in the 2016 Global Partnership for Financial Inclusion (GPFI) report on "*Global Standard-Setting Bodies Financial Inclusion: The Evolving Landscape*" (GPFI White Paper in March 2016) available at http://www.gpfi.org/sites/gpfi/files/documents/GPFI_WhitePaper_Mar2016.pdf accessed on November 12, 2019.

20 Ibid, 46

21 Institute of International Finance (IIF), "Digital Identity: Key Concepts", (July 2019). Available at https://www.iif.com/Portals/0/Files/content/Regulatory/iif_digital_id_07022019.pdf, accessed on November 12, 2019.

22 International Telecommunication Union, "*Digital Identity Road Map Guide*", (2018) available at https://www.itu.int/en/ITU-D/ICT-Applications/Documents/Guides/Digital_Identity_Roadmap_Guide-2018-E.pdf accessed on November 12, 2019.

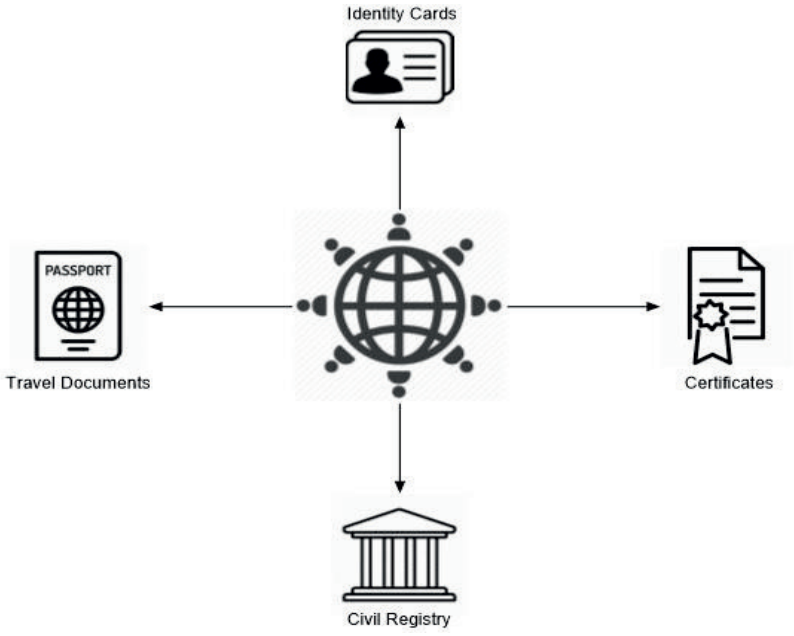
authentication, and portability/federation must be digital." As may be noted from a review of the definition provided by FATF, unlike the definition of Digital ID provided above, the requirement will be surrounding the various stages/ components of the identification process to be digital for an identity system to be considered as a Digital ID.

In any event, all organizations agree that the material requirement of any identity system, including a Digital ID system will be to prove the "*official identity*"[23] of a person.

4.1 Identity System Types: Functional or Foundational?

World Bank has categorized identity systems into two major categories: *foundational* and *functional.* A *foundational* identification system is an identity system created for general public administration and identification—including civil registries, national IDs, and national population registers.[24] They may serve as the basis for a wide variety of public and private transactions, services and derivative identity credentials. These are, hence, mostly official identification documents and typically providers of such identities are national governments who are interested in giving their citizens a means to prove who they are. The foundational identification systems are built in a top-down manner with the objective of bolstering national development by creating a general-purpose identification of persons.

FIGURE 1 - Foundational Identity

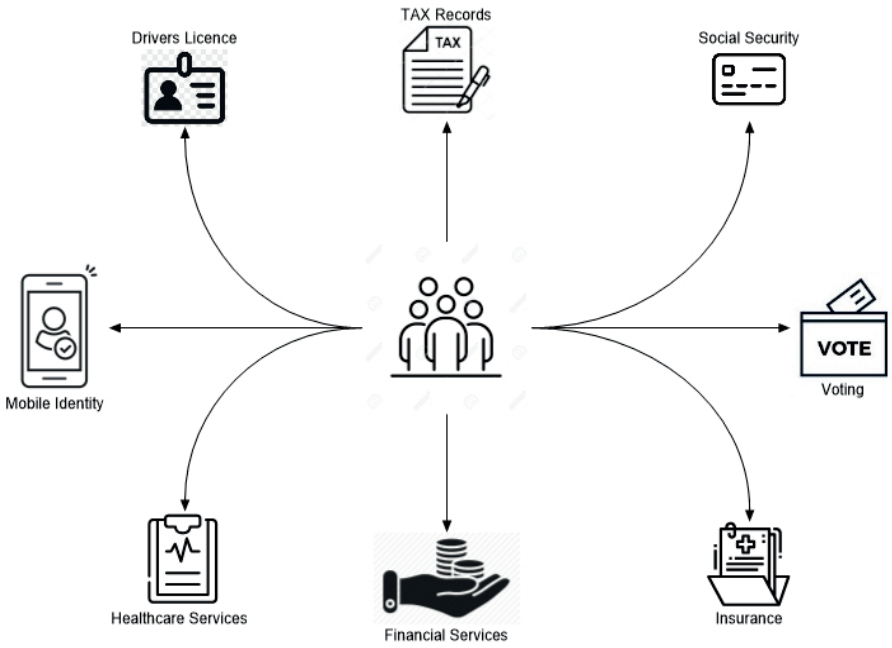


[23] Under FATF, "*Public consultation on FATF draft guidance on digital identity"* available at https://www.fatf-gafi.org/publications/fatfrecommendations/documents/consultation-digital-id-guidance.html accessed on December 9, 2019, "*o**fficial identity"** is defined as the specification of a unique natural person that: (a) is based on characteristics (identifiers or attributes) of the person that establish a person's uniqueness in the population or particular context(s), and (b) is recognized by the state for regulatory and other official purposes*.

[24] World Bank, "*Technology Landscape for Digital Identification",* (Washington, DC: World Bank License: Creative Commons Attribution 3.0 IGO CC BY 3.0 IGO in 2018). available at https://openknowledge.worldbank.org/bitstream/handle/10986/31825/Technology-Landscape-for-Digital-Identification.pdf?sequence=1&isAllowed=y accessed on November 12, 2019.

In contrast, a *functional* identification system is an identity system created in response to a demand for a particular service or transaction[25]. Though created for a specific purpose, such an identity may be commonly accepted for broader identification purposes but may not always bestow legal identity. The providers of these identity documents may be government or non-government players, such as NGOs and private organizations.

FIGURE 2 - Functional Identities



In countries with limited or no foundational systems, functional IDs may evolve to take on a more foundational role.

Most countries in the Arab region have functional identity system. For example, several systems of identification are currently in effect in Lebanon, each managed by the authority that issues it and the related data is held by each authority. Further, customers of banks and FIs who have credit history also have a Digital ID with a unique Number and its related data held by the *Centrale des Risques* (Public Credit Registry) at the *Central Bank of Lebanon* (Banque du Liban)[26]. However, the need for a unified national identity has now been recognized and has been proposed under Law No. 241 dated 22/10/2012 for the use one national identity number to identify all Lebanese citizens in front of public and governmental authorities and entities.

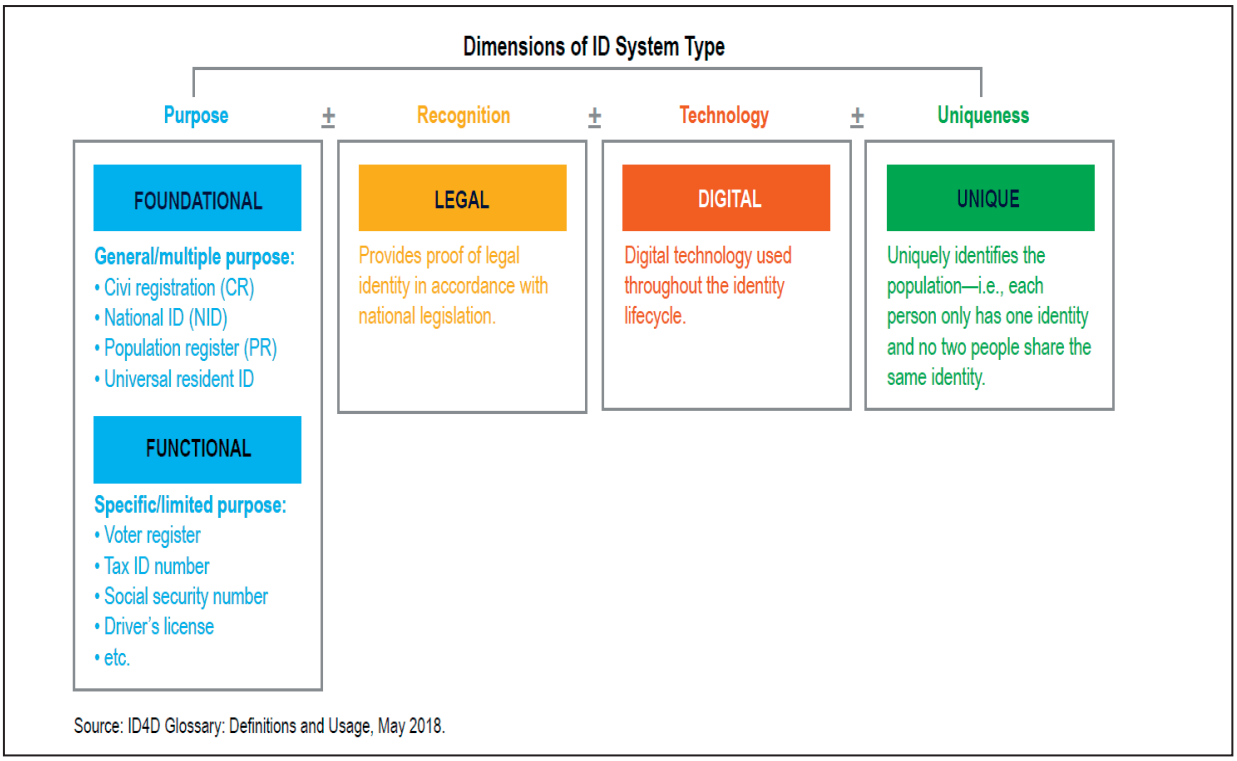
4.2 Dimensions of Digital Identity System

Both *foundational* and *functional* ID systems vary along multiple dimensions, including the technology they use, whether it establishes a unique model and who they cover in the population.

[25] Ibid
[26] Survey response submitted by Banque Du Liban

From a financial services perspective, it is necessary that the identity system is legal, unique and digital. These characteristics are not mutually exclusive, and an identity system can possess one or all of these characteristics to varying degrees.[27]

FIGURE 3 – Dimensions of ID Systems



Source: ID4D Glossary: Definitions and Usage, May 2018.

- **Legal / Official –** An identity is considered legal if it is recognized as providing proof of legal identity[28] in accordance with a national legislation[29]. UN's operational definition of '*Legal Identity*' defines it as "*the basic characteristics of an individual's identity. e.g. name, sex, place and date of birth conferred through registration and the issuance of a certificate by an authorized civil registration authority following the occurrence of birth.*"[30] In the absence of birth registration, legal identity may be conferred by a legally-recognized identification authority. Without any formal recognition as a legal credential, that credential may be unreliable for CDD checks affecting access to certain financial services. Any hindrance in access to the wider financial ecosystem may contribute to financial exclusion.

[27] World Bank Group, *"G20 Digital Identity Onboarding"* (2018), available at https://www.gpfi.org/sites/gpfi/files/documents/G20_Digital_Identity_Onboarding.pdf accessed on November 12,2019

[28] Proof of legal identity is defined as a credential—e.g. birth certificate, identity card or digital identity credential—recognized as proof of identity provided by law. See United Nations, "*UN Legal Identity Agenda*" available at https://unstats.un.org/legal-identity-agenda/ accessed on November 12, 2019.

[29] World Bank Group, "*G20 Digital Identity Onboarding*" (2018), available at https://www.gpfi.org/sites/gpfi/files/documents/G20_Digital_Identity_Onboarding.pdf accessed on November 12, 2019.

[30] United Nations, "*UN Legal Identity Agenda*" available at https://unstats.un.org/legal-identity-agenda/ accessed on November 12, 2019.

- **Uniqueness -** An identity is considered unique if each individual only has one identity and no two people share the same identity[31]. It also proposes that each identity is claimed only by one person[32]. It is important to strive for a unique identity system as it greatly diminishes the chances for fraud while simultaneously boosting efficiency. The availability of a unique Digital ID also has a social grounding - it gives visibility to a large portion of the population that would have been invisible to the system, *i.e*. a tool for social inclusion[33]. A lack of a unique identity essentially prevents the customer activity being reliable and thus impacts their access to the full range of financial services[34]. To be a reliable system, it is necessary that the identity system has identity proofing procedure and systems to prevent duplication.

- **Digital -** An identity is considered to be digital if an individual's attributes can be captured and stored electronically and issued on digital credentials that can identify a person[35]. A Digital ID can provide higher levels of security and facilitate the use thereof by the private sector as a platform for providing other services[36].However, not all segments of an identity system are necessarily digital. In consonance with the position adopted by the NIST Digital ID Guidelines, the Draft FATF Guidance indicates that to be considered as a Digital ID system certain component of the Digital ID lifecycle would essentially have to be undertaken digitally (Refer to Section 4.3 of this report).

Each of the above dimensions impact the sustainability, affordability and reach of the financial services affecting financial inclusion objectives[37]. Absence of legal, unique identity captured across institutions will hamper efforts to gain a proper visibility of customer base, thus limiting the services available to the individual and increasing inefficiencies and costs because all the verifications would have to be performed manually[38].

The provision of the identity may not necessarily be facilitated through a centralized government agency. Digital ID ecosystems at the national level can be loosely categorized into the following types (based on different cultural, legal, and political approaches):

---

[31] Ibid
[32] World Bank Group, "*ID4D Practitioner's Guide*", (October 2019) available at http://documents.worldbank.org/curated/en/248371559325561562/pdf/ID4D-Practitioner-s-Guide.pdf accessed 12 November 2019.
[33] ICAR, "*The unique digital identity will be crucial for worldwide social and economic development"* (2018), available athttps://www.icarvision.com/en/the-unique-digital-identity-will-be-crucial-for-worldwide-social-and-economic-development accessed 28 October 2019.
[34] World Bank Group, "*G20 Digital Identity Onboarding*", (2018), available at http://documents.worldbank.org/curated/en/362991536649062411/pdf/129861WP-10-9-2018-17-26-21-GDigitalIdentityOnboardingReportlowres.pdf accessed 28 October 2019.
[35] Ibid
[36] International Telecommunications Union, "*Unique, Legal and Digital: Three Characteristics Of ID Crucial To Financial Inclusion"* (2019), available at https://news.itu.int/unique-legal-digital-id-financial-inclusion/ accessed 28 October 2019.
[37] World Bank Group, "*G20 Digital Identity Onboarding*" (2018), available at http://documents.worldbank.org/curated/en/362991536649062411/pdf/129861WP-10-9-2018-17-26-21-GDigitalIdentityOnboardingReportlowres.pdf accessed 28 October 2019
[38] Ibid

- **Government Issued System:** Under this model, a Digital ID, is issued by the statement and the identity attributes are stored in one or more government owned database(s). UAE's Emirates ID is a classic example which may be used as the basis for verifying other digital identities, such as banking and mobile phone credentials.

- **Private Sector Initiated and government-endorsed digital identity providers:** In this model a semi-centralized system, individuals are free to choose between multiple trusted identity providers (e.g., banks, mobile operators, etc.) and use these credentials to access a broad range of public and private services *via* an identity hub or gateway that facilitates authentication across multiple platforms (e.g., Sweden, Finland, UK, Australia).

4.3 Lifecycle of a Digital ID System

The lifecycle of identity systems includes three major components[39]:

- **Component One: Identity proofing and enrolment (with initial binding/credentialing)**

This component is the most important step in creation of a Digital ID. It answers the question of "Who are you?". This process involves collecting, validating and verifying the identity information of an individual, enrolling the individual with an identity account and connecting (or binding) the individual's unique identity to authenticators possessed and controlled by this person. Thus, this component involves the following stages:

- **Collection of identity information:** Includes registering an individual though a registration process during which phase, information relating to core attributes and other identifiers of the individual is collected e.g. by filling out an online form; sending a selfie photo for collection of facial recognition attributes.

- **Validation of identity information:** Once a person has claimed an identity during enrollment, this identity is then validated by checking the attributes presented against existing data. The validation process establishes the reliability and genuineness of the data and checks whether or not the claimed identity exists at the time of registration (i.e., the person is alive and present) and can be localized (i.e., the person can be reached through their address, phone number, or e-mail).

- **Resolving data information:** This process involves resolving identity evidence and attributes to a single unique identity within a given population or context(s). The process of resolving identity evidence and attributes to a single unique identity within a given population or context (s) is called *de-duplication*. Some government-provided

[39] Under FATF, "*Public consultation on FATF draft guidance on digital identity"* available at https://www.fatf-gafi.org/publications/fatfrecommendations/documents/consultation-digital-id-guidance.html accessed on December 9, 2019

digital identity solutions include a *de-duplication* process as part of identity proofing, which may involve checking specific the applicant's biographic attributes (e.g., name, age, and gender); biometrics (e.g., fingerprints, iris scans, or facial recognition images); and government-assigned identifiers (e.g., driver's license and/or passport numbers or taxpayer identification number) against the identity system's database of enrolled individuals and their associated attributes and identity evidence to prevent duplicate enrolment.

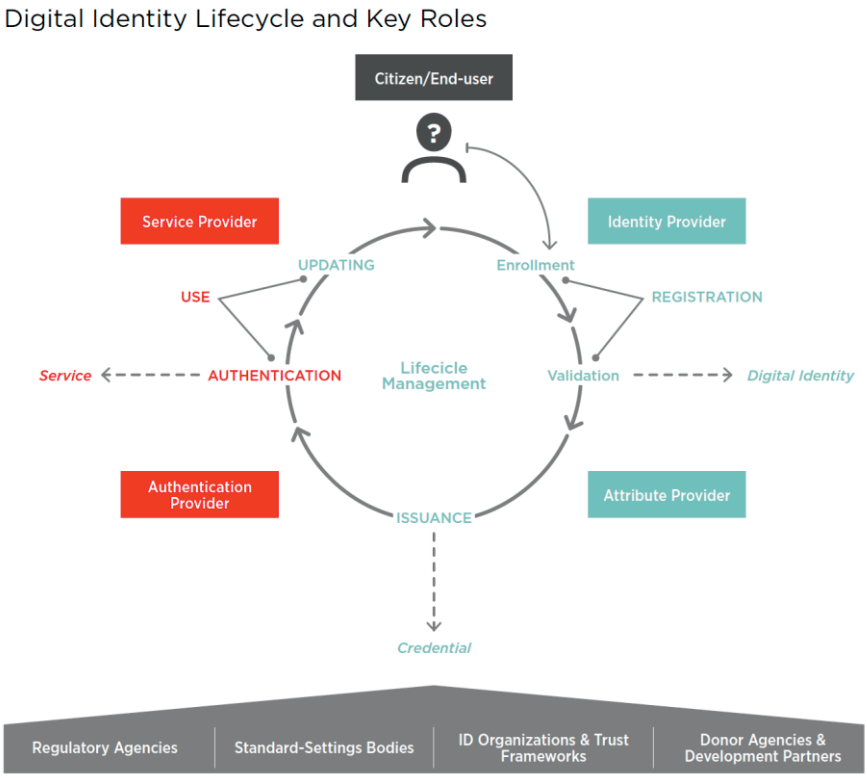
- **Verification:** Involves confirming that the validated identity relates to the individual (applicant) being identity proofed. For example, the identity service provider could send an enrolment code to the applicant's validated phone number which is tied to the identity, require the applicant to provide the enrolment code to the identity service provider; and confirm the submitted enrolment code matches the code the identity service provider sent, verifying that the applicant is a real person, in possession and control of the validated phone number. At this point, the applicant would have been identity proofed.

- **Enrolment:** Means the process by which an identity service provider enrolls an identity-proofed applicant as a 'subscriber' establishes their identity account. This process authoritatively binds the subscriber's unique verified identity (i.e., the subscriber's attributes/identifiers) to one or more authenticators possessed and controlled by the subscriber, using an appropriate binding protocol. The process of binding the subscriber's identity to authenticator(s) is also referred to as 'credentialing'.

- **Component Two: Authentication**

Authentication answers the question, "*Are you who you say you are?*". It establishes that the individual seeking access to an account (or other services or resources) - the claimant is the same person who has been identity proofed, enrolled, and credentialed (e.g., is the on-boarded customer). Authentication itself could be undertaken utilizing attributes which the person either '*has'* (*e.g.* cryptographic keys stored in hardware, a OTP in a hardware device, or a software OTP generator installed on a digital device, such as a mobile phone), '*knows'* (*e.g.* a shared secret, a personal identification number (PIN), or a response to a pre-selected security question) or '*is'* (*e.g.* facial, fingerprint or retinal pattern biometrics).

FIGURE 4 – Identity Lifecycle



Source: GSMA, World Bank and Security Identity Alliance, Digital Identity towards Shared Principles for Public and Private sector Co-operation available at https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2016/07/Towards-Shared-Principles-for-Public-and-Private-Sector-Cooperation.pdf accessed on November 14, 2019

- **Component Three: Portability and Interoperability mechanisms**

Portable identity means that an individual's digital identity credentials can be used to prove official identity for new customer relationships at unrelated private sector or government entities, without their having to obtain and verify personally identifiable information and conduct customer identification and verification each time. Portability requires developing interoperable digital identification products, systems, and processes. Portability/interoperability can be supported by different Digital ID architecture and protocols.

In accordance with the Draft FATF Guidance, essentially Component One and Component Two would mandatorily be required to be digital for an identity system to be considered as a Digital ID system.

4.4 Technical Standards & System Requirements

Globally it has been recognized that a Digital ID system should be technologically robust and must be based on 'open standards'. Various international bodies may have different parameters for defining 'open standards'. For instance, ITU-T defines 'open standards' '*as standards made available to the general public and are developed (or approved) and maintained via a*

collaborative and consensus driven process."[40] ITU-T recognizes that open standards facilitate interoperability and data exchange among different products or services and intend widespread adoption between different players.

To be classified as 'open standards', the technological standard should be publicly available or be published.The standard specification document is available either freely or at a nominal charge. Such standards may usually be developed through efforts of not-for-profit organizations, and its ongoing development occurs on the basis of an open decision-making procedure available to all interested parties (consensus or majority decision etc.) Standards may also define how various identity systems may be able to communicate with each other without compromising the privacy and security requirements of each individual identity system..

Open standards are also a key to solving another major pain point in the introduction of Digital ID systems by regulatory bodies – vendor "lock-in" or technology dependency. Open standards create a framework for developers by defining the components of a system and how they interact with each other. The standards may provide basic parameters for operation of the system without limiting or inhibiting technology providers from protecting their intellectual property and differentiating themselves from the competition, thus continuing to drive innovation. By standardizing what components make up a system and how they communicate, systems become more agile and agnostic. This results in provider and technology neutrality and provides the governments flexibility in choosing between the various technological solutions available. The risk of a wrong decision or choice is significantly reduced because the systems are based on accepted and recognized open standards which are agile and adaptable. Also, governments will be at a lower risk of contractual lock-in because patents and other proprietary issues no longer stand in the way. Ultimately, an open standards approach allows governments to strategically plan and evolve their systems without fear of future compatibility issues – providing a guarantee of consistency and harmonization across government identity ecosystems.

- **Levels of Assurance**

When utilizing a technology provider and a related a Digital ID system, it is pertinent to gauge the Level of Assurance provided by the identity system. When a person identifies or authenticates herself using one or multiple identity attributes, the degree of confidence that he/she is who he/she claims to be depends on the degree of security assurance provided and the context in which the information is captured.[41] A level of (identity) assurance (LOA) is the certainty with which a claim to a particular identity during authentication can be trusted to actually be the claimant's "*true*" identity[42]. Higher levels of assurance reduce the risk of a fraudulent identity and increase the security of transactions. However, this can also mean increased the cost to

[40] ITU-T, "*Definition of Open Standards*" available at https://www.itu.int/en/ITU-T/ipr/Pages/open.aspx accessed on February 2,2020
[41] World Bank, "*Catalog of Technical Standards for Digital Identification Systems*" available at http://documents.worldbank.org/curated/en/707151536126464867/pdf/129743-WP-PUBLIC-ID4D-Catalog-of-Technical-Standards.pdf accessed on December 11,2019
[42] World Bank, "*ID4D Practitioners Guide Version 1.0*" available at http://documents.worldbank.org/curated/en/248371559325561562/pdf/ID4D-Practitioner-s-Guide.pdf accessed on December 11,2019

parties concerned including the identity holders and relying agencies indirectly resulting in exclusion.

The LOA of a Digital ID system depends on the strength of the identification and authentication processes and are critical to access control and reducing identity theft. The higher the LOA, the lower the risk is that service providers will rely on a compromised credential during a transaction. LOA depends on the strength of the identity proofing process and the types of credentials and authentication mechanisms used during a transaction.

For identity proofing, the level of assurance depends on the method of identification (e.g., in-person vs. remote), the attributes collected, and the degree of certainty with which those attributes are verified (e.g., through crosschecks and deduplication). For authentication, the level of assurance depends on the type of credential(s), the number of authentication factors used (i.e., one vs. multiple), and the cryptographic strength of the transaction.[43]

Various organizations and entities have developed frameworks for identity systems – notable ones being ISO/IEC 29115, eIDAS Regulation and the NIST Guidelines (U.S.A). In this respect, of particular interest is the eIDAS Regulation (Regulation for electronic Identification, Authentication and trust Services - EU No 910/2014), which was published in 2014 and applies as law within the whole of the EU. In support of the European Commission's Digital Single Market initiative, eIDAS aims to facilitate the smooth flow of commerce in the EU. The Regulation aims to remove existing barriers to the cross-border use of electronic identification means, at least for public services (Recital 12 eIDAS Regulation). In furtherance to the same, identification continues to be a matter of national sovereignty, but member states are obliged to accept notified electronic identification means of other member states. This obligation applies if they allow the use of electronic identification means for online access to their public services, and if the LOA of the notified means is equal or higher than the one necessary to access the service. The eIDAS Regulation defines three different assurance levels (low, substantial and high) depending on the degree of confidence in the claimed or asserted identity of a person.

TABLE 6: Levels of Assurance -eIDAS

Level of Assurance	Identity assurance (identity proofing at registration)	Authentication assurance
Low	• Present ID from authoritative source (remote or in-person)	• Single factor (e.g., password or PIN)
Substantial	• Present ID (remote or in-person) • ID verification performed by registration authority	• Multi-factor (e.g., mobile phone + PIN)
High	• In-person ID proofing at registration authority	• Multi-factor • Must access private data/keys stored on tamper-resistant hardware token

[43] Ibid

	• ID verification using official government sources and documents	• Cryptographic protection of personally identifying information (PII)

The eIDAS regulation constitutes a major step towards the vision of a single market between member countries in the EU. This regulation provides a reference for regulators implementing a Digital ID system.

- **Interoperability of the System**

The World Bank's ID4D has laid down their key objective of globally spreading fully functional and interoperable identity systems that provide all individuals with the right to a unique and secure identity. ID4D believes that disintegration and division of identity systems, with redundant and contradictory databases, is one of the main barriers in the adoption of an effective and trusted foundational identity system.[44] Interoperability is the ability to transfer and render useful data and other information across systems, applications, or components.[45] Interoperability ensures a common understanding of the exchanged data between systems and across organizations, consequently thereby improving access to eGovernment services, smarter governance and easier access to healthcare, education and other financial inclusion objectives[46].

The attributes that get recorded as a part of the identity and the method used to capture them have important implications for the trustworthiness of the identity and its interoperability with other domestic and international identity systems. Moreover, a high level of interoperability contributes in reducing operating costs. Implementing the systems based on a unified technical standard would hence be a pertinent requirement for the purposes of creating a universal Digital ID system with a cross-border utility.

In general, technical standards contain a set of specifications and procedures with respect to the operation, maintenance, and reliability of materials, products, methods, and services used by individuals or organizations.[47] Adoption of standards has a positive impact in market penetration and international trade. A lack of standards creates issues for the effectiveness and robustness of an identity system, including problems with interoperability, interconnectivity and vendor lock-in.[48] Several organizations are actively developing technical standards for Digital ID systems, including international organizations such as the ISO and other UN specialized agencies, industry

[44] Vyjayanti Desai, Alan Gelb, Julia Clark, Anna Diofasi, World Bank "Ten Principles on Identification for Sustainable Development", (February 2017) available at http://blogs.worldbank.org/ic4d/ten-principles-identification-sustainable-development accessed on November 17, 2019.
[45] Urs Gasser, "*Interoperability in the Digital Ecosystem*" (July 6, 2015), available at https://ssrn.com/abstract=2639210 or http://dx.doi.org/10.2139/ssrn.2639210 , accessed on November 13, 2019.
[46] Id4africa.com, "*Interoperability in African Governments: Digital Identity as an Enabler*", (2019) available at http://www.id4africa.com/2019_event/presentations/InF11/4-Chimezie-Emewulu-Seamfix.pdf accessed on November 13, 2019.
[47] World Bank,, "*Technical Standards for Digital Identity",* (ID4D in 2017) available at http://pubdocs.worldbank.org/en/579151515518705630/ID4D-Technical-Standards-for-Digital-Identity.pdf accessed on November 14, 2019.
[48]Ibid

consortia, and country-specific (national) organizations.[49] However, choosing between standards is challenging due to rapid technological innovation and disruption, product diversification, changing interoperability and interconnectivity requirements, and the need to continuously improve the implementation of standards.

From a regulatory standpoint, the regulators and international agencies may need to recognize and recommend standards which may be adopted and the systems that need to be implemented in this respect. An important case in point is the European Council's efforts in this respect – adopting two regulations establishing a framework for interoperability between EU information systems in the area of: (a) justice and home affairs[50]; and (b) police and judicial cooperation, asylum and migration[51]. The regulations establish the following interoperability components[52]:

- **A European search portal**, which would allow competent authorities to search multiple information systems simultaneously, using both biographical and biometric data.
- **A shared biometric matching service**, which would enable the searching and comparing of biometric data (fingerprints and facial images) from several systems.
- **A common identity repository**, which would contain biographical and biometric data of third-country nationals available in several EU information systems.
- **A multiple identity detector**, which checks whether the biographical identity data contained in the search exists in other systems covered, to enable the detection of multiple identities linked to the same set of biometric data.

The systems covered by the two regulations provide support for national authorities and include the entry/exit system, the visa information system, the European travel information and authorization system, Eurodac, the Schengen information system and the European criminal records information system for third country nationals, as well as other relevant databases on travel documents.[53]

4.5 Digital Identity for Legal Persons

A large number of financial and banking transactions are undertaken at the behest of corporate bodies. Businesses, consumers and government agencies are all faced with the challenge to understand 'who is who' in the digital and global supply chain. In this report, the primary focus relates to creating identity for individuals. However, it is relevant to highlight the importance of

[49] Other organisations include international organisations like the IEC, ITU-T, country-specific organizations like the ANSI; the NIST, DIN; the UIDAI; the BIS; and the PSA and industry consortia like Biometric Consortium; SIA, CITeR; IEEE Biometrics Council; Biometrics Institute, Australia; Smart Card Alliance; IBIA; Kantara Initiative; Open Identity Exchange; Open Security Exchange etc.
50 Regulation (EU) 2019/817 on establishing a framework for interoperability between EU information systems in the field of Borders and Visa.
[51] Regulation (EU) 2019/818 of the European Parliament and of the Council of 20 May 2019 on establishing a framework for interoperability between EU information systems in the field of police and judicial cooperation, asylum and migration and amending Regulations (EU) 2018/1726, (EU) 2018/1862 and (EU) 2019/816
[52] Council of EU, "*Interoperability between EU information systems: Council Presidency and European Parliament reach provisional agreement*" , (May 2019) available at https://www.consilium.europa.eu/en/press/press-releases/2019/05/14/interoperability-between-eu-information-systems-council-adopts-regulations/ accessed on November 14, 2019.
[53] Ibid

creating identity for corporate bodies as well. FATF Recommendation 10(b) recognizes the importance of identifying the ownership of corporate bodies.

Globally, legal systems have made differentiation between natural persons / individuals and corporate bodies, with each being granted legal status to undertake transactions and deals. The details surrounding this classification is often embedded in national legislations. Undertaking CDD on corporate entities would include tracing back the ultimate owners of the entities. In line with the international and national regulations, banking systems have adopted measures to identify the ultimate owner. The Digital ID system would be major contributor in this process. For example, in Bangladesh, the digital IDs of the board of directors and management team is being recorded along with the businesses for larger businesses, for validating beneficial ownership of the business.[54]

However, in addition to the identification of beneficial ownership, there is a growing demand to create a system for identification of businesses themselves. A case in point is Singapore's 'CorpPass', which is a corporate digital identity for businesses and other entities (such as non-profit organizations and associations) to transact with government agencies online.[55] In any event, a corporate digital identity is useful and relevant only if it can be a '*reliable'* source of identification for the entity. It would also require access by a 'natural person', who must assert and authenticate his/her own identity attributes, before being allowed to access and assert the corporate identity and associate it with a transaction.

Even if entities have an identification system nationally, a global single identification code unique to each institution is significant to identify the transaction details of individual corporations, identify the counterpart of financial transactions, and calculate the total risk amount. To meet the requirements surrounding such a unified identity, the LEI was adopted by the G20 in 2012. The LEI is a 20-character, alpha-numeric code based on the ISO 17442 standard. It connects to key reference information that enables clear and unique identification of legal entities participating in financial transactions. Each LEI contains information about an entity's ownership structure and thus answers the questions of 'who is who' and 'who owns whom'.[56] While there is no prohibition for legal entities in other sectors to request a LEI, there is a substantial cost attached and needs to be renewed on an annual basis.

5 Benefits of a Digital ID System

As per McKinsey Global Institute, a 'good' Digital ID is identification that is verified and authenticated to a high degree of assurance over digital channels, is unique, is established with

[54] World Bank Group, "*G20 Digital Identity Onboarding*" (2018), available at http://documents.worldbank.org/curated/en/362991536649062411/pdf/129861WP-10-9-2018-17-26-21-GDigitalIdentityOnboardingReportlowres.pdf accessed on 28 October 2019
[55] GovTech Singapore, "CorpPass" available at https://www.tech.gov.sg/products-and-services/corppass/ accessed on December 11,2019
[56] GLEIF, "*Introducing the Legal Entity Identifier (LEI)"* available at https://www.gleif.org/en/about-lei/introducing-the-legal-entity-identifier-lei accessed on December 11,2019

individual consent, protects user privacy and ensures control over personal data[57]. Such an identification system would benefit not only FIs but also the users, identity providers, relying parties, governments and regulators. It has the potential to benefit the individuals already active in the digital world by facilitating greater control of data, privacy protections, security for online interactions and reduced friction in managing online accounts.

- **Increased use of and access to financial services**

  Digital ID helps individuals meet customer identification and verification requirements and enables remote customer registration for financial services. According to a World Bank survey, lack of documentation, non-proximity to FIs, and cost of financial services are each cited by 20% -30% of respondents as a reason for not having access to a bank account.[58] As per ID4D Findex survey reports, in Brazil, for example, Digital ID could help 39 million adults improve access to financial services and facilitate increased extension of credit to both individuals and MSMEs.[59].

  Similarly, in Sweden, the adoption of the BankID has revolutionized the banking system. BankID is a leading electronic identification system adopted by a number of large banks in Sweden for use by members of the public, authorities and companies. Currently, 8 million people have been reported to use BankID on a regular basis for a wide variety of private and public services.[60] Many services are provided where citizens can use their BankID for Digital ID as well as signing transactions and documents. The services range from online and mobile banking, e-trade to tax declaration and are provided by government, municipality, banks and companies.[61]

  The African experience has shown that digital financial services can pave way to resolving the concerns surrounding financial exclusion. Since its launch in 2008, in Tanzania, mobile money has helped Tanzania to expand access to financial services to almost half the population. The rate of mobile money use in Tanzania is amongst the highest in the world with 48% of the population reporting to have used the services.[62] However, an effectiveness

[57] Olivia White et al, "*Digital identification A key to inclusive growth"* (McKinsey) available at https://www.McKinsey.com/~/media/McKinsey/Business%20Functions/McKinsey%20Digital/Our%20Insights/Digital%20identification%20A%20key%20to%20inclusive%20growth/MGI-Digital-identification-Executive-summary.ashx accessed on October 28, 2019.
[58] Leora Klapper et al, "*The Global Findex Database: Measuring Financial Inclusion and the Fintech Revolution*", (World Bank, 2017) available at https://globalfindex.worldbank.org/ accessed on November 18, 2019.
[59] Leora Klapper et al, "*The Global Findex Database: Measuring Financial Inclusion and the Fintech Revolution*", (World Bank, 2017) available at https://globalfindex.worldbank.org/ accessed on November 18, 2019 ; See also, World Bank "*World Development Indicators*", available at http://datatopics.worldbank.org/world-development-indicators/ , accessed on November 18, 2019.
[60] BankID.com, "*This is BankID*" available at https://www.bankid.com/en/om-bankid/detta-ar-bankid accessed on November 17, 2019.
[61] Ibid
[62] Financial Inclusion Insights Program, "*Digital Pathways to Financial Inclusion*" (Tanzania, Wave 1 in November 2014), available at http://finclusion.org/uploads/file/reports/FII-Tanzania-Wave-One-Wave-Report.pdf , accessed on November 15, 2019.

of such a system can be fully achieved with a Digital ID system facilitating and easing CDD processes.

- **Individuals and institutions can benefit from Digital ID in a range of other interactions – mobile registrations, e-services, employment, healthcare, asset base etc.**

  Individuals can use identification to interact with businesses, governments, and other individuals in six capacities - as consumers, workers, microenterprises, taxpayers and beneficiaries, civically engaged individuals, and asset owners.[63] Correspondingly, institutions can use an individual's identity in a variety of positions - as commercial providers of goods and services, interacting with consumers; as employers, interacting with workers; as public providers of goods and services, interacting with beneficiaries; as governments, interacting with civically minded individuals; and as asset registers, interacting with individual asset owners.

  Upon implementation of a Digital ID model, the identity system may be used as an authentication tool for various purposes including opening bank accounts, mobile registrations, accessing e-services *etc*. For example, Pakistan's CNIC is a legal Digital ID card issued by Pakistan's NADRA. The regulatory agencies in the telecom sector in Pakistan (namely the Pakistan Telcom Authority and the Ministry of Information Technology) collaborated to introduce a SIM registration system, which made it mandatory for the cell phone owners to register each new SIM against their CNIC number[64].

- **Time and cost savings.**

  Digitization of identity enables process streamlining and automation while reducing the need for travel, a particular benefit for people who live in far away locations. For instance, in Estonia, Digital ID enables voting online, saving 11,000 working days per election.[65]
  Both private and public institutions benefit most from cost savings as a result of Digital ID. In Estonia, for example, the identity system saves an estimated 2% of GDP each year by reducing identity related transaction costs and facilitating online services.

  Digital ID systems also eliminate redundant systems improving efficiency of identity related transactions.[66] This can include avoiding duplicate data collection or eliminating obsolete databases or credentials. In Malawi, for example, integration between the national ID and

---

[63] Olivia White et al, , "*Digital identification A key to inclusive growth"* (McKinsey) available at https://www.McKinsey.com/~/media/McKinsey/Business%20Functions/McKinsey%20Digital/Our%20Insights/Digital%20identification%20A%20key%20to%20inclusive%20growth/MGI-Digital-identification-Executive-summary.ashx accessed on October 28 2019

[64] DAWN Newspaper, *"Unregistered mobile phones to become unusable after 20th: PTA"* availalble at https://www.dawn.com/news/1438714/unregistered-mobile-phones-to-become-unusable-after-20th-pta accessed on November 20, 2019.

[65] E-Estonia.com, "*e-Identity: ID card*," available at http://www.e-estonia.com/solutions/e-identity/id-card, accessed on November 17, 2019.

[66]World Bank, "*Public Sector Savings and Revenue from Identification Systems: Opportunities and Constraints*", (2019) available at http://documents.worldbank.org/curated/en/745871522848339938/Public-Sector-Savings-and-Revenue-from-Identification-Systems-Opportunities-and-Constraints.pdf accessed on November 15,2019

voter registration eliminated the need for a separate voter ID card, saving approximately US$44 million ahead of the 2019 elections[67].

- **Reduced fraud.**

Digitization can reduce risks of fraud, identity theft and misplacement of documents, and reduce the overall cost of customer verification processes. The fraud-reduction mechanism operates by eliminating multiple and ghost beneficiaries. In Uganda, the government reportedly saved US Dollars 6.9 million in less than a year by verifying the identities of civil servants against the national identity database, removing some 4,664 ghost workers from the public payroll.[68]

- **Increased tax collection.**

A unique identity can be used to de-duplicate tax records and identify individuals who use multiple tax identities to decrease their liabilities. Similarly, identification systems that link the tax administration with other data sources—e.g., land records, vehicle registers, customs databases, and social benefits registers—can better identify businesses or individuals who are underreporting their earnings or assets. In Tanzania, the National Identification Authority estimates that of the 14 million people capable of paying taxes, only 1.5 million, or around 10% do so.[69] In India, the Ministry of Finance estimates that only 35 million people (less than 3 percent of the total population) are in the taxpayer base.[70] In Latin American countries, some studies have estimated that approximately half of potential tax revenues are lost to tax evasion.[71]

- **Other Social Benefits**

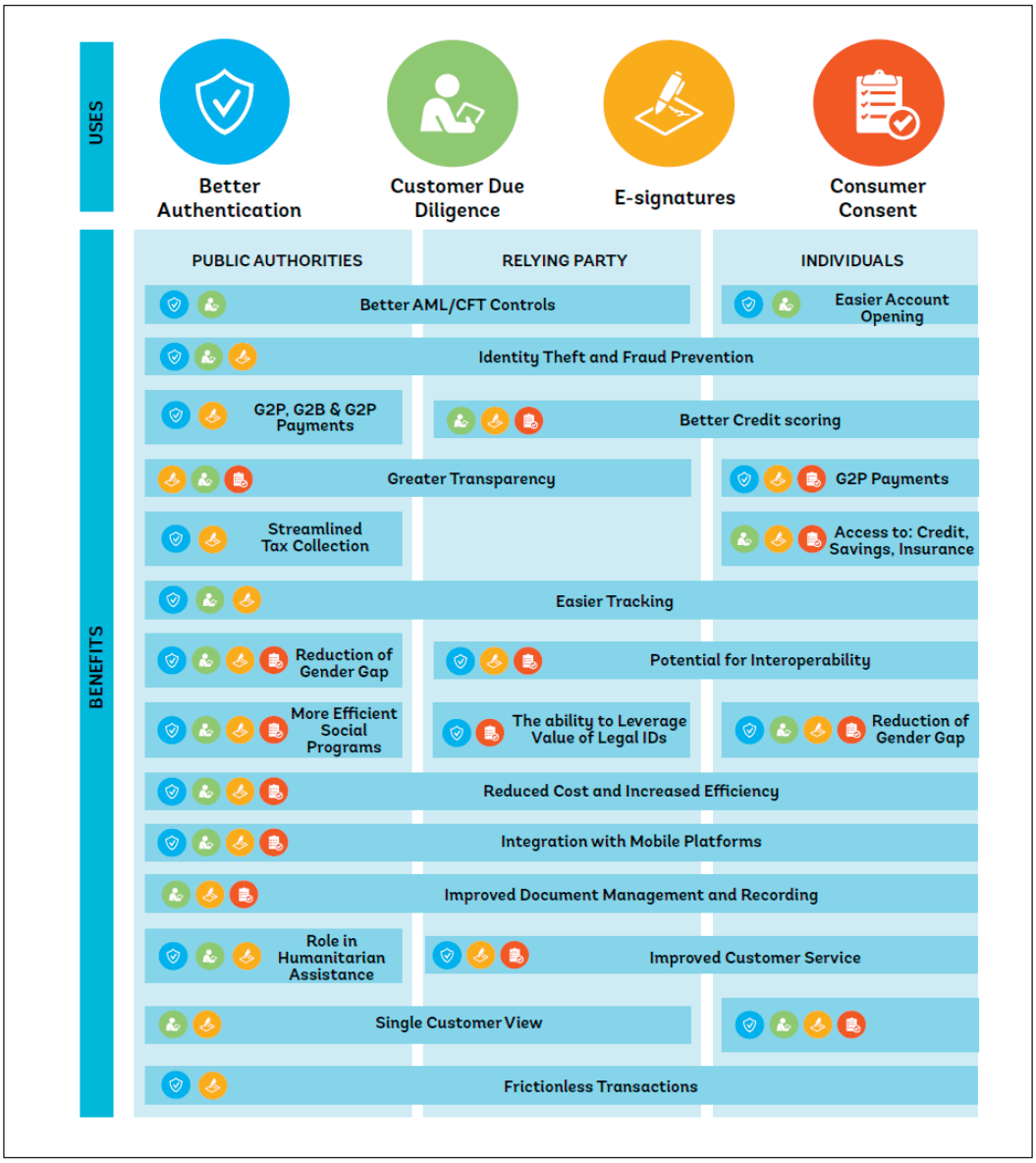
Digital ID can also be a major trigger for reducing gender cap and has a major effect in humanitarian efforts. Apart from the benefits to the government and the customers, a Digital ID is also highly beneficial for service providers also. Service provider that connect to the Digital ID system program are able to[72]:

---

[67] Ibid
[68] World Bank, "*Public Sector Savings and Revenue from Identification Systems: Opportunities and Constraints*", (2019), available at http://documents.worldbank.org/curated/en/745871522848339938/Public-Sector-Savings-and-Revenue-from-Identification-Systems-Opportunities-and-Constraints.pdf accessed on November 15, 2019.
[69] Joseph J. Atick, "*Digital identity: The essential guide*", (ID4Africa Identity Forum, 2014), available at http://www.id4africa.com/main/files/Digital_Identity_The_Essential_Guide.pdf, accessed on November 17, 2019.
[70] Ibid.
[71] Eduardo Cavallo et al. (2016),"*Saving for development: How Latin America and the Caribbean can save more and better*", (InterAmerican Development Bank in June 2016), available at https://publications.iadb.org/publications/english/document/Saving-for-Development-How-Latin-America-and-the-Caribbean-Can-Save-More-and-Better.pdf, accessed on November 17, 2019
[72] Digital Transformation Agency, "*Benefits of joining the digital identity ecosystem*" available at https://www.dta.gov.au/our-projects/digital-identity/benefits-joining-digital-identity-ecosystem, accessed November 17, 2019.

- Improve efficiency – the need to maintain expensive identity and access management systems and support systems such as help desks will be significantly reduced, allowing staff to focus on the delivery of services.
- Minimize costs and regulations –private services will benefit from reduced operating costs and reducing the need for many people to verify their identity in person.
- Improving security and enhancing privacy – the Digital ID ecosystem will enhance their ability to work more collaboratively with their public sector counterparts. The requirement for providers to be accredited against government security standards nationally will contribute to a significant increase in security awareness across all levels of the public service.

FIGURE 5 – Benefits of The ID System



6 Risks and challenges in implementing a Digital Identity System

Digital ID tends to be complex and subject to failure to deliver on high expectations. Risks associated with unsuccessful implementation can be mitigated by adopting guidelines that have emerged from the collective experience of Digital ID schemes rollouts around the world. Additionally, in the financial sector, certain risks associated with or related to money laundering or terrorist financing may also have a significant impact on the implementation of a Digital ID system – the detailed analysis of the various money laundering and terrorist financing risks (ML/TF risks is included in Annex I).

6.1 The risk of exclusion

The World Bank's ID4D program has also taken a key leadership role in supporting developing country governments towards the goal of financial goal: *"We believe that every person has the right to participate fully in their society and economy. Without proof of identity, people may be denied access to rights and services – they may be unable to open a bank account, attend school, collect benefits such as social security, seek legal protection, or otherwise engage in modern society. No one should face the indignity of exclusion, nor be denied the opportunity to realize their full potential, exercise their rights, or to share in progress. No one should be left behind."*[73]

Demographics, culture and ethical considerations all require attention when defining a Digital ID. An effective Digital ID is inclusive, but there might be certain segments of the population from whom collecting biometric information is difficult, inaccurate or impossible. Such populations might include vulnerable populations (including tribal and ethnic populations or those with unclear migration status) as well as those with low digital literacy or lack of connectivity. Physical features, cultural and religious beliefs, age factors, occupational factors might make fingerprint and iris capture of sufficient detail and quality, problematic. For example, persons working in hard labor occupations or have leprosy likely will be unable to successfully scan their fingerprints. Similarly, changes in age may result in changes in facial features, affecting facial recognition.

Legal, procedural, and social barriers to enroll in and use identification systems should be identified and mitigated, with special attention to poor people and groups who may be at risk of exclusion for cultural, political or other reasons (such as women, children, rural populations, ethnic minorities, linguistic and religious groups, migrants, the forcibly displaced, and stateless persons).

The UNHCR estimates that there are more than 65 million FDPs worldwide.[74] FDPs are less likely than other migrants and foreign nationals to possess proof of identity, which may have been forgotten, lost, destroyed, stolen in transit, or purposefully left behind.[75] FDPs face identity-related barriers that contribute to instances of exclusion and limit their access to mobile connectivity, financial services, education, healthcare and employment.

[73] World Bank, "*Principles on Identification- For sustainable development: Towards the Digital Age*", (February, 2017) available at http://pubdocs.worldbank.org/en/200361509656712342/web-English-ID4D-IdentificationPrinciples.pdf accessed on November 17, 2019.
[74] UNHCR, "*Figures at a Glance*", (2019), available at http://www.unhcr.org/uk/figures-at-a-glance.html accessed on November 17, 2019.
[75] GSMA, "*Refugees and Identity: Considerations for mobile-enabled registration and aid delivery*", (2017), available at https://www.gsmaintelligence.com/research/?file=1cb984aae8f279c617fb30b151bad5a8&download accessed on November 17, 2019.

6.2 Political Concerns[76]

Creating an identity system is a complex political process and issuing legal identity documents involves the complex process of determining who is eligible and has access to particular rights and entitlements. The creation of a national identity system (digital or otherwise) therefore requires a unified vision and approach that can overcome the common fragmentation of identity by ministries, departments, regions, or donor funded projects related to identification.

6.3 Cost Implications[77]

Creating a Digital ID system is a costly project that may require extensive investment in building or updating infrastructure and technology. Discussions with key stakeholders about technology choices and business models—including ways to accelerate national and regional deployment and uptake—are pivotal for avoiding unforeseen costs and ensuring that identity systems can grow efficiently to meet future needs.

6.4 Data Privacy, Protection and Security

Digital ID systems aim to achieve multiple global development goals at large (financial and economic inclusion, social protection, healthcare, education for all, gender equality, child protection, agriculture, good governance, as well as safe and orderly migration). Such goals are achievable through empowerment of individuals and facilitating their access to rights, services, and economic opportunities, however – all of which requires proof of identity of such individual(s), all of which raises challenges and risks for digital privacy and data protection. While harnessing the full potential of Digital ID for development, it is important to be mindful of the fact that digitization can exacerbate the scale and frequency of such risks, which may have serious and often immeasurable consequences for people, thus, requiring appropriate protections.[78]

Data privacy differs from the right to privacy - the right to be let alone,[79] which means the appropriate and permissioned use and governance of personal data. The European Union's (EU) General Data Protection Regulation (GDPR)[80] provides an international good practice standard for data protection and privacy. In identity systems, data privacy means that data should only be accessed, processed, or shared by and with authorized users for pre-determined and specified purposes which have been consented to by the data subject, in advance. Data protection is

[76]GSMA, World Bank and Security Identity Alliance, "*Digital Identity towards Shared Principles for Public and Private sector Co-operation*", (July 2016) available at https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2016/07/Towards-Shared-Principles-for-Public-and-Private-Sector-Cooperation.pdf accessed on November 14, 2019.
[77] Ibid
[78]Julia Clark and Conrad Daly, "*Digital ID and the Data Protection Challenge*", (World Bank, 2019) available at http://documents.worldbank.org/curated/en/508291571358375350/Digital-ID-and-the-Data-Protection-Challenge-Practitioners-Note , accessed on November 20, 2019.
[79] Wikipedia, "The right to privacy (article), available at https://en.wikipedia.org/wiki/The_Right_to_Privacy_(article) , accessed on November 20, 2019.
[80] GDPR. "General Data Protection Regulation" available at https://gdpr-info.eu/ accessed on November 20, 2019.

fundamental to ensuring data privacy - this includes the legal, operational, technical methods/controls for securing information and enforcing rules over access and use.[81]

Digital ID involves the collection, safekeeping (as custodian) and processing of an individual's (data subject's) personal data. Digital databases that contain identity attributes used for identity proofing may include personally identifiable information and attributes, such as an individual's name, age, height, date of birth, ID numbers, as well as fingerprints or other biometric information.[82]

TABLE 7: Personal Data Guidance

According to the UN Personal Data Protection and Privacy Principles[83] personal data should be:

1. **Processed in a fair and legitimate manner, taking into account the person's consent and best interests, as well as larger legal bases.**
2. **Processed and retained consistent with specified purposes, taking into account the balancing of relevant rights, freedoms and interests.**
3. **Proportional to the need, by being relevant, limited and adequate to what is necessary to the specified purposes.**
4. **Retained only for the time necessary for the specified purposes.**
5. **Kept accurate and up to date in order to fulfill the specified purposes.**
6. **Processed with due regard to confidentiality.**
7. **Secured by appropriate safeguards (organizational, administrative, physical, technical) and procedures should be implemented to protect the security of personal data, including against or from unauthorized or accidental access, damage, loss or other risks presented by data processing.**
8. **Processed with transparency to the data subjects, as appropriate and whenever possible.**
9. **Only transferred given appropriate protections to a third party.**
10. **Done accountably, with adequate policies and mechanisms in place to adhere to these Principles.**

A data controller is a person, company, or other body that is responsible for the preservation of the confidentiality, accuracy, integrity and availability of the data. In this context, the data controller is a Digital ID service provider.[84] In terms of the classification of data, not all types of data merit the same level of protection. Personal data (which is any information relating to an identified or identifiable natural person)[85] and sensitive personal data (any personal data which is which is particularly sensitive in relation to a data subject) merit specific protection, because

[81] Julia Clark and Conrad Daly, "*Digital ID and the Data Protection Challenge*", (World Bank, 2019) available at http://documents.worldbank.org/curated/en/508291571358375350/Digital-ID-and-the-Data-Protection-Challenge-Practitioners-Note , accessed on November 20, 2019.
[82] FATF-GAFI (2019), "*Draft Guidance on Digital Identity*", available at https://www.fatf-gafi.org/media/fatf/documents/publicconsultation/Digital%20ID-public-consultation-version.docx , accessed on November 20, 2019.
[83] See United Nations System, "*Personal Data protection and Privacy principles*" (December 2018), available at https://www.unsystem.org/personal-data-protection-and-privacy-principles , accessed on November 20, 2019.
[84] FATF-GAFI (2019), "*Draft Guidance on Digital Identity*", available at https://www.fatf-gafi.org/media/fatf/documents/publicconsultation/Digital%20ID-public-consultation-version.docx, accessed on November 20, 2019.
[85] Article 4 GDPR, "*Article 4 GDPR: Definitions*" available at https://gdpr-info.eu/art-4-gdpr/, accessed on November 20, 2019.

of the fact that the processing of such data could create substantial risks to a person's fundamental rights and freedoms.

Any activity that collects, stores, or processes personal data raises certain risks, including, but not limited to security breaches, unauthorized disclosure, function creep, identity theft, surveillance risk etc. While the above-discussed risks are present in any identity system, Digital ID systems may augment both the risks and the harms beyond traditional, paper-based systems because they enable:[86]

1. Ever-increasing and mass data security breaches through the consolidation of data, while also making such databases more attractive targets.
2. Digitization allows for the easy (or mass) deletion / destruction of data. Without appropriate data safeguards, entire records may disappear
3. Easy copying of digital records, as opposed to the physical copying and subsequent collation of documents.
4. Exposure of "hidden", but connected personal data: Automatic data processing, as supported through artificial intelligence and machine learning, makes possible discovery of vast arrays of patterns and other information through analytics, by connecting distinct informational pieces about a person from dissimilar sources, or in using metadata about individuals or groups.

In the context of data protection and privacy, as well as international good practice standards, Digital ID systems raise data privacy concerns because they collect and allow for the use and processing of personal data. A Digital ID system should ideally be designed to adequately provide for the strengthening of transparency, efficiency, availability, effectiveness of governance and service delivery, in order to ensure the proper functioning of Digital ID systems and in turn, this can assist the public sector reduce fraud and leakage in government to person data transfers, facilitate new modes of service delivery and proliferate overall administrative efficiency. In the context of a digital economy and in combination with trust services (such as e-signatures / digital signatures), Digital ID systems facilitate trusted transactions, streamline business operations and create opportunities for innovation.[87]

Security benefits of digitized systems present various new opportunities and technological means for greater protection. Specifically, Digital ID systems may offer:[88]

1. More accurate identification and authentication in the leveraging of computer processing and advanced technologies, thus offering a higher level of assurance and accuracy than manual, paper-based authentication processes (volatile to human error and discretion). This increases trust, reduces costs and supports sustainable, flexible systems.

[86] Julia Clark and Conrad Daly, "*Digital ID and the Data Protection Challenge*", (World Bank, 2019) available at http://documents.worldbank.org/curated/en/508291571358375350/Digital-ID-and-the-Data-Protection-Challenge-Practitioners-Note , accessed on November 20, 2019.
[87] Julia Clark and Conrad Daly, "*Digital ID and the Data Protection Challenge*", (World Bank, 2019) available at http://documents.worldbank.org/curated/en/508291571358375350/Digital-ID-and-the-Data-Protection-Challenge-Practitioners-Note , accessed on November 20, 2019.
[88] Ibid

2. Improved data integrity through the adoption of adequate data protection measures better assurance of the integrity and use of collected data, in stark contrast to paper-based records systems that can be easily destroyed, damaged, or altered. Furthermore, automated, safeguarded and tamperproof transaction logging provides auditable records of data processing, thereby improving accountability and aiding the addressing of security breaches.
3. Better and more distinctive data privacy guarantees: Digital technology enables new privacy-enhancing features that were previously not possible. In systems using non-digital credentials, transaction typically involves presenting a physical identity card to a service provider, and therefore revealing all the displayed information (in example: presenting a physical credential as proof of a person's age reveals additional information, such as their full name, date of birth and, often, their address). Digital technology can help resolve this issue through digital credentials that obscure or selectively present only the data necessary.
4. Increased agency and control: New technologies and design strategies give individuals greater control over their personal data, including access portals that allow users to verify the correctness of their data and monitor the usage of their data, which could automate data breach notifications.
5. Emerging Digital ID ecosystems provide users with wider choice of ID providers.

Protecting data and privacy in a digital world[89]

Data privacy and security measures should be integrated throughout the identity lifecycle and data protection must become an organizational standard (norm). This requires a privacy and security by design approach[90], including a privacy and security by default approach, following the foundational principles of:

1. Developing a proactive and not a reactive system that take a preventative approach;
2. Making privacy the default setting, rather than requiring affirmative action;
3. Embedding privacy into the technical design from the start rather than retrofitting it;
4. Construing privacy in a positive-sum manner (as a win-win based scenario manner of thought), and not as a zero-sum (being exclusionary as an 'either/or' approach);
5. Developing end to end security with a view to full lifecycle protection;
6. Building a system allowing for visibility and transparency, as well as keeping systems open and accountable; and
7. Keeping the system user centric, with an eye to respecting user data privacy, as an ethical responsibility.

[89] Julia Clark and Conrad Daly, "*Digital ID and the Data Protection Challenge*", (World Bank, 2019) available at http://documents.worldbank.org/curated/en/508291571358375350/Digital-ID-and-the-Data-Protection-Challenge-Practitioners-Note , accessed on November 20, 2019.
[90] Ann Cavoukian "*Privacy by Design: The 7 foundational principles*" (2011) Available at https://iab.org/wp-content/IAB-uploads/2011/03/fred_carter.pdf. accessed on November 20, 2019.

Designing systems that implement data protection principles[91]

Legal frameworks are fundamental to protecting personal data in ID systems and as such, must be put into practice with organizational, management, and technology safeguards, therein too translating laws and regulations into their technical and operating specifications, including limits on data collection and usage. For this purpose, operational controls (such as: detailed operational manuals, staff training, physical and cybersecurity measures etcetera) and privacy enhancing technologies are necessary. These technologies and controls work to implement privacy principles through various strategies, including minimizing data processing; hiding, separating, or aggregating personal data; informing individuals and giving them control over data use; and embedding 'compliance by design' and 'compliance through design' approaches, and demonstrating compliance with legal requirements as well as international legal and technical standards. [92]

Additional risks:

In elaboration of the risks discussed above, further or greater risk is posed in terms of the volume and nature of data breaches or spills, be it through inadequate protective measures, accidents (with the possibility of negligence, depending on application of the principles of foreseeability and reasonableness) or malicious, intentional attacks to infiltrate systems, in order to gain access to data. Data breaches can constitute a privacy threat and also, a national security risk. The consequences of failing to protect individuals' data must be commensurate with the risks that individuals and a State or Country would suffer from the theft of personal data.

As discussed below, the largest breach documented to date of a national Identity data base is that of India's national ID database, known as the Aadhaar. This breach affected and exposed the national ID numbers, addresses, phone numbers, email addresses, postal codes, and photographs of Indian citizens – and adding to this, the data then being sold for profit and likely used for various scrupulous, unauthorized purposes and which can continue for as long as such data remains in the hands of such unauthorized persons / parties. The impact of such a breach is momentous and can certainly have a ripple effect on the economic population and the society of such country (or any such affected Country) and its citizens. Furthermore, such data is vulnerable to exploitation in the hands of scrupulous actors, along the likes of Nation States, cyber criminals etc. thereby placing national security at risk.

---

[91] Julia Clark and Conrad Daly, "*Digital ID and the Data Protection Challenge*", (World Bank, 2019) available at http://documents.worldbank.org/curated/en/508291571358375350/Digital-ID-and-the-Data-Protection-Challenge-Practitioners-Note , accessed on November 20, 2019.

[92] Compliance by Design (CbD) means that the set of rules is taken into account in the design stage of the business process. The conformity check takes place in advance. Hence, CbD has a *preventive* side: it means that compliance "should be embedded into the business practice, rather than be seen as a distinct activity". On the other hand, Legal Compliance through Design (LCtD) complements CbD by recognizing the role of social, political, and economic conditions (as pre-conditions) and governance and ethical requirements (as constraints) when designing legal compliance, encompassing norms and principles that require a balancing of competing rights, obligations or policies. See Pompeu Casanovasabc, Jorge González-Conejeroc, Louis de Koker, "*Legal Compliance by Design (LCbD) and through Design (LCtD): Preliminary Survey",* available at http://ceur-ws.org/Vol-2049/05paper.pdf, accessed on November 20, 2019

In terms of the threat of geopolitical risk, with associated risks, such as financial, legal, and cybersecurity being functions of a geopolitical risk ecosystem, one must have a keen understanding of how geopolitical risks can serve as causal factors for concrete and direct risks to information security. One example hereof is hacktivism, which epitomizes the irrefutable impact of socioeconomic and cultural factors on cybersecurity wherein hacktivism is used as an act of protest or retaliation against political oppression, economic depravity, and injustice. Varied effects can be seen here from, one being in the example of Anonymous' Operation Tunisia93 DDoS attacks during the 2010 Arab Spring94, wherein Anonymous, a decentralized international hacktivist group that is widely known for its various DDoS cyberattacks against several governments, government institutions and corporations.

Current legislative framework in the Arab region[95]

It is remarkable to note that the countries in the Arab Region have taken cognizance of the developments globally surrounding protection of personal data. Few nations have explicitly identified specialized laws which relate to personal data and data privacy while others depend on their other generic rules and regulations to this end. Some key legislations in this respect include:

- Lebanon - Law no. 81 of 10 October 2018 (on Electronic Transactions and Personal Data) and Banque du Liban Basic Decision no. 12872 of 13 September 2018 (on General Data Protection Regulation (GDPR));
- Mauritania - Law 2017- 020 on Data Protection;
- Bahrain - Law no. (30) of 2018 regarding Issuing the Personal Data Protecting Law;
- Morocco - Law 09-08 on the Protection of Individuals with regard to the Processing of Personal Data;
- Algeria - Law no. 07-18 that dated 10 June 2018 related to Protecting Person when Dealing with Personal Data;
- Tunisia - Act no. 2004 – 63 of July 27th 2004, on the Protection of Personal Data.[96]

7 CDD & e-KYC:

The legislative and policy developments globally have increased the AML/CFT compliances which must be followed by entities during financial transactions. Extensive processes and procedures have been implemented, which are to be followed by FIs to eliminate or mitigate financial fraud and money-laundering. On the other hand, in response to the growing demands of the digital world, the FIs are striving to deliver better customer friendly onboarding

[93] The Atlantic, "*The Hacks That Mattered in the Year of the Hack"* available at https://www.theatlantic.com/technology/archive/2011/12/hacks-mattered-year-hack/333755/ accessed on December 23,2019
[94] Ibid
[95] Survey Response by Participating Countries
[96] As per the response, Tunisia was one of the first Arab country to ratify the Convention no. 2018 of the Council of Europe via the organic Law No. 2017-42 of May 30, 2017, approving the accession of the Republic of Tunisia to Convention No. 108 of the Council of Europe for the Protection of Individuals with regard to the automated processing of personal data and its Additional Protocol No. 181 concerning supervisory authorities and cross border data flows.

experiences. These contrasting positions between the public and private sector highlights the requirements to have a strong CDD regime. As highlighted extensively in Annex I, FIs must take into account the various ML/TF risks and implement proper process to eliminate or mitigate such risks.

Essential to operationalizing financial integrity is the need for FIs to know who their customers are. A financial system in which customers are anonymous is one that can easily be abused and corrupted. To foster financial inclusion, a few countries have put in place the systems for electronic customer identification and verification, enabling providers to capture user identification details electronically or digitally, as would occur using Digital ID.

As per the Global Findex Database 2017[97], financial inclusion is being driven by the uptake of mobile phones and access to the internet. Financial services are no longer the preserve only of FIs. DFS is a relatively new, low-cost means of digital access to transactional financial services[98]. Often termed 'mobile money' or 'mobile financial services,' DFS is one of the core solutions used in developing countries to provide the marginalized populations much-needed low-cost access to financial services. DFS may be offered by FIs or other non-banking financial service providers referred to as DFSPs[99] - who may be licensed or authorized by a range of regulators to provide these services, either on their own or in mandated partnerships. The need to have a robust KYC regime that may facilitate the use of such innovative solutions to achieve financial inclusion is the need of the hour.

7.1 The responsibility of verifying customer identity; and ascertaining suitability and preferences

The FATF Recommendations on CDD are the most comprehensive and elaborate among the 40 Recommendations. 'KYC' is often used colloquially when customer identification and verification is discussed. FATF does not use the term 'KYC'. Its standards use and detail CDD. 'KYC', referring to "Know Your Customer" does not have an internationally accepted definition. It is sometimes used synonymously with 'CDD' but more often used to refer only to the 'customer identification and verification' element of CDD i.e the 'customer onboarding process'. International AML/CFT standards set by FATF require FSPs to perform specific CDD measures both upfront when approached by a prospective customer and during the relationship. The various CDD measures which are required to be undertaken by the FSPs are listed below.

[97] World Bank, "*The Global Findex Database 2017*", (2018) available at https://globalfindex.worldbank.org/ accessed on November 17, 2019.
[98] Leon Perlman, "*The Digital Financial Services Primer*", (2018) available at http://www.citicolumbia.org/wp-content/uploads/2018/11/DFS-primer-for-publication.pdf , accessed on November 19, 2019
[99] Ibid

TABLE 8: Customer Due Diligence

CDD measures	Associated actions
Customer identification and verification	• Collecting identifying particulars of prospective customers and establishing the veracity of the key identifying particulars using reliable, independent source documents, data, or information
Establishing beneficial ownership	• In relation to individuals, determining whether a person is acting on behalf of another or on behalf of a group (such as a household or a savings scheme in the financial inclusion context) • In relation to legal entities, trusts, and arrangements, determining who is the actual controller of a customer or the beneficiary of a business relationship, service, or transaction • In practice, depending on the information found, undertaking further processes to identify other associated persons that may give rise to AML/CFT risk relevant to the business relationship
Risk assessment and profiling	• Collecting information to understand the purpose and intended nature of the business relationship and to create a risk profile of the customer • The collection process includes checking customers, beneficial owners, and associated persons against sanctions and blacklists and determining whether the customer is a "politically exposed person" (PEP) (e.g., senior politicians, senior civil servants, and their relatives who may be vulnerable to corruption)
Transaction monitoring and reporting	• Continuously monitoring transactions to detect and investigate any unusual transactions and report those that are potentially suspicious to the Financial Intelligence Unit (FIU)—a governmental body set up to receive and analyze such transaction reports • Continuously monitoring transactions to identify ones that, though not necessarily suspicious, are nonetheless reportable, such as transactions involving more than a set amount in cash in countries with cash reporting requirements • Assisting the FIU with further enquiries regarding reported transactions

Source : Timothy Lyman, et al. "*BEYOND KYC UTILITIES: Collaborative Customer Due Diligence for Financial Inclusion"* available at https://www.cgap.org/sites/default/files/publications/2019_08_28_Working_Paper_Beyond_KYC_Utilities_0.pdf accessed November 17, 2019.

Traditionally, the process of customer identification and verification was undertaken by FSPs by relying on information provided by customers or inferred from an identification document which was produced / submitted by the customer. The physical identity document would then be used to verify any details

through the submission of physical supporting documents like proof of identity. In essence, a person is identified when the key identifiers are noted. The identifying information can be provided orally by the client or taken from the document. The document is then used to verify those details.

Therefore, FSPs would examine unexpired government-issued identification documents such as a driver's license and/or passport. Upon the introduction of a legal, unique, interoperable and digital identity, countries would need to consider appropriate amendment to their CDD framework to ensure that it responds appropriately to the new Digital ID system.

FATF Recommendation 10 mandates that the "*principle that financial institutions should conduct CDD should be set out in law."* Though countries have been granted the choice to determine the means of enforcement of CDD regime, the requirement is to be implemented

through legal provisions. To undertake the CDD, the regulated entities may use a reliable and independent source to determine the customer identity. As highlighted by the Draft FATF Guidance, the necessity of a "reliable and independent" identity source may be addressed by a trustworthy Digital ID system.[100] FSPs may be able to rely on a Digital ID system verified, assured, audited, certified by the government (either directly, or by designating organizations to act on its behalf) to undertake CDD[101]. In the absence of such a reliable identity system, the FSPs would be obliged to ensure the robustness of such a system.

The FATF Recommendations are underpinned by a 'risk-based' AML/CFT principle which requires FIs to assess the money laundering or terrorist financing risks posed by their products, services, customers and jurisdiction. These should be classified from higher to lower risks and measures should be adopted to mitigate these risks proportionally. Where higher risks are identified, enhanced CDD measures must be adopted. Countries may however allow institutions to adopt simplified CDD measures where risks are assessed as lower. The Wolfsberg Group details these principles, reflecting that CDD is a key aspect of AML controls[102].

Further, the FSPs are also expected to review and analyze the risks associated with the use of a Digital ID system. Governments and FSPs are encouraged to consider if, depending on the potential ML/TF risk factors and mitigating measures, the same degree of reliability may not be required for each component of the Digital ID system. Governments and FSPs are encouraged, to consider the reliability of Digital ID information based on the assurance frameworks and standards followed by the Digital ID system.

7.2 Approaches to Customer Identification and Verification

Customer identification and verification is critical process in CDD. A KYC regime may be utilized by the FSP to have knowledge of a client's objectives, needs and circumstances or be prepared to say that the client has refused to identify those objectives. Such a process may also result in the FSP making an affirmative inquiry as to the financial circumstances and position of a customer, thus attempting to match the value of the transactions undertaken by such customer against their financial position.

As highlighted by GSMA association in its report, there are two approaches to conducting customer identification and verification process[103]. The first approach includes the ***'Tiered Customer Due Diligence'.*** Under the tiered system, CDD requirements increase as product

[100] FATF, "*Public consultation on FATF draft guidance on digital identity"* available at https://www.fatf-gafi.org/publications/fatfrecommendations/documents/consultation-digital-id-guidance.html accessed on December 9,2019.
[101] Ibid
[102] The Wolfsberg Group, "*The Wolfsberg Frequently Asked Questions on Risk Assessments for Money Laundering, Sanctions and Bribery & Corruption"* available at https://www.wolfsberg-principles.com/sites/default/files/wb/pdfs/faqs/17.%20Wolfsberg-Risk-Assessment-FAQs-2015.pdf accessed on November 20, 2019.
[103] Jim Woodsome and Michael Pisa, "*Overcoming the Know Your Customer hurdle: Innovative solutions for the mobile money sector"*, (GSMA, 2019), available at https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2019/02/Overcoming-the-KYC-hurdle-Innovative-solutions-for-the-mobile-money-sector.pdf, accessed on November 19, 2019.

functionality and risks associated with a product increase. This allows people to access very basic products with simplified CDD but more CDD requirements apply progressively should they want to access products with a higher functionality. Accordingly, FSP may undertake simplified, basic or enhanced CDD depending on the risks associated with the transaction or the customer.

- Basic Customer Due Diligence is information obtained for all customers to verify the identity of a customer and assess the risks associated with that customer;
- Simplified Due Diligence are suited for situations where the risk for money laundering or terrorist funding is low;
- Enhanced Due Diligence is additional information collected for higher-risk customers to provide a deeper understanding of customer activity to mitigate associated risks.

Simplified due diligence is of particular benefit to the poor and underserved people who may not have the identity documents required to meet the full range of CDD. However, certain other marginalized groups or sections of society (like refugees who are members of communities that are associated with terrorist financing and people living in rural areas where illicit drug crops are cultivated) may still be excluded due to the 'high risk' posed by them. Even if simplified CDD does apply, an FSP may still determine that it is too expensive to onboard a customer segment that may not be highly profitable. In both cases, collaboration on one or more of the associated CDD elements outlined above may lower FSP compliance costs and thereby address financial inclusion.

The second approach is e-KYC is to allow approved entities to query a national identity system to authenticate or verify customers' identities and, in some cases, to retrieve basic attributes about them, which attributes may be stored electronically or digitally. E-KYC programmes can improve the onboarding process by reducing or eliminating paper-based procedures and record-keeping, which reduces cost and time spent on verification, making it more profitable to provide services to low-income customers. However, an e-KYC system requires a robust Digital ID system to be effective.

Based on the FATF Recommendations, governments and regulatory agencies in various parts of the world have provided guidelines to the FIs on the anti-money laundering and countering the financing of terrorism. A summary of some of the key directions/ guidelines provided to the FIs in relation to CDD is included as Annex II.

In accordance with the findings of the survey of the Arab countries (please refer below), most countries in the Arab region are still in the early stages of introduction of e-KYC. For example, Central Bank of Egypt has confirmed that presently tiered KYC regime is being followed in the country and an e-KYC solution is being explored. Similarly, in the survey response, Central Bank of Tunisia has identified that customer identification and verification process adopted in the country may be simplified or enhanced depending on risk profile of both the client and the nature

of account. Tunisia is also proposing to implement e-KYC for payment institution accounts only where, it is utilized for two types of account[104]:

a) First - Account where the cap of total amounts to be collected is 500 Tunisian dinars (the cash outflows per day should not be over 250 Tunisian dinars)
b) Second -Account where the cap of total amounts to be collected is 1000 Tunisian Dinars (the cash outflows per day should not be over 500 Tunisian dinars). In this scenario, simplified CDD procedures are also required to be followed.

It may be highlighted that, though as a part of the customer identification and verification process undertaken based on a Digital ID, all details that are available in relation to such person may not be shared or disclosed with the FSP, to ensure compliance with the data privacy and security requirements. However, tracking the individual's transactions based on the individual's profile including the financial situation and needs, tax status, investment objectives, investment experience, liquidity needs, risk tolerance, and any other information the customer may disclose to the FSP could be useful in detecting any irregular, improper or illegal transaction.

7.2 Challenges of e-KYC programmes[105]

The KYC process, which protects against AML/CFT violations, have seen inconsistent levels of adoption amongst FSPs due to:

a) Absence of Legal Certainty: Legal certainty is critical in embarking on Digital ID and e-KYC programs, especially if harmonization and integration of various identity databases is required as part of (creating) a national Digital ID. This process requires clear legal frameworks and delegation of responsibilities to the contributing authorities or agencies who control part or all of each component database.
b) Limited budgets: Cost remains a key consideration for all parties concerned, including the government as well as the regulated FSPs. A new technology would be adopted if it could provide financial and compliance benefits, at the existing stage the quality of CDD could be compromised due to cost impact – including capital and operational costs
c) Lack of internal technological and compliance capabilities: Internal challenges including insufficient compliance expertise and resources as well as technological constraints are another barrier for adopting complex emerging technologies required for e-KYC programmes.
d) Security of Systems, Privacy and Data Protection: The design imperatives on usability and security of an e-KYC programme is crucial are for use in CDD process. Any imminent threats to cyber security could potentially question the reliability of the data provided. Ensuring data protection and privacy when dealing with large volumes of e-

[104] Survey Response of Central Bank of Tunisia/ Tunisian Financial Analysis Committee
[105] Finda Systems, "*Digital KYC proof-of-concept white-paper 1 : Overview of the Digital KYC authentication system*" (November 2018) available at https://findasystem.com/download/KPI%20FINDA%20FSTI%20POC%20paper%201%20-%2019Nov2018.pdf , accessed on November 19, 2019

KYC data is a major issue and the absence of data protection laws may create a important challenge in adoption of e-KYC programmes

e) Absence of shared compliance utilities: CDD is conducted in isolation by each regulated institution no CDD information is shared.

f) Lack of reliable and high-quality data: Lack of reliable data could arise due to several reasons such as manual customer onboarding, inefficient data capture practices.

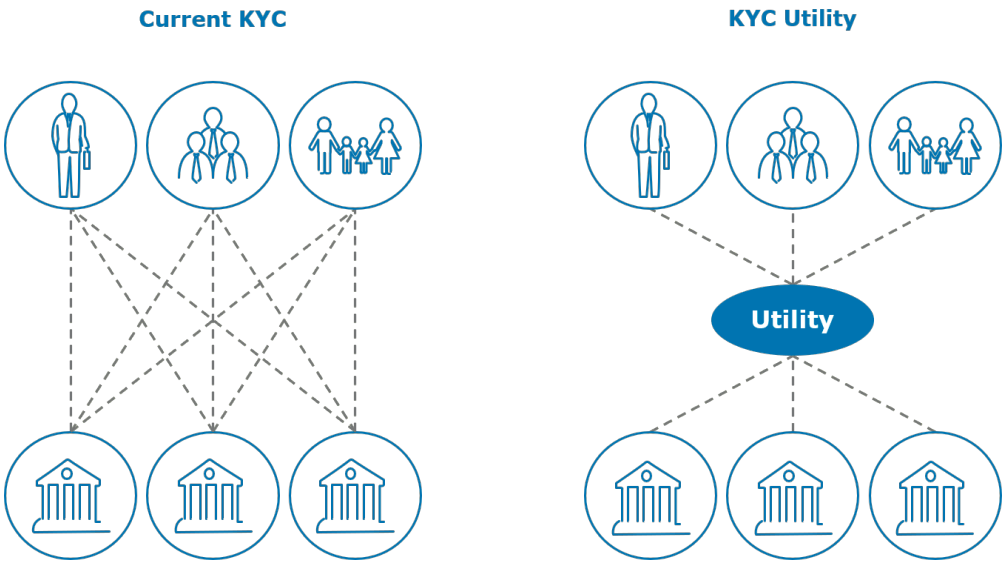
g) Lack of Co-ordination: Further, lack of coordination amongst regulatory bodies within a nation as well as technology failures can result in expensive effects on the society and the economy. Coordination is hence needed not just for a legal framework to use Digital IDs but also for technical and financial feasibility for service providers to use a common database for e-KYC. Similarly, over-bearing - or uncoordinated – customer identification and verification requirements issued by some regulators as part of the mandate may unintentionally exclude vulnerable and socially disadvantaged consumers.

h) Need for regional standardization: The larger regulated institutions that operate over different jurisdictions would require a degree of CDD standardization across those jurisdictions. Based on the national legislations, larger regulated institutions would be required to modify or adapt their CDD systems to comply with the national legislations and practices, often increasing costs and bringing about complexities.

7.3 KYC Utilities and Collaborative CDD models

Historically, FSPs were obligated to carry the full operational and financial burden associated with CDD. However, with the developments in technology, various solutions called 'KYC Utilities' have emerged. A 'KYC Utility' is a venture which centralizes collection, verification, storage, and sharing of clients' data and documents.

FIGURE 6 – KYC Utility



Source: Capgemini, "*KYC Utility: why should you consider it?*" available at https://www.capgemini.com/2019/07/kyc-utility-why-should-you-consider-it/ accessed on December 22, 2019

Presently, such KYC Utilities are being developed by commercial providers or industry bodies that store customer identity data in a single repository for use by multiple FSPs[106]. By pooling resources, reducing duplicative efforts, and digitizing processes through KYC Utilities, FSPs can shorten the time required for identity checks and verification, reduce CDD compliance costs and potentially improve the quality and reliability of customer data. However, as has been highlighted by CGAP (global partnership of 34 leading organizations), KYC Utilities are just one of the many approaches adopted by FSPs and governments in their endeavors to resolve the financial inclusion challenges posed by measures to combat money laundering and the financing of terrorism. The various approaches are referred to as 'Collaborative CDD'107. Collaborative CDD may adopt various forms including having the government provide e-KYC as a service or have the private sector pioneer new technologies to address the toughest challenges posed by identity creation by utilizing innovative technologies like blockchain technology. Parallelly, there is a rise in collaboration between the law enforcement agencies or regulatory bodies aimed at improving measures that are taken for conducting CDD.

In practice, better results in financial inclusion can be achieved by allowing digital identification, enabling e-KYC and adopting collaborative CDD models. Such solutions may include approaches such as the following:[108]:

a) E-KYC programs led by the public sector: In this scenario, the national identity authorities that support Digital ID verification by FSPs provide e-KYC as a service. Such a service is extremely effective, given the acceptability and reach of such programs. A good example of such a system would be the e-KYC program in Pakistan which leverages the country's extensive national biometric ID system developed and managed by NADRA. NADRA data are used for identity verification of individuals relating to both bank account opening and mandatory mobile SIM card registration.
b) Centralized KYC solutions: In this structure, the CDD service providers hold centralized, verified identity particulars of persons or businesses and makes these available to multiple FSPs for a fee. These approaches differ from typical outsourcing arrangements in that they require participating FSPs to standardize their customer data in accordance with an agreed format and contribute the data to the central pool. For example, in India, as per the directives of the Ministry of Finance, the CERSAI is to perform the functions of the Central KYC Records Registry (CKYCR). The CERSAI will receive, store, safeguard and retrieve know your customer records in digital form for a client, as against other KYC Registration Agencies such as Computer Age Management Services and Karvy, which maintain KYC information provided by investors on their individual systems and verified

[106] Timothy Lyman and Louis De Koker, "*KYC Utilities and Beyond: Solutions for an AML/CFT Paradox?"* (2018) available at https://www.cgap.org/blog/kyc-utilities-and-beyond-solutions-amlcft-paradox , accessed on November 19, 2019
[107] Ibid.
[108] Timothy Lyman, et al, "*BEYOND KYC UTILITIES: Collaborative Customer Due Diligence for Financial Inclusion"* (August, 2019) available at https://www.cgap.org/sites/default/files/publications/2019_08_28_Working_Paper_Beyond_KYC_Utilities_0.pdf accessed November 17, 2019.

in person.[109] Upon an enrollment by a customer, a customer's data may be verified using e-KYC or other verification processes. The customer details once included into the registry will entitle him to a KYC identifier. Customers can use the identifier when they deal with another FSP. As of May 2019, the centralized KYC is still in an early phase where the database is being built with new customer identification and verification information.[110]

c) Identity management solutions led by the private sector: Another category of customer identification and verification services enables customers to manage their own identification data digitally and provide selected information at a specific point in time for customer identification and verification purposes. Such services are usually based on distributed ledger. In contrast to the centralized registry approach, these services decentralize data and empower customers to hold and manage their own identity data. For example, the KYC solution built on Corda blockchain, which went through a successful trial by 21 corporates and 5 banks in France in December 2018.[111] Under this utility, users to have complete control of their data, being certain that this data will not be shared with other actors unless these users have given their explicit permission.

In addition to most of the above structures, one additional model which will be of significance would be a KYC Utility model which works under public private partnership model. However, this is still a conceptual proposition since there are no examples available to analyse the benefits of such a model.

Collaborative CDD approaches including KYC Utilities can mutually reinforce changes that help countries reduce certain types of crime, improve productivity, increase financial inclusion; and potentially improve trust in AML/CFT capacity, and increase integration and economic growth. However, to this to be achieved, the legislative mandate to FSPs to rely on e-KYC identity verification may have a major role to play.

As per the survey of the Arab countries, it appears that at this juncture, the nations have not considered the use of banks or other FIs to be an additional vehicle for authenticating and onboarding customers to the KYC repository.

7.4 Lifecycle of Financial Services and Common Authentication Processes

Access to financial services may divided into various stages : (a) account opening; (b) customer due-diligence; (c) transaction authentication; (c) periodic re-validation for reverifying the CDD data; and (d) product-specific events, such as the reissuance of an internet banking password, which require the re-validation of identity documents to ensure that the information is being

[109] Asim Parashar and Anish Chandra, "*Central KYC; What it means for investors and institutions"* (PWC, 2017) available at https://www.pwc.in/assets/pdfs/financial-service/central-kyc.pdf , accessed on November 19, 2019.
[110] Timothy Lyman, et al, "*BEYOND KYC UTILITIES: Collaborative Customer Due Diligence for Financial Inclusion"* (August, 2019) available at https://www.cgap.org/sites/default/files/publications/2019_08_28_Working_Paper_Beyond_KYC_Utilities_0.pdf accessed November 17, 2019.
[111] Fintech Futures, "*Regional KYC utilities: genesis of global collaboration on shared compliance platforms"* (2019) available at https://www.fintechfutures.com/2019/11/regional-kyc-utilities-genesis-of-global-collaboration-on-shared-compliance-platforms/, accessed on November 19,2019

provided to the rightful owner of the account relationship.[112] To achieve this objective, various authentication processes or methodologies may be adopted. Authentication attempts to answer the question – ' Are you who you say you are' and hence relies on what a person 'has', 'is' or 'knows'. The processes or methodologies utilized for this purpose may include[113]:

a) Single-factor Authentication: A single factor authentication applies where the customer logs in with just a username and password, passcode, or PIN. This is the lowest level of secure access management an organization can deploy, and should only be used for accessing non-sensitive information
b) Two Factor Authentication: A two-factor authentication applies where the customer logs in using a username and password, passcode, or PIN. This is the lowest level of secure access username/password, passcode, or PIN, and then are requested to input a second security measure, like an SMS or token-based OTP. This level of authentication should only be used for accessing non-sensitive information. Using a second factor is a significant bump in security that should be used for any account that has even marginal access to sensitive data.
c) MFA: Adding in a third, fourth, or even fifth authentication factor expands the security of any access management solution. The additional factors included would include passwords, secret questions, OTP, biometrics, user behavior, registered mobile devices, and more.

Within the realm of multi-factor authentication, some types of authentication systems include smartcards, mobile SIM authentication and biometric authentication, each of them briefly explained below[114]:

- A 'Smartcard' is a card that has embedded integrated circuit or chip. Smartcards can be used to store attributes and credentials such as biometric data and can enable interaction with recorded data. For example, a smartcard can be used to verify that a fingerprint sample collected by a connected device is the same as a template stored in the smartcard.
- Mobile SIM Authentication: This authentication measure uses the unique identification numbers associated with mobile subscriber identity modules or SIM cards. The algorithms contained in the SIM card allow for encrypted communication between the user and the network. For authentication, the authenticating body generates a random sequence of numbers that is sent to the user's mobile- this is the user's public key.
- Biometrics Authentication: Biometric authentication, if employed accurately, could act as one of the reliable means of supporting identity verification at a large scale than data generated by human processes. Biometrics include physical and behavioral attributes of

[112] Harish Natarajan (2018), "*G20 Digital Identity Onboarding*" (World Bank Group, 2018), available at https://www.gpfi.org/sites/gpfi/files/documents/G20_Digital_Identity_Onboarding.pdf accessed on November 12, 2019.
[113] Veridium, *"What is Two-Factor Authentication (2FA)?",* available at https://www.veridiumid.com/two-factor-authentication-2fa/ accessed on November 19, 2019.
[114] Harish Natarajan (2018), "*G20 Digital Identity Onboarding*" (World Bank Group, 2018), available at https://www.gpfi.org/sites/gpfi/files/documents/G20_Digital_Identity_Onboarding.pdf accessed on November 12, 2019.

a person which are unique to an individual. It includes features like iris scan, fingerprinting etc. When considering which biometric to use for authentication, jurisdictions should consider the accuracy, universality, stability, the ease of collection and cost components involved. Particularly, for a biometric solution to be effective, it must carefully balance several considerations:[115]

a) Security: This is a crucial aspect of any biometric solution. Centrally storing biometric data on a national identity authority's server is convenient. However, the risk of identity theft is a major risk in this scenario resulting from a server hack. To this end the security measures adopted should be well defined and technologically sound.
b) Cost and convenience: Security is of the utmost importance in a biometric solution, but it is also important to recognize that enhanced security features can be expensive to implement resulting in a slow adoption of such techniques across developing countries.
c) Inclusiveness: In addition to balancing security with costs and convenience, a biometric identity solution must be as inclusive as possible. For example, iris scans may be challenging when creating ID documents for persons with eye diseases. Similarly, facial features may change with age or may even be difficult to be collected from sections of the population (like women) due to religious and cultural practices.
d) Accuracy and Reliability: Governments, FSPs and users all need to have confidence in a CDD mechanism for it to work. As with security, accuracy and reliability are important factors in establishing confidence.

It may be highlighted that the nature of measures utilized and the factors utilized increases the level of security assurance in each financial transaction. Most countries in the Arab region collect biometric information in the nature of fingerprints as a part of the identity collection.

8. CASE STUDIES FROM NON-ARAB COUNTRIES

8.1 India

With the second most populous country in the world, India can lay claim to having the world's single largest biometric-based digital identification system - Aadhaar (which roughly translates to "Foundation" in English). The program assigns each registrant a unique 12-digit identity number that is linked to minimal personal information (including name, gender, date of birth, and a digital photo) and biometric information (fingerprints and iris scans) that can be used for authentication.

Many Indian residents today have several forms of identity for different purposes, such as a voter ID card, a ration card for accessing the public distribution system, a PAN card for tax registration,

[115]Paul Makin and Chrissy Martin, "*The Biometric Balancing Act in Digital Finance*", (CGAP, 2018) available at https://www.cgap.org/blog/biometric-balancing-act-digital-finance , accessed on November 19, 2019

a driver's license, and a passport. The application and verification process for each of these identities is different and procedurally complex. Therefore, although India's Electoral Commission began issuing photo identity cards as early as 1993, the launch of Aadhaar is often viewed as the government's first national identity initiative.

It is estimated that Aadhaar covers about 1.2 billion people. In 2008, it was estimated that only 40 million had a passport, 70 million a PAN card 220 million a ration card, and 500 million a voter ID card.[116] To resolve this, the government proposed creating a single biometric identification system that would be housed in and monitored by the UIDAI and that would allow a more accurate representation of each of the Indian residents and their access to and use of public services. It is estimated that there has been over 90% adoption of Aadhaar. Launched in 2009 Aadhaar enables biometric digital authentication as part of broader digital ecosystems with additional functionality.

Mandatory Requirement:

Of one of the most intriguing debates in the implementation of Aadhar, the most important one was the de-linking of Aadhar by the Supreme Court of India for certain sectors. The Supreme Court adjudged that Aadhar cannot be made mandatory for openings of a bank account and for getting mobile connections and fundamental rights like the right to obtain school admissions. However, linking of the Aadhar with the PAN Card for the purposes of tax was upheld to be mandatory under Section 139AA of the Income Tax Act.[117]

Lessons from the Aadhaar experience

The following lessons from India's experience can help other countries navigate the issues involved in the implementation of a national identity system.

- **Identity First**

Aadhar is an 'identity first' approach and has been de-linked from a person's nationality and is instead available to all "residents" and is not limited to Indian citizens only. [118] To be eligible for enrolment, an applicant does not have to prove their Indian citizenship; they are required to

[116] GSMA, "*Aadhaar: Inclusive by design: A look at India's national identity program and its role in the JAM trinity*", (March 2017) available at https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2017/03/gsma-aadhaar-report-270317.pdf , accessed on November 19, 2019.
[117] Economic Times, "*What's valid and what's not: Everything you need to know about Aadhaar verdict*", (September, 2018), available at economictimes.indiatimes.com/articleshow/65961427.cms?from=mdr&utm_source=contentofinterest&utm_medium=text&utm_campaign=cppst , accessed on November 19, 2019.
[118] The Aadhaar (Targeted Delivery Of Financial And Other Subsidies, Benefits And Services) Act, 2016 is a legislation which is aimed to provide for, as a good governance, efficient, transparent, and targeted delivery of subsidies, benefits and services to individuals residing in India through assigning of unique identity numbers to such individuals. Under Article 2(v) '*resident'* means an individual who has resided in India for a period or periods amounting in all to 182 days or more in the preceding 12 month period.

supply only proof of residence.[119] Therefore, the number of persons having Aadhaar as an identity does not establish nationality or confer any rights or benefits; it merely establishes who a person is to enable such individual to claim their entitlements from the government and other programs.

- **Minimalistic data collection[120] to create a Foundational ID System**

The Aadhaar's minimal data-collection approach, and the fact that it requires very little information from a person that needed to be verified to create a foundational identity system for the individual.

- **A Focus on Inclusion**

Aadhaar has also been focused on inclusion as a major objective to be achieved through its adoption. For example, before Aadhaar, the ration card was a common identification document issued at the household level which was typically in the name of the male head. This was a household identity but not an individual identity that could be used to access other services. The Aadhaar number allows women to directly receive transfers under the National Rural Employment Guarantee Scheme, and has helped many apply for SIM cards etc. Though these benefits exist, the extent of impact of Aadhaar in achieving inclusion is still to be studied.

- **Make Privacy and User Consent a True Priority**

One of the principal reasons why "legal identity for all" enjoys widespread acceptance, while "digital identity" creates debate, is the concern regarding privacy and information security. Aadhaar was introduced at a time when data protection laws were still not present in India. The concerns associated with data breaches continues to be one of the key concerns surrounding Aadhar (elaborated below).

Results and Impact

In just a few years, Aadhaar has given almost 1.2 billion individuals a nationally recognized identity that unlocks a wide variety of government and private sector services. Connection of services to Aadhaar is completely changing sectors across India. Over USD 12 Billion in financial transactions have taken place and over a billion bank accounts and mobile phones have been linked to Aadhaar.[121]A 2008 report found, for instance, that more than a third (36.7%) of subsidized grain was sold to the non-poor, and 58% was not reaching the intended

[119]Srijoni Sen, "*A Decade of Aadhaar: Lessons in implementing a foundational ID system*", (May, 2019) available at https://www.orfonline.org/research/a-decade-of-aadhaar-lessons-in-implementing-a-foundational-id-system-50464/ , accessed on November 19, 2019.
[120] Ibid
[121] OECD (2018), "*Embracing Innovation in Government: Global Trends 2018; Aadhaar. India*", available at https://www.oecd.org/gov/innovative-government/India-case-study-UAE-report-2018.pdf, accessed on November 19, 2019.

beneficiaries.[122] To this end, the government's 'JAM Trinity' scheme was proposed in the Economic Survey of 2014-15, bringing together three critical elements: Jan Dhan, Aadhaar and Mobile (JAM). Aadhaar numbers are used to biometrically identify and authenticate disadvantaged citizens (but not to determine eligibility), while mobile devices can be used to access funds transferred into Jan Dhan and other bank accounts linked to an Aadhaar number[123].

Major Concerns

Undoubtedly, Aadhaar has been as controversial as it has been innovative. The use of Aadhaar for KYC has, however, raised privacy concerns. For example, using the tool for KYC authentication provides FSPs with additional personal information about their customers, which poses a potential data privacy risk. The means of mitigating this is to only share the minimum relevant information necessary with third parties, without exposing customers' personal information, as implemented by the UIDAI.[124] Some also raise concerns about the potential for privacy leaks[125] or hacks of the Aadhaar database, which could potentially result in fraudulent use of an individual's identity. The World Economic Forum's Global Risks Report 2019, says, "*The largest (data breach) was in India, where the government ID database, Aadhaar, reportedly suffered multiple breaches that potentially compromised the records of all 1.1 billion registered citizens. It was reported in January 2018 that criminals were selling access to the database at a rate of Rs.500 for 10 minutes, while in March a leak at a state-owned utility company allowed anyone to download names and ID numbers*.[126]

The constitutionality of Aadhar was tested by the Indian Supreme Court in *Justice Puttaswamy (Retd.) and Anr. v Union of India and Ors*. In the said case, the Indian Supreme Court upheld the overall validity of the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016 (the "Aadhaar Act"). In a 4:1 verdict, the five-judge bench of the Supreme Court held that clarified that the Aadhaar Act was constitutional and did not violate the right to privacy (a fundamental right under the Indian Constitution). However, even though, the legislation itself was upheld, the Supreme Court did strike down certain provisions of the Aadhaar Act. The most relevant provision which was struck down court was Section 57 of the

[122] Frances Zelazny (2012). "*The Evolution of India's UID Program: Lessons Learned and Implications for Other Developing Countries*." (Center for Global Development Policy Paper 008. Washington, D.C, 2012) available at https://www.cgdev.org/sites/default/files/1426371_file_Zelazny_India_Case_Study_FINAL.pdf, accessed on November 19, 2019.
[123] GSMA (2017), "*Aadhaar: Inclusive by design: A look at India's national identity program and its role in the JAM trinity*", (March 2017) available at https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2017/03/gsma-aadhaar-report-270317.pdf , accessed on November 19, 2019.
[124] UIDAI "Unique Identification Authority of India" (2018), "*Enhancing Privacy of Aadhaar Holders – Implementation of Virtual ID, UID Token and Limited KYC*", available at https://uidai.gov.in/images/resource/UIDAI_Circular_11012018.pdf , accessed on November 19, 2019.
[125] Counter Currents Collective, "*Right to Privacy: Judgement Highlights and Full Judgement*", (August, 2017) available at https://countercurrents.org/2017/08/right-to-privacy-judgement-highlights-and-full-judgement , accessed on November 19, 2019.
[126] Available at http://www3.weforum.org/docs/WEF_Global_Risks_Report_2019.pdf. See also, Yogesh Sapkale, "*Aadhaar data breach largest in the world, says WEF's Global Risk Report and Avast*" (February, 2019) available at https://www.moneylife.in/article/aadhaar-data-breach-largest-in-the-world-says-wefs-global-risk-report-and-avast/56384.html , accessed on November 19, 2019.

Aadhaar Act which allowed Government entities, body corporates and individuals to use the Aadhaar number for establishing the identity of an individual for "*any purpose, pursuant to any law or contract*". Three important aspects in this respect must be noted here[127]:

a) The Supreme Court raised objections to the phrase 'any purpose' stating that it does not fulfil the proportionality test due to its wide ambit. The Supreme Court laid down that the purpose has to be *'backed by law'*.
b) It also held that the possibility of collecting and using Aadhaar numbers for authentication pursuant to a contract was disallowed since this may result in individuals being forced to give their consent in the form of a contract for an unjustified purpose. The Supreme Court laid down that the contract has to be '*backed by law*'.
c) Private entities are not permitted to use Aadhaar numbers for the purpose of authentication, on the basis of a contract with the concerned individual, since it would enable commercial exploitation of an individual's biometric and demographic information by private entities. This effectively prevents companies from using Aadhaar based e-KYC authentication of an individual's identity, which was primarily the way in which many companies complied with the relevant know your customer (KYC) requirements.

Further, to the decision, in January 2019, the Indian government made amendments to the Aadhaar Act under Aadhaar and Other Laws (Amendment) Act, 2019 and the Aadhaar (Pricing of Aadhaar Authentication Services) Regulations, 2019. Through these legislative changes, the Indian Parliament provided for the use of Aadhaar number for KYC authentication on voluntary basis under the Telegraph Act, 1885, and the Prevention of Money Laundering Act, 2002. The amendment and the regulations allow voluntary use of Aadhaar number for authentication and identity proof in opening bank accounts and procuring mobile phone connections. However, in November 2019, a fresh public interest litigation has been filed where in the validity of the 2019 legislative developments have been challenged on various grounds including that they are violative of fundamental rights of privacy, equality and freedom of speech and expression. The Indian Supreme Court has ruled that the government and the UIDAI must respond to a petition and the case is currently pending before the court.

The results and impact of Aadhaar are poised to expand beyond the borders of India. Despite the ongoing controversies, other countries are interested in potentially implementing similar identity programs and the underlying technology.

8.2 Estonia

Estonia is one of the most digitally integrated nations in the world and is known for pioneering digital governance. This digital integration in Estonia is enabled by a strong legal and regulatory

[127] Namita Viswanath , Savithran Ramesh, "*India: The Supreme Court's Aadhaar Judgement And The Right To Privacy*", available at http://www.mondaq.com/india/x/744522/Data+Protection+Privacy/The+Supreme+Courts+Aadhaar+Judgement+And+The+Right+To+Privacy accessed on December 23,2019

framework supported by robust technology. The key to accessing all public and private services in Estonia is the *Estonian Digital Identity card* launched in 2002.

Concept

On the front of Digital ID and e-KYC, Estonia has developed a comprehensive system for electronic identification, authentication and digital signature. Estonia has three recognized identification methods- (i) Electronic ID, the Digital ID and the Mobile ID. Fundamentally the three streams are the same with the same identity requirements. Though biometrics are often discussed in conjunction with Digital ID systems, they are not synonymous as Estonia's ID, does not use biometrics, but instead employs a chip card (also called a smart card) and a PIN.

The Estonian ID System is leveraged three ways:

- ID Card: This card contains the general components of a legal photo ID. In addition to the legal photo ID components, a chip on the card carries embedded files, and using public key encryption, it can be used as definitive proof of identity in the electronic environment.[128]
- Mobile ID: Mobile ID allows people to use a mobile phone as a form of secure Digital ID. Like the ID-card, it can be used to access secure e-services and digitally sign documents but has the added feature of not requiring a card reader. The system is based on a special Mobile ID SIM card, which the customer must request from the mobile phone operator. [129]
- Smart ID: Smart-ID works as an identification solution via a mobile application and thus does not require a SIM card in the mobile smart device.[130]

Mandatory Requirement

It is mandatory for every Estonian ***citizen*** above the age of 15 and every European citizen residing in Estonia to obtain this identity card. It serves the twin function of giving proof of identification and establishing one's identity specifically in the electronic environment, including serving as one's digital signature. Whether you decide to use a physical ID card, a mobile ID, or a smart ID, your credential has two digital certificates—one for authentication of the user and one for digitally signing documents. Access to these certificates on the card or mobile device is secured by a PIN. So even if the card or mobile device is lost, it cannot be used by another user without having the PIN.

Lessons from the Estonia Experience

[128] See E-Estonia ID Card Description: E-Estonia.com, "*E-identity: id-card*", available at https://e-estonia.com/solutions/e-identity/id-card , accessed on November 19, 2019.
[129] See E-Estonia Mobile ID Description: E-Estonia.com, "*E-identity: mobile-id*", available at https://e-estonia.com/solutions/e-identity/mobile-id. , accessed on November 19, 2019.
[130] See E-Estonia Smart ID Description: E-Estonia.com, "*E-identity: smart-id*", available at https://e-estonia.com/solutions/e-identity/smart-id. , accessed on November 19, 2019.

In 2002, the government introduced eID-cards to support online transactions. At that time 57 percent of Estonian Internet users were using internet banking. This trust in e-banking helped to seed the take-up of eID verification system which would enable government services to work online. Some examples of how it is regularly used in Estonia:

- legal travel ID for Estonian citizens travelling within the EU
- national health insurance card
- proof of identification when logging into bank accounts
- for digital signatures
- for i-Voting
- to check medical records, submit tax claims, etc.
- to use e-Prescriptions

Results and Impact

Unlike India, where the impact of Aadhar largely gets determined on the volume of the data and sheer size of the population, Estonia has seen the eIDs penetrate to the very core of the population. What also stands out in the case of Estonia is that issuing of eID takes less than an hour as pre-produced cards are used to generate IDs. Estonia prides itself of having been able to completely digitize the government as early as in 2000 giving it enough time to implement and test the national ID system

Concerns[131]

In August 2017, a researcher with the Centre for Research on Cryptography and Security at Masaryk University notified Estonia of a security vulnerability on the chips used in the Estonian ID card. According to the analysis by the research group, the vulnerability, internationally known as ROCA (Return of the Coppersmith Attack), affected RSA cryptographic keypair generation in chips produced by one of the leading manufacturers, Infineon – the supplier for the Estonian eID Card. Theoretically, the security vulnerability could have allowed the private key (which is used for authentication and signing) to be calculated from the public key – in theory, making it possible to clone the victim's cryptographic keys and use them for authentication, sign or decrypt documents even without being in physical possession of the card. In Estonia, all the eID cards (800 000) issued since autumn 2014 were at risk.[132] Ultimately, a new solution – based on elliptic curve cryptography (ECC) instead of an RSA library – was available before Estonia needed to suspend the affected certificates.[133]Nonetheless, the crisis management team made the decision early on to be transparent in its public communication. The strategy of Estonia in overcoming this issue was allowing cardholders to update the certificates remotely. After the suspension of

[131] Republic of Estonia's Information system authority, "*ROCA vulnerability and eID: Lessons learned*", available at https://www.ria.ee/sites/default/files/content-editors/kuberturve/roca-vulnerability-and-eid-lessons-learned.pdf , accessed on November 19, 2019.
[132] E-Estonia, "*What we learned from the eID card security risk*" (May, 2018) available at https://e-estonia.com/card-security-risk/ , accessed November 19, 2019.
[133] Republic of Estonia's Information system authority, "*ROCA vulnerability and eID: Lessons learned*", available at https://www.ria.ee/sites/default/files/content-editors/kuberturve/roca-vulnerability-and-eid-lessons-learned.pdf , accessed on November 19, 2019.

the certificates of the cards with vulnerable chips on 3 November 2017, 94% of the eID cards which are electronically used have been renewed. This experience evidences how risk management, continuity planning, and openness are the keywords in overcoming security threats.

8.3 Nigeria

The cornerstone of the digital identification initiative in Nigeria, a country with a population of nearly 190 million people is the National Identity Management Commission (NIMC), that is the parent organization of the National Identification Number (NIN)[134].

Concept

The NIN is a set of numbers assigned to an individual upon successful enrolment. Every citizen or legal resident above the age of 16 is eligible to enroll for the NIN. For the purpose of enrolling, the citizen or legal resident is required to approach the enrollment centre with their Bank Verification Number (BVN) and other supporting documents (like old National ID Card, Driver's License, Voter's card (temporary or permanent), passport, birth certificate, NHIS ID card, tax clearance certificate etc.)[135]The BVN is a unique identification number initiative that was launched in 2014 by the Central Bank of Nigeria. It uses and stores biometric information to identify and verify customers who have accounts at any Nigerian FI, as well as track their credit histories in order to prevent identity theft and reduce the incidence of non-performing loans. Identity captured by the BVN system consists of "442" fingerprints — two sets of four fingers and two thumbs — signature and facial recognition (iris and face)[136].

The enrolment consists of the recording of an individual's demographic data and capture of ten (10) fingerprints, head-to-shoulder facial picture and a digital signature, which are all used to cross-check data in the National Identity Database to confirm that there is no previous entry of the same data[137]. The NIN can be used for multiple purposes, such as obtaining a National e-ID, passport, driver's license, permanent voters' card and accessing services such as opening personal bank accounts, participating in the National Health Insurance Scheme and to pay taxes[138].

[134]World Bank Group (2018), *"G20 Digital Identity Onboarding"*, available at https://www.gpfi.org/sites/gpfi/files/documents/G20_Digital_Identity_Onboarding.pdf accessed on November 12,2019
[135] NIMC, "*How to enroll Adults*", available at https://www.nimc.gov.ng/how-to-enrol-adults/ accessed on November 19, 2019.
[136]https://www.afi-global.org/sites/default/files/publications/2019-03/KYC-Innovations-Financial-Inclusion-Integrity-Selected-AFI-Member-Countries.pdf
[137] World Bank Group (2018), *"G20 Digital Identity Onboarding"*, available at https://www.gpfi.org/sites/gpfi/files/documents/G20_Digital_Identity_Onboarding.pdf accessed on November 12 ,2019.
[138] Ibid

After the NIN has been obtained by an individual, a card comes next as an additional token. The National Electronic Identity Card (e-ID card) is a chip-based card with multiple functions. It is important to note that:

- The NIN can be used on its own for digital identity verification without the e-ID card.
- The e-ID card cannot be used on its own for digital identity verification without the NIN first being stored within its chip.
- The number printed on the e-ID card is not the NIN but the PAN used for accessing the card's payment feature once activated.

The e-ID Card can be leveraged as[139]:

- Travel Document with ICAO standards
- Electronic ID - This offers strong authentication and digital signature. The micro-controller securely holds the National Identification Number (NIN), the holders address, name, and other details. This is also a key tool for banks for customer on-boarding procedures known as KYC.
- Biometric eID - The card contains 10 fingerprints captured during the registration procedure. The card supports biometric identification through the use of fingerprinting. It uses the "**match on card**" method, which involves making a fingerprint comparison on the card rather than on the reader. As the biometric data never leave the card, the interception of data during transfer to a reader is impossible.
- Payment card - The payment application turns the Nigerian national ID card into a tool for payments or can be used at ATMs or for transfers. It will offer millions of Nigerians – the majority of whom have never had access to a banking service – with the security, convenience, and reliability of electronic payments with 13 applications, including Mastercard's prepaid payment technology.

Mandatory

With effect from 1st January 2019 the use of the National ID number has become mandatory by law. As of October 2019, government Agencies like the Central Bank of Nigeria, Nigerian Immigration Services, Pension Commission, Joint Admissions and Matriculation Board, Nigerian Communication Commission etc. are currently in compliance with NIMC by making the NIN a prerequisite for transactions and accessing services they provide.[140]

[139]Gemalto, "*Nigerian national ID program: an ambitious initiative",* available at https://www.gemalto.com/govt/customer-cases/nigeria-eid accessed on November 19,2019
[140] NIMC (2019), *"Nigerians Embrace the Mandatory Use of NIN*", available at https://www.nimc.gov.ng/nigerians-embrace-the-mandatory-use-of-nin/ accessed on November 19, 2019

Lessons Learnt from Nigeria Experience

The establishment of a centralized biometric database has proven successful in assisting Nigeria to overcome identity barriers to financial inclusion. It alleviates much of the due diligence burden for existing customers when using accounts or opening new ones, and facilitates onboarding with a set of fingerprints. However, key to the success of the system itself has been the collaboration between the CBN and the private sector. Legal certainty is critical in embarking on eID and e-KYC programs, especially if harmonization and integration of various identity databases is required as part of (creating) a national ID database. The regulatory positions adopted by the Nigerian government has paved way for the adoption of the NIN.

Benefits

The full-fledged implementation of the NIN system will have major benefits including more convenient access to financial services, eliminate ghost workers from payrolls, provide the residents better access to entitlements and improve the electoral process amongst others. However, these factors need further testing since the NIN is yet to be fully adopted among the residents.

Results/Impact

There are initiatives to integrate the NIN, e-ID and BVN to achieve the harmonization objective and facilitate e-government and public-sector applications. However, the results and benefits thereto still require more adoption among the local population to provide more data in this respect.

Concerns

Despite the technologically layered system, Nigeria's identity system is seriously lacking in adoption among the local public. Core challenges also include a lack of rural identification centers and an inequitable regulatory system[141]. In relation to the adoption of BVN, some of the major concerns include[142]:

- The BVN requirement for physical enrolment limits coverage to predominantly urban regions, implying a costly barrier to citizens in remote/rural regions.
- Low public awareness and confusion around the program has limited the uptake of the BVN.
- Patriarchal practices have hindered female access to BVN enrolment in Northern Nigeria

[141] World Bank Group (2018), *"G20 Digital Identity Onboarding"*, available at https://www.gpfi.org/sites/gpfi/files/documents/G20_Digital_Identity_Onboarding.pdf accessed on November 12, 2019.

[142] Alliance for Financial Inclusion, "*KYC Innovations, Financial Inclusion and Integrity In Selected AFI Member Countries*", available at https://www.afi-global.org/sites/default/files/publications/2019-03/KYC-Innovations-Financial-Inclusion-Integrity-Selected-AFI-Member-Countries.pdf accessed on November 12,2019

- Slow integration of BVN data into the national ID database has inhibited the effectiveness of BVN verification.

Each of the above, may have had consequent effect on the adoption of NIN as well. As per reports, less than 20% Nigerians are registered in the National Identity Database of the NIMC. Furthermore, over 700,000 are yet to collect their e-ID cards.[143] One of the major factors for non-collection is said to be the change of location of enrollees from the location where they initially registered or the change in phone numbers provided at the point of enrolment into the National Identity Database.

9. EXPERIENCE FROM ARAB COUNTRIES

9.1 Assessment of status of Digital Identity and e-KYC schemes across AMF member state

With the purpose of analyzing and understanding the current state of digital identity system and the consequent developments surrounding e-KYC across the Arab countries, a survey was initiated with the member countries of AMF. As a part of the survey, a detailed questionnaire relating to the current status of Digital ID system as well as e-KYC programmes was prepared and circulated to the 22 member countries. Financial sector regulatory authorities in 18 countries submitted their response. With a few countries submitting responses from more than one financial regulator, a total of 22 responses were received from the member states. The list of the member countries and their respective agencies that responded to the survey is included in Annex III and the sample survey questions is attached as Annex IV.

Findings[144]

The results of the survey have revealed that most respondents have adopted a national ID system in their country. Among the 18 respondent countries only Yemen and Tunisia have specified that they are still to implement a government issued national identity system. In both instances, the government has expressed its keen intention to implement such a system. However, Yemen has expressed the political situation as its current major constraint to achieve this objective, Tunisia has confirmed that under its proposed national strategic plan "*Tunisie Digitale 2020*", such a Digital ID system is being proposed for corporates and citizens. Though most countries have managed to adopt a national ID system, as per the survey responses, it seems that only a few of these countries have implemented a Digital ID system.

[143] "*Nigeria: National ID Card Is Free, but Only 19% Nigerians Are Registered – Official*" available at https://allafrica.com/stories/201910210021.html accessed on November 21, 2019.

[144] While tabulating the responses, we have analyzed the responses provided by the member nations and consolidated our findings based on position of each member country for the purposes of this report. However, where we have encountered differing views from two separate organizations of a single member country, we have considered the response provided by the Central Bank of such country to be reference response for the purposes of this report.

FIGURE 7 – Existence of National ID

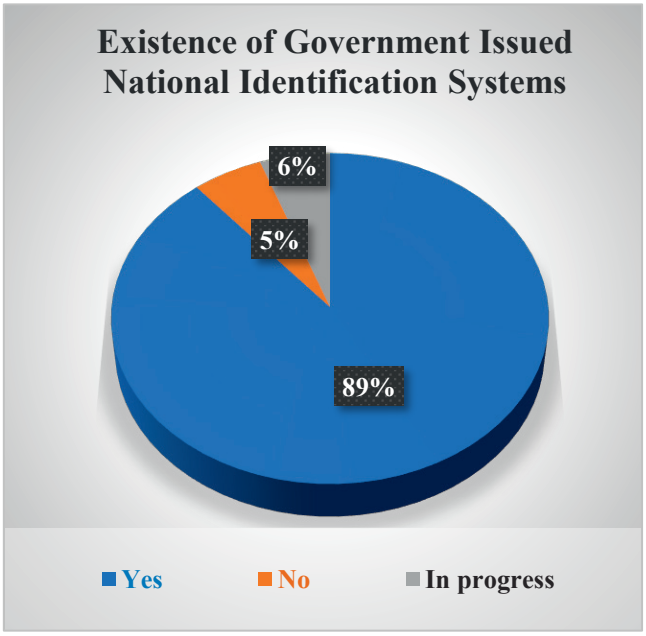


FIGURE 8 – Implementation of Digital ID

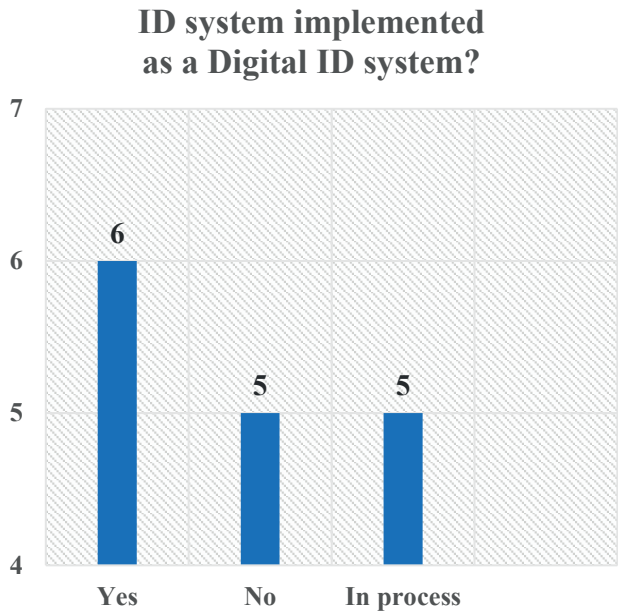
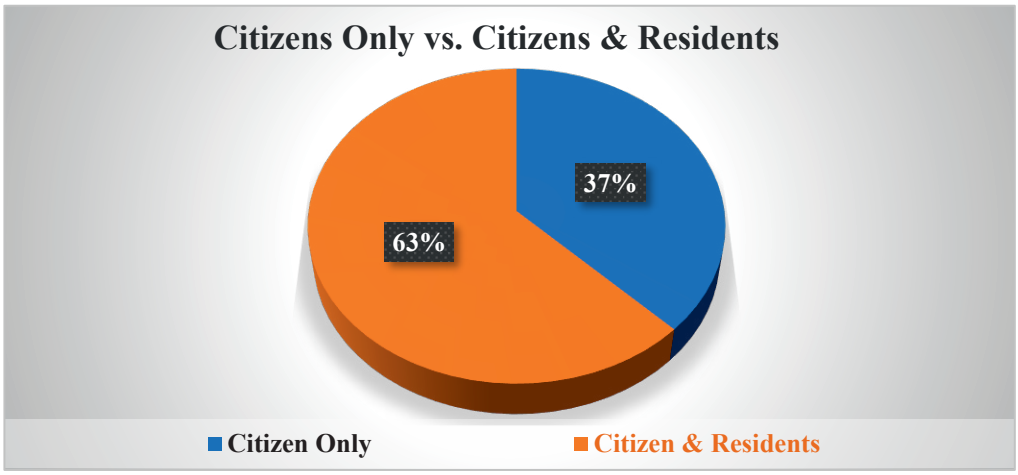


FIGURE 9 – Catering to Citizens vs. Residents



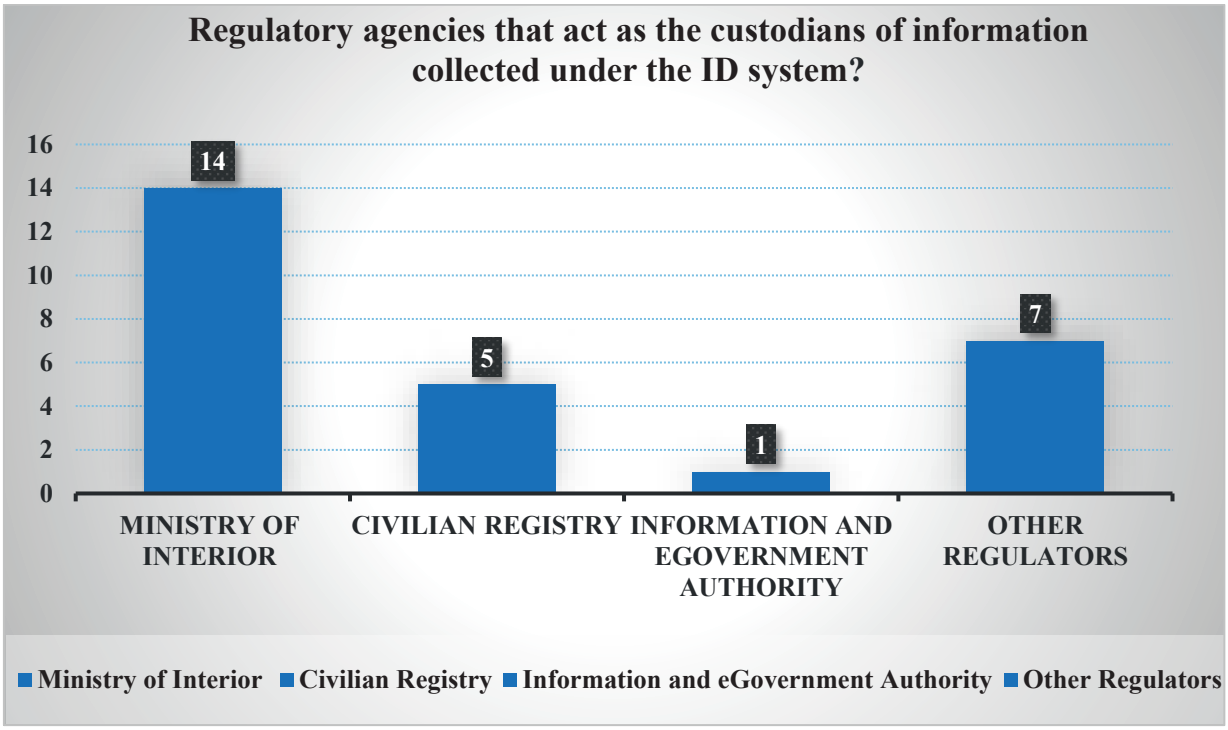
The excessive migrations between the countries due to various factors (including civil unrest and wars) and the existence of a large expat workforce (particularly in many countries in the Middle East region) has resulted in a large part of the local population in these countries being consisting of non-citizens. Despite such a diversity in the local population, in many countries the identity systems continue to cater only to citizens.

In any event, all countries have other functional IDs like driver's license, travel documents, tax IDs *etc.* be used by the local population, irrespective of whether they have a national ID system or not. It may be highlighted, that many of them are collecting. Except for seven (7) respondent countries, all the remaining member countries have confirmed that they collect biometric information biometric information of the individuals during the data collection stage – most of them collecting fingerprint as the biometric information collected.

National Data Base & Custodian

Considering the nature of sensitive information collected, it is pertinent to understand which regulatory agency will be custodian of such information and the current scheme of development in management of personal data in such countries – with a special focus to such data protection laws. More often than not the main custodian of such information in the 22 responses provided by the 18 respondents is the Member State's Ministry of Interior. Nevertheless, it may be noted that the information may be collected at other government departments as well. Most countries appear to have more than one authority which may act as custodian of such information. For example, in its response Iraq has mentioned that the Ministry of Interior, Ministry of Trade, Independent High Electoral Commission may act as custodian. Similarly, Tunisia has mentioned that the custodian of the information is depending on the functionality of the identity. For example, the Technical and Scientific Police may have information relating to the passport while the Ministry of Transportation may have information relating to Driver's License.

FIGURE 10 – Custodians of Information under the ID system



The other regulators include Palestine's Ministry Finance and Planning, Oman's Ministry of Technology and Communications, United Arab Emirates' Federal Authority for Identity and Citizenship, Tunisia's Technical and Scientific Police, Iraq's Ministry of Trade and Independent high electoral commission, Bahrain's Information and eGovernment Authority (IGA), Mauritania's National Agency of the register of the Population and Secured Title and Saudi Arabia's Ministry of Commerce and Investment (in relation to corporate entities).

Except for three nations, all other nations have a law governing the use of data included in their national database. Some major aspects relating to such databases and its relevance in financial sector is included below:

FIGURE 11 – Capturing Financial Transactions Data (like credit history and credit rating) via National Database

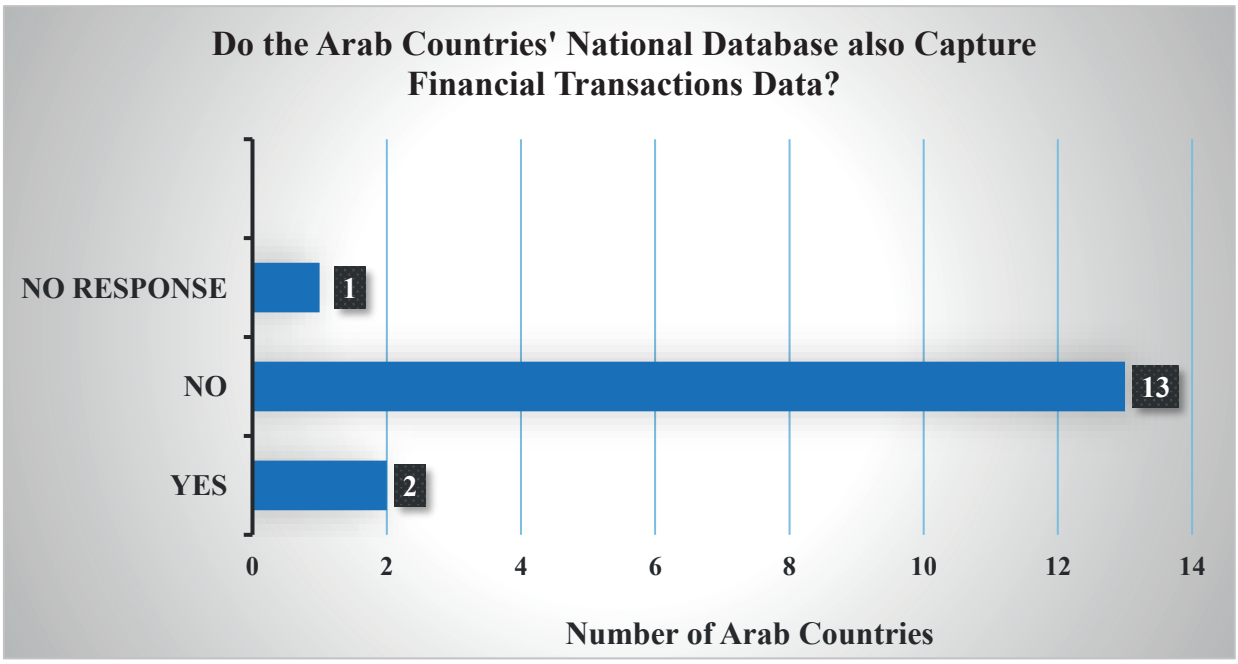


FIGURE 12 – Access of Financial Institutions to Database

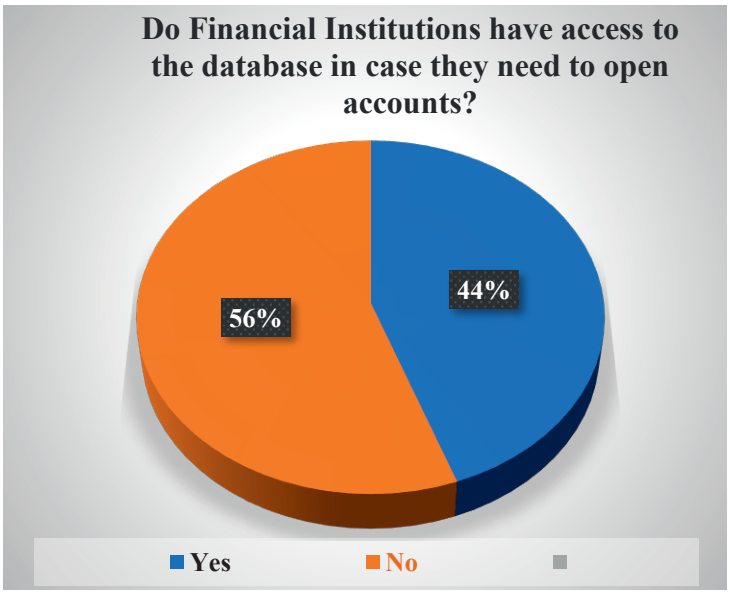
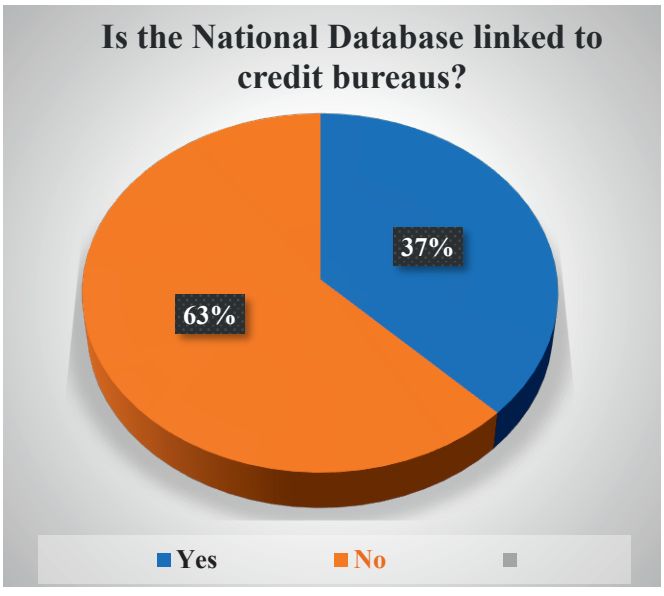


FIGURE 13 – Linking National Database to Credit Bureaus



Data Protection

The regulatory developments surrounding data protection is at varied stages. All respondent member countries have recognized the importance of data protection, not all are at the same stage of regulatory growth in this respect. Few nations have explicitly identified specialized laws which relate to personal data and data privacy while others depend on their other generic rules and regulations to this end. Some key legislations in this respect include:

- Lebanon - Law no. 81 of October 10 2018 (on Electronic Transactions and Personal Data) and Banque du Liban Basic Decision no. 12872 of September 13 2018 (on GDPR);
- Mauritania - Law 2017- 020 on Data Protection;
- Bahrain - Law no. (30) of 2018 regarding Issuing the Personal Data Protecting Law;
- Morocco - Law 09-08 on the Protection of Individuals with regard to the Processing of Personal Data;
- Algeria - Law no. 07-18 that dated June 10 2018 related to Protecting Person when Dealing with Personal Data;
- Tunisia - Act no. 2004 – 63 of July 27 2004, on the Protection of Personal Data.[145]

Financial Inclusion

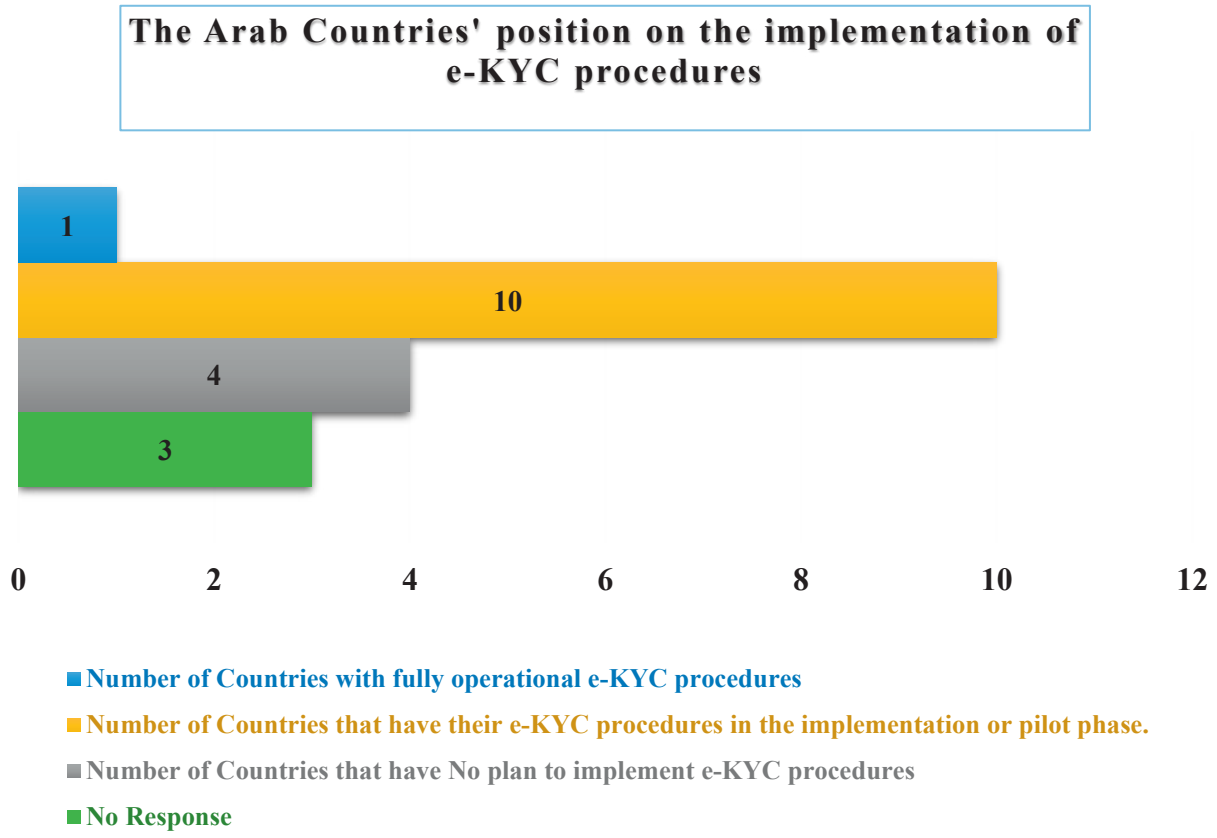
Though countries have implemented some form of ID system – foundational or functional, the data the percentage of population covered by an ID system has not been provided. Therefore, at this juncture, except for the four countries[146] that have provided information around this, the extent of financial inclusion achieved by each individual country is difficult to ascertain.

Customer Identification & Verification

Based in the responses from the surveys, it is noted that most countries are still following physical KYC structure with face-to-face interactions (or equivalent) and physical documents being the basis for client on-boarding and verification models. In compliance with the AML/CFT regulations and standards globally, banks and FIs in most countries adopting clear procedures for account opening and conduct due diligence measures, such as verifying the identity of their permanent and transient customers, whether resident or non-resident, and identifying the nature of their business, understanding the ownership structure and/or control of the concerned legal entity, understanding the purpose and nature of the business relationship and/or the account opening, identifying the beneficial owner and the source of funds, and monitoring operations on a continuous basis[147]. Countries also have Tiered (or Simplified) CDD and Enhanced CDD models as well. Bahrain is the sole country with a fully operational e-KYC structure and the same has been discussed in detail below, while UAE has very recently launched this initiative.

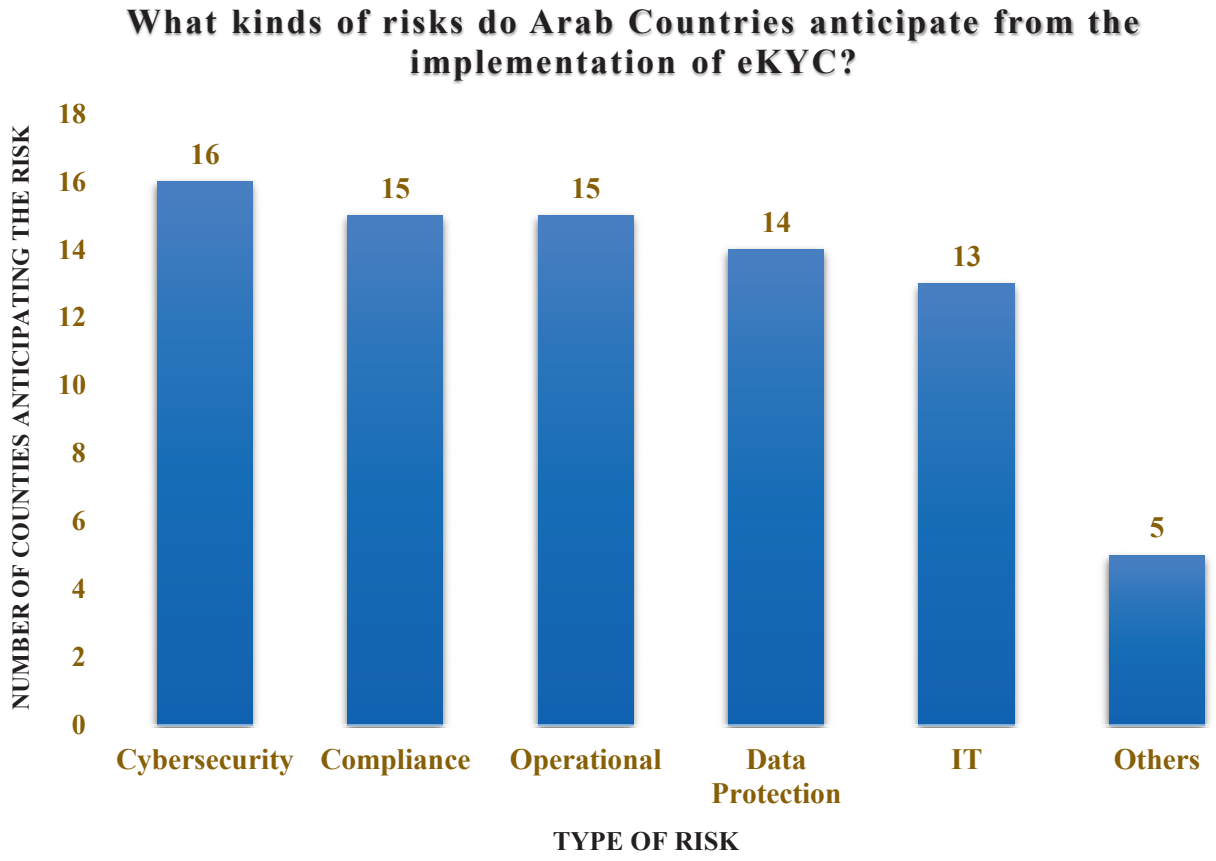
[145] As per the response, Tunisia was one of the first Arab country to ratify the Convention no. 2018 of the Council of Europe via the organic Law No. 2017-42 of May 30, 2017, approving the accession of the Republic of Tunisia to Convention No. 108 of the Council of Europe for the Protection of Individuals with regard to the automated processing of personal data and its Additional Protocol No. 181 concerning supervisory authorities and cross border data flows.
[146] As per the response by UAE, Jordan and Bahrain 100% of the residents and citizens of the local population is covered by an identity system. Oman has specified that 99.5% of the population have been covered by a identity system. Bahrain has been able to specify the inclusion by a gender basis also - Male 50.6% / Female 49.4%
[147] Survey response submitted by Banque Du Liban.

FIGURE 14 – Implementation of e-KYC in Arab Countries



Though many countries have no e-KYC system (fully operational or in pilot phase), it is promising to note that some of them have confirmed that the government agencies have already recognized the need for such systems and specified that they are evaluating various studies to evaluate the mechanism to be utilized for implementation of such systems. Many countries have also identified that they are exploring implementation of the e-KYC system utilizing blockchain technologies. Countries are also evaluating the various technologies through regulatory sandboxes. It is interesting to note that between the 22 respondent regulatory agencies perception of the risks that may be encountered as a part of such an e-KYC implementation are varied in nature.

FIGURE 15 – Type of Risks Anticipated by Arab Countries



Due to the nascent stage of a nationalized ID systems, there is still significant legwork to be undertaken in this respect. However, the efforts of the countries that have initiated the relevant processes is commendable. Specifically, the experience of UAE and Bahrain may be further reviewed and studies for the benefit of all member countries.

9.2 Case Studies

The UAE Experience

UAE Pass is the nation's first single mobile identity that can be used to assess an array of services across various sectors, as well as eventually allowing users to digitally sign documents. Launched at GITEX 2018, it aims to serve as a single digital identity for local and federal entities, while maintaining a high level of security assurance and seamless user experience. UAE PASS is a fundamental enabler for digital transformation initiatives, and a contributor towards achieving the goals of UAE Vision 2021, UAE Centennial 2071, and sustainable development. At present, citizens and residents with a valid Emirates ID card are currently the only users eligible for UAE PASS.[148]

Currently, many banks have developed or are developing their own non-face-to-face on-boarding services to allow customers to open a simple bank account without the need of physical presence and through the use of biometric technology and a mobile app. In September 2019, the Central Bank of UAE declared its decision to adopt 'UAE PASS' initiative and announced that it was allowing banks and other financial firms to use the app to check customers' identities when they were opening bank accounts or conducting transactions as individuals or representatives of corporates.[149] It may be highlighted, that the UAE PASS is still in its initial stages and banks will still be able to carry out KYC procedures in other ways. The use of the UAE PASS is optional, but it is likely to mean that clients will no longer have to supply a hard copy of their Emirates identification card.

In the UAE, the government is planning to introduce a digital vault that stores all digitized and digitally signed documents by the issuer. Through the UAE PASS as a Digital ID, the digital vault can be accessed by the owner (either individual or a company) and digital documents can be shared with a third party with the approval from the owner. This provides the golden source data and will form the foundation of the future e-KYC platform. Through the authentication of UAE PASS, owners can grant the approval to send the required electronic documents to the banks.[150]

To avoid any misuse of information, measures include very stringent authentication mechanism, robust audit trail, strong cyber and information security controls have been implemented along with regular reviews by dedicated teams.

---

[148]Mohap, "*UAEPASS: User Guide; Version 1.0*", available athttps://www.mohap.gov.ae/Documents/Banner/UAEPASS_User_Guide_1.0.pdf, accessed on November 19, 2019.

[149] Nada El Sawy (2019), "*Financial institutions gear up to integrate UAE Pass*", available at https://www.thenational.ae/business/money/financial-institutions-gear-up-to-integrate-uae-pass-1.915602 , accessed on November 19, 2019.

[150] Survey Response of Central Bank of UAE.

The Bahrain Experience

Bahrain's Electronic Network for Financial Transactions (BENEFIT), a company owned by 13 banks, is presently in the process of implementing the world's first national KYC Utility that incorporates blockchain technology[151]. Through the letter dated March 7,2019, the Bahrain Central Bank directed all banks and licensed institutions to the national e-KYC project, thus making it an e-KYC program supported by the public sector. The project, funded by BENEFIT, is intended to provide an advanced state of the art electronic platform and a database for FIs to authenticate the identities of their clients and validate their information before granting financial services. The project also aspires to help financial technology companies offering financial and banking products using online applications, and facilitate the launch of their products and services.[152]

FIs that subscribe to BENEFIT can instantly complete KYC and AML/CFT compliance procedures when onboarding new individual and corporate customers through the e-KYC hub and rules engine utilizing blockchain. The centralization of customer data removes the need for duplicate requests for information, enabling FIs to onboard new customers and products swiftly and seamlessly. The elimination of manual processes reduces costs and improves operational efficiencies, ultimately optimizing customer experiences.[153]

The Bahrain Information and eGovernment Authority acts as the custodian of the collected information which is shared only with the permission of the owner thereof.[154] The data may be accessed by Central Bank Licensees including banks, financial companies, microfinance institutions, crowdfunding platform operators, and some car dealers can access customer liabilities database.

The e-KYC system is currently at its initial stage where all the FIs have access to the e-KYC platform for retail customers. The platform has been launched and is live since April 30, 2019. The e-KYC platform is linked to the Information and e-Government database to authenticate customers through national eKey (digital identity) or biometric fingerprint and retrieve KYC data. Phase 2 of the project is working in process to include API's for seamless digital on-boarding and integration with the FIs core systems and digital channels. It will also introduce identity verification through facial recognition, customer self-onboarding, maintenance of existing customers KYC records as well as integration with blockchain. Phase 3 of the project will be launched to allow corporates clients to be on-boarded utilizing the same platform by integrating with Ministry of Industry, Commerce, and Tourism and other data providers. The

[151] Fenergo (2019), "*Fenergo Partners with BENEFIT to Create National eKYC Utility in Bahrain*" (PR Newswire, May 2019) available at https://www.prnewswire.com/ae/news-releases/fenergo-partners-with-benefit-to-create-national-ekyc-utility-in-bahrain-850186014.html , accessed on November 19, 2019.
[152] Bahrain News Agency (2019), "*BENEFIT launches first eKYC project in Arab World*", (February, 2019) available at https://www.bna.bh/en/BENEFITlaunchesfirsteKYCProjectinArabWorld.aspx?cms=q8FmFJgiscL2fwIzON1%2BDnjwKS5lgF8vEgrzLWh3IgA%3D , accessed on November 19, 2019.
[153] Ibid
[154] Survey Response of Central Bank of Bahrain.

Central Bank of Bahrain, Information & e-Government Authority and Ministry of Industry, Commerce and Tourism would be the main data providers for the e-KYC platform.

As a precautionary measure for misuse of information, the following measures have been included:

- Digital authentication of customer identity using National eKey, biometric fingerprint and facial recognition.
- Customer consent to retrieve and share KYC data and documents
- Maker checker process for customer on-boarding which involves at least two staff in any FI to complete customer on-boarding.
- Maker checker process to create any user to the platform
- Regular audit logs shared with the regulator
- Immutable KYC records on the blockchain
- The platform operator has no access to KYC records

10. Range of Actions for Governments of the Arab countries

Based on an analysis and review of the international developments globally, the experience of other jurisdictions during the development of Digital ID systems as well as the findings of the regional developments, a range of action items may be developed for the various players – the Governments, the pan-national organisations as well as the private players.

- **Establishment of a unique, legal, interoperable, Digital ID with an 'identity first' focus that collects minimal information for creation of an identity**

Countries should establish a Digital ID framework at the national level, that may be utilized to identify citizens and residents in the country. Such an identity must capable of creating a unique identification for each individual. The identity system must be interoperable and meet the desired levels of assurance resulting in the creation of a "reliable, independent" source of customer identification.

Each regulator may at its option determine the mechanism that it utilizes during each segment / component of identity lifecycle. For creation of a Digital ID, countries may consider working with private sector entities under a public-private partnership model, outsourcing model, or as the identity service providers. Such engagement may not just be limited to utilizing the services of private sector as a technology provider, but also utilizing the private sector solutions during the identity enrollment process (as agents at local kiosk centers etc.) or as funding partners.

Governments may determine the particular attributes / authenticators that they would prefer to be collected from individual, taking into the account, the beliefs and practices of the jurisdiction. However, the approach should be limited to collecting the 'minimal' amount of information necessary to identify an individual, having regard to risks associated with Digital ID systems – including those associated with cyber security and identity theft. It is also material to create a mechanism for the individuals to control and update the information to maintain accurate and complete information about the individual.

From the review of the survey responses, it is clear that though most countries have managed to adopt a national ID system, most of them are not implemented as Digital ID. It may be highlighted that the identity itself – may be *a foundational identity or functional identity* – the significance thereof, for financial transactions is the reliability or credibility of such an identity system.

- **Support the Digital ID Framework by adoption of policies, rules and regulations addressing the risks or concerns associated with the use of Digital ID**

The implementation of the Digital ID framework should be supported through the legislations and policies including a strong and robust data protection law, cyber security framework, laws governing the ***mandatory*** use of the Digital ID, laws governing digital signatures and other risks involved thereto.

When supported by a national legislation or policy, the national ID frameworks have better acceptance and hence it is advisable to consider a national level law associated with the identity creation. However, the countries may consider that the adoption be undertaken in a phased manner – commencing with specific sectors – like the financial sector.

It is clear from the survey results that the countries have identified the various types of risks associated with the creation of the Digital ID as well as its use (risks identified being cybersecurity concerns, data protection and operational risks). The responses evidence that the member countries are implementing legislations to support the protection of personal data, a major risk associated with digitized identity system. Similarly, there are developments which give validity and enforceability to digital contracts/ transaction through the various legislations in this respect.

- **Establish a 'risk-based' CDD regime which balances the AML/CFT objective and financial inclusion objectives**

While implementing a CDD regime, countries should cater to the recommendations provided by FATF and other international organization relating to CDD and target compliance with AML/CFT obligations. The countries may implement measures to mandate a Tiered KYC regime to cater to the risk-based approach proposed under FATF recommendations. The compliance with the AML/CFT best standards would assist in safeguarding market integrity and financial stability.

For example, in Saudi Arabia, all customers must identify and verified during financial transactions. However, the level of KYC whether simplified due diligence, basic due diligence, or enhanced due diligence is based on the customer risk.

While implementing the KYC regime, countries should create balance compliance with the AMF/CFT commitments internationally and the objective of financial inclusion. Disproportionate KYC requirements for marginalized groups may affect accomplishment of the financial inclusion objective.

Countries with a high-degree of Digital ID coverage should focus on building up the capability of their identity systems to enable relying parties like FIs. Nevertheless, the approach the country adopts should depend on the current scope and capabilities of its identification infrastructure, as well as the timeframe in which a solution is sought.

- **Prioritize integrity of user data and facilitate processes and procedures for minimalistic sharing of the information during CDD**

The usefulness of information collected is relevant only when the information is complete and accurate. Therefore, individuals must be able to update information regularly. The sharing of information should also be consent -based and the individual must at all events have an oversight on the manner in which the information is shared. Among the Arab countries, the consent – based approach has been adopted in the e-KYC programmes which have been implemented in UAE

and Bahrain. Egypt has confirmed that the importance of customer / user involvement in updating and amending information has been noted by it and the same is being included as a part of its upcoming KYC initiative.

Further, in the interest of protection of user data, the KYC regime should not provide FSPs access to all information held in relation to an individual. Information shared should be limited to those required for the purposes of undertaking CDD only.

- **Create benchmarks and standards for use of any 'non-government' backed identity systems**

In certain instances, the FSPs may utilize Digital ID systems which are not necessarily '***government backed***'. However, it must be considered that international guidelines require reliance on 'reliable' identification source. Governments may explicitly deem a Digital ID system to be appropriate for use in CDD by issuing regulations or providing guidance to regulated entities, either permitting or requiring regulated entities to use the Digital ID system(s) for certain aspects of CDD.

Countries should consider if such identity system, should be permissible for use for undertaking CDD and, if so permitted, mandate the 'open standards' which may have to be evidenced by such system. The adoption of such parameters would be necessary to safeguard the sanctity of the information utilized from such systems. In any event, the systems which are adopted should thus be technologically strong and robust and protect user privacy.

- **Ensure complete, accurate and better integrated databases that can be utilized for customer identification and verification purposes**

Integration and harmonization of the databases and legacy systems reduces siloed data and costs associated with KYC. Data related to individuals could exist across various databases including social security, voters, driving, mobile banking etc. These may be considered nationally and inter-departmental collaboration is a major element to facilitate this.

In the Arab nations, most identity systems which are prevalent are functional identities and therefore the information is spread across various government departments and authorities. Pooling of such information as well centralizing the data would result in better results in KYC.

As a long-term objective, countries may consider creating centralized KYC repository which hold centralized, verified identity particulars of persons or businesses that may expedite the KYC process.

- **Implement a Strong Governance Model to Manage the Digital ID and CDD regime**

To cater to the various concerns and risks arising out of the Digital ID regime, a strong system for governance and oversight of the Digital ID system should be implemented by the countries. Such a supervisory function is necessary for the purposes of handling any concerns or complaints by users and consumers.

- **Provide regulatory clarity, remove barriers and foster enabling regulatory environment for innovation which may provide newer solutions for CDD.**

Regulators could consider providing regulatory clarity for Fintech innovators to foster growth in the Fintech sector. Adoption of measures like regulatory sandboxes that may provide novel solutions that may facilitate CDD and KYC should be encouraged

- **Collaborate with regional and international bodies and regulators**

Cross- country interactions and collaboration would help countries who are initiating Digital ID regimes to learn from past experiences and best practices.

- **Formulate transnational frameworks for interoperability and levels of assurance being implemented across Arab countries.**

Arab countries should consider adopting a framework or standard which would address the interoperability and standards that the identity systems may be required to comply with. A guidance to this end, would ensure uniformity in the nature of adoption in the long-run, facilitate better and easier exchange of information between countries.

11. CONCLUSION

In summation, Digital ID systems can offer new possibilities for achieving sustainable development goals if they are inclusive and trustworthy. When designed appropriately, Digital ID systems can be more secure than analogue systems, with stronger, more intelligent, and more easily monitorable data protection measures, which in turn offer better guarantees of data privacy. Taking advantage of these benefits, however, requires purposeful preventative action and an ongoing commitment to identifying and mitigating potential threats. Absence of such officially authenticated identification may pose disadvantages and undermine the financial inclusion of such individuals. The inability to credibly prove one's identity does not only hinder financial inclusion but may lead to an individual's political and social exclusion. In the financial services domain, absence of a valid and officially authenticated identification renders inaccessibility to the basic yet most crucial facilities like loans, bank accounts, ATMs etc. National governments play a primary role in enacting measures to facilitate the recording of legal identity for its residents.

With increasing digitization, national governments must now focus on implementing robust and digitally enabled identification systems that can increase individual's access to financial services and more holistic representation in the digital world. Therefore, it is incumbent that countries establish a reliable supervisory model to introduce efficient Digital ID systems.

However, such implementation of systems on a nation-wide scale has its own challenges, namely:

- the risk of exclusion
- political concerns
- cost implications
- data privacy, protection and security

The regulators and international agencies may need to recognize and recommend standards which may be adopted and the systems that need to be implemented in this respect.

Essentially, for operationalizing financial integrity for FIs, it is not only desirable but, in most cases, mandatory to understand and officially record the identity of their customers. A financial system in which customers are anonymous is one that can easily be abused and corrupted. To foster financial inclusion, tiered and electronic KYC regime may be utilized by the FIs to gain foresight of their customer's objectives, needs and circumstances or be prepared to say that the client has refused to identify those objectives.

Annex I
Risk Factors – ML/TF Risks

To implement a reasonable and effective risk-based approach, FIs have to identify the risks, the extent to which it can be sufficiently identified and identify the categories of customers and transactions. There is no agreed upon set of risk categories and the FATF has identified these categories to serve as a guidance for developing strategy[155].

- Geographic Risk

Each country will have its own set of threats and risks with respect to money laundering or terrorist financing. While analyzing if any of the geographies / countries pose a threat, a review may be undertaken of various factors including whether the country is subject to sanctions, or has been identified by credible sources as lacking sufficient AML/CFT laws and regulations or providing funds and support to terrorist activities or has a high level of corruption and criminal activity.

- Customer Risk

Additionally, FIs may also take cognizance of the risks posed by a customer or group of customers. For instance, customers who may have a higher risk include, amongst others:

a) Customers conducting their business relationship or transactions in unusual circumstances, such as significant and unexplained geographic distance between the institution and the location of the customer, unexplained movement of accounts to different institutions or unexplained movement of funds between institutions in various geographic locations
b) Customers where the structure or nature of the entity or relationship makes it difficult to identify the true owner or controlling interests
c) Customers involved in high risk businesses like casinos, betting, gambling related activities
d) Customers undertaking frequent transaction on a cash basis
e) Charities and other "not for profit" organizations which are not subject to monitoring or supervision (especially those operating on a "cross-border" basis)
f) Customers that are Politically Exposed Persons (PEPs)

- Product/Service Risk

Risks may also arise based on any products or services that are offered by FIs, themselves including the new and innovative products and services that may not be directly offered by FIs but that make use of their services to deliver the product. Such risks inherently exist in digital transactions such as online banking, stored value cards, international wire transfers etc. Such risk may also arise in potentially higher risk activities like services involving banknote and precious metal trading and delivery.

Different channels for the acquisition and management of customer relationships, as well as for the delivery of products and services, pose different types and levels of risk. Supervised institutions should identify and evaluate these risks at both the enterprise-wide and the customer-

[155] FATF Guidance, GUIDANCE ON THE RISK BASED APPROACH TO COMBATING MONEY LAUNDERING AND TERRORIST FINANCING, 2007

specific levels. FIs should specifically monitor those channels which have the potential to be anonymous.

- Other Risk Variables

There are other risk variables that a FI may take into account including:

- The purpose of the account or relationship, the duration of the relationship etc.
- The level of assets deposited by a particular customer or the size of transactions undertaken
- The level of regulation or other government regime that a customer is subject to
- The use of intermediate corporate vehicles or other structures that have no apparent commercial rationale or that unnecessarily increase the complexity or result in a lack of transparency. The use of such vehicles or structures, without an acceptable explanation, increases the risk.

Proper identification of risk factors is crucial to the effective implementation of a risk-based approach to assessing and mitigating ML/TF risk. Identified risk factors are used for the accurate categorization of risks, as well as for the application of appropriate mitigation measures at both the enterprise and the customer level.

Risk- Based Assessment- Guiding Principles and Considerations

A risk-based assessment means that countries, competent authorities and FIs are expected to identify, assess and understand the money laundering and terrorist financing risks that they are exposed to and take AML/CFT measures accordingly to mitigate these risks effectively. An effective risk-based approach will balance, allowing FIs to exercise reasonable business judgment without hindering the business activities of FIs or their relationships with their customers. The Financial Actions Task Force (FATF) have identified five high level principles that can be used as a guide when designing an effective and balanced risk-based approach:

- Understanding and Responding to the Threats and Vulnerabilities at a National Level: There needs to be a complete and comprehensive understanding of all the threats and vulnerabilities at a national level. This understanding can come from a national risk assessment that has to be modified and adjusted according to the circumstances of each country as each country will have their own specific threats and vulnerabilities.
- A Legal/Regulatory Framework that supports a Risk-Based Approach: The legal and regulatory framework of a country has to be supportive and conducive to the implementation of a risk-based approach.
- Design a Supervisory Framework to support the Risk-Based Approach: For the effective implementation of a risk-based approach, there needs to be a supervisory framework that has the necessary authority and has trained staff that can make principle-based decisions to implement a risk-based approach.
- Identifying the Main Actors and Ensuring Consistency: Countries should identify who the main stakeholders are in order to adopt an effective risk-based approach. Each country will differ, and consideration should be given as to how to divide responsibility and share information between the parties. Potential stakeholders may include the government, law enforcement, financial service regulators, private sector and public sector FIs

- Information exchange between Public and Private Sector: Public authorities are privy to information that may help FIs reach informed judgments when applying a risk-based approach to combating money laundering and terrorist financing. Similarly, private FIs have an in-depth understanding of their client's business. Hence an effective information exchange between both sectors is an integral part of a country's strategy in implementing an effective approach for AML/CFT. Both sectors should work collaboratively, and public sectors should emphasize that any generalized information from them cannot be used as a substitute for a private institution's own judgment.

Annex II

Guidelines by Authorities for Financial Institutions – CDD Measures

In order to provide guidance to FIs on the processes and procedures to be followed by them to manage the ML/TF risks, some of the global regulators have published guidelines or directions for the FIs. To understand the general guidelines provided by the authorities in relation to conducting CDD, an analysis of four separate guidelines have been undertaken:

a) Anti-Money Laundering and Countering the Financing of Terrorism Guidelines for the Financial Sector dated September 2019 of the Central Bank of Ireland (available at https://www.centralbank.ie/docs/default-source/regulation/how-we-regulate/anti-money-laundering-and-countering-the-financing-of-terrorism/guidance/anti-money-laundering-and-countering-the-financing-of-terrorism-guidelines-for-the-financial-sector.pdf?sfvrsn=4)
b) Anti-Money Laundering and Combating the Financing of Terrorism and the Financing of Illegal Organizations Guidelines for Financial Institutions dated June 23,2019 by UAE Central Bank (available at https://www.centralbank.ae/sites/default/files/2019-07/ME%20PMO%20AML-CFT%20%20Guidance%20-%20FIs%20Only%20-%20For%20publication%20on%20CBUAE%20website.pdf);
c) Guideline on Anti-Money Laundering and Combatting Terrorism Financing by UAE Central Bank of Trinidad and Tobago (available at https://www.central-bank.org.tt/sites/default/files/page-file-uploads/AML_CFT%20Guideline%20Final-April%2013%202018_0.pdf);
d) Master Direction – Know Your Customer (KYC) Direction, 2016 (as updated on May 29,2019) issued by the Reserve Bank of India (available at https://www.rbi.org.in/Scripts/BS_ViewMasDirections.aspx?id=11566)

Some of the key highlights under the CDD measures prescribed by them are summarized herein. To act as an effective risk assessment framework is based on strong processes and procedures to identify customers and verify their identity. Such a framework should identify which customers or categories of customers present higher risk and accordingly increase the requirements of checks to be undertaken upon them (through the implementation of enhanced due diligence measures). Similarly, where the FI determines that a customer or a category of customers presents low risk, simplified due diligence (SDD) should be applied.

As a part of the identification process, CDD measure must where applicable, identify the customer's beneficial owner or legal representatives as well as obtain information regarding the purpose and intended nature of the business relationship. Prior to establishing a business relationship, a FI should ensure that the customer's identity has been verified. The customer's physical identity should be verified using one (1) form of photo ID may be a valid passport, national identification card or driver's license. Additional picture identification should be requested by the FI only where higher risk is identified and enhanced due diligence is warranted. FIs are prohibited from opening anonymous accounts or accounts in fictitious names. Where a FI is unable to verify the true identify of a prospective client or beneficial owner, the FI is

prohibited from establishing the business relationship, or if already established must immediately terminate the business relationship and consider filing a suspicious transaction report.

It is essential that the CDD is undertaken at not just the inception of the business relationship (like prior to signing any contract or agreement or undertaking any transaction for them) but also during one-off or occasional transactions which are undertaken for persons with whom the FI does not have a business relationship. Examples of such transactions include, but are not limited to exchange of currencies, issue or cashing/redemption of traveler's cheques etc. The CDD measures, especially in relation to occasional transactions, may be increased in case of one-off or occasional transactions (like wire-transfers), where the transaction is carried out in a single operation or in several operations that appear to be linked, may be of a cumulative value higher than a set monetary limit.

Though it is important to stress on the requirement of a CDD policy, to achieve the objective of financial inclusion, it is also essential that the CDD policy is not restrictive or inflexible such that it results in a denial of access to basic financial services, especially for those who are economically or socially vulnerable such as low-income groups, the elderly, the disabled, students and minors. To this end, where the customers pose a lower risk gradient, the FIs may apply Simplified Due Diligence (SDD). SDD should be commensurate with the identified lower risk factors (e.g. the simplified measures may relate only to customer acceptance measures or to aspects of ongoing monitoring). It should be noted that SDD never means a complete exemption or absence of CDD measures but rather, FIs may adjust the frequency and intensity of measures to satisfy the minimum CDD standards.

For an SDD to be implemented, it would hence be imperative to consider that beneficial owner will in most instances be the customer himself or a closely related family member. Where there is suspicion that the account owner is being used as a 'strawman' and is not the beneficial owner, normal or enhanced due diligence measures should be applied and an internal suspicious report must be filed with the organization's compliance officer.

SDD generally involves a more lenient application of certain aspects of CDD measures, including, but not limited to, such elements as:

- A reduction in verification requirements with regard to customer or Beneficial Owner identification;
- Fewer and less detailed inquiries in regard to the purpose of the business relationship, the nature of the customer's business, the customer's source of funds, and the purpose of individual transactions;
- More limited supervision of the business relationship including less frequent monitoring of transactions, and less frequent review/updating of customer due diligence information.

Some examples of customers to whom CDD measures may apply are:

i. Customers whose sole source of funds is a salary credit to an account or with a regular source of income from a known source which supports the activity being undertaken;

ii. Pensioners, social benefit recipients or customers whose income originates from their spouses'/partners' employment);
iii. Financial products or services that provide appropriately defined and limited services to certain types of customers. For customers who do not have photo identification or have limited identification documentation such as tourists or those who are socially or economically vulnerable such as the disabled, elderly, minors or students, a 'tiered' CDD approach allows financial access with limited functionality. For example, a FI may offer banking accounts with low transaction/payment/balance limits with reduced documentation requirements. Access to additional services such as higher transaction limits or account balances or access to diversified delivery channels should only be allowed if and when the customer can satisfy additional identification requirements. Where this obtains FIs must have monitoring systems to ensure that transaction and balance limits are observed;
iv. Customers represented by those whose appointment is subject to court approval or ratification (such as executors or receivers).

Even in case of SDD, a FI should be wary of unusual transactions or any other suspicious activity that may occur. In such an incident, additional measures of CDD may be included.

Enhanced Due Diligence: For categories of customers, business relationships or transactions that are determined to present higher ML/TF risk due to business activity, ownership structure, nationality, residence status, politically exposed status or other higher risk indicators a FI must apply an EDD. In certain scenarios, it must be mandated that any transactions with such high-risk clientele or products require the special attention of senior management.

EDD must be applied in the following circumstances:
i. Business transactions with persons and FIs in or from other countries which do not or insufficiently comply with the FATF Standards;
ii. Complex, unusual or large transactions, whether completed or not, to all unusual patterns of transaction and to insignificant but periodic transactions which have no apparent economic or visible lawful purpose;
iii. When establishing correspondent banking relationships;
iv. Where the customer is a politically exposed person (PEP); and
v. Non face-to-face business relationships or transactions.

Where having regard to the type of customer or the nature of transaction an EDD is the preferred type of CDD, FIs may adopt more intrusive and exhaustive steps to complete CDD. Such steps may include:

i. Increasing the quantity of information obtained for CDD purposes (e.g. request additional information as to the customer's residential status, employment, salary details and other sources of income) and requesting additional documentary evidence or utilizing publicly available sources (e.g. scrutiny of negative media news, internet searches, use of social media)
ii. Understand the customer's ownership and control structure to ensure that the risk associated with the relationship is well-known.
iii. Understand the intended nature of the business relationship and the reasons for intended or performed transactions. This may include obtaining information on the number, size

and frequency of transactions that are likely to be conducted. It may be appropriate to request a customer's, business plans, cash flow projections, copies of contracts with vendors etc. The FI should understand why the customer is requesting a certain service or product particularly when it is unclear why the customer is seeking to establish business relationships in another jurisdiction from where he is domiciled. The account may have to be monitored for a period of time to establish a full view of the nature of activity and whether it fits with the initial risk profile of the customer.

iv. Establish the source of funds or source of wealth of the customer. Where the risk associated with the customer is particularly elevated, intrusive measures to verify the source of funds and wealth may be the only adequate risk mitigation measure.
v. Evaluate the principals and conduct reference checks and checks of electronic databases, if possible & legally permissible;
vi. Review current financial statements; and
vii. Conduct enhanced, ongoing monitoring of the business relationship, by increasing the number and timing of controls applied, and through more frequent formal review.

Aadhaar based KYC – Requirements under the Master Direction – Know Your Customer (KYC) Direction, 2016 issued by the Reserve Bank of India ('**Master Direction**').

Further to the introduction of Aadhaar in India, the FIs are, in accordance with the provisions of the Master Direction, entitled to undertake CDD utilizing the Aadhaar number. The Aadhaar number may be used by the FIs to identify a customer including a beneficial owner, authorized signatory or the power of attorney holder related to any legal entity. A FI shall carry out authentication of the customer's Aadhaar number using e-KYC authentication facility provided by the UIDAI. A customer may also provide proof of possession of Aadhaar where offline verification can be carried out. It is mandated therein a FI shall, where its customer submits a proof of possession of Aadhaar Number containing Aadhaar Number, ensure that such customer redacts or blacks out his Aadhaar number through appropriate means where the authentication of Aadhaar number is not required. Biometric based e-KYC authentication can be done by bank official/business correspondents/business facilitators.

Further, accounts may be opened using OTP based e-KYC, in non-face-to-face mode, provided they comply with the following conditions:

- The customer provides his/her specific consent for authentication through OTP.
- The aggregate balance of all the deposit accounts of the customer shall not exceed INR100,000/-.
- the aggregate of all credits in a financial year, in all the deposit accounts taken together, does not exceed INR 100,000/-.
- As regards to borrowal accounts, only term loans shall be sanctioned. The aggregate amount of term loans sanctioned shall not exceed INR 60,000/- in a year.
- Accounts, both deposit and borrowal, opened using OTP based on e-KYC shall not be allowed for more than one year within which proper identification / CDD under which the Master Direction is carried out.
- If the CDD procedure as mentioned above is not completed within a year, in respect of deposit accounts, the same shall be closed immediately. In respect of borrowal accounts no further debits shall be allowed.

- A declaration shall be obtained from the customer to the effect that no other account has been opened nor will be opened using OTP based KYC in non-face-to-face mode with any other FIs
- FIs shall have strict monitoring procedures including systems to generate alerts in case of any non-compliance/violation, to ensure compliance with the above-mentioned conditions.

FIs may undertake live video-based customer identification process ('**V-CIP**'). V-CIP is equivalent to face-to-face identification process and is defined as a method of customer identification by an official of the FI by undertaking seamless, secure, real-time, consent based audio-visual interaction with the customer to obtain identification information including the documents required for CDD purpose, and to ascertain the veracity of the information furnished by the customer. Amongst other requirements during a V-CIP, it is mandated that:

- the FI track the live location of the customer (geotagging) shall be captured to ensure that customer is physically present in India;
- capture a clear image of PAN card to be displayed by the customer during the process, except in cases where e-PAN is provided by the customer
- process is a seamless, real-time, secured, end-to-end encrypted audiovisual interaction with the customer and the quality of the communication is adequate to allow identification of the customer beyond doubt. RE shall carry out the liveliness check in order to guard against spoofing and such other fraudulent manipulations
- the video recording is stored in a safe and secure manner and bears the date and time stamp
- ensure security, robustness and end to end encryption, the FIs shall carry out software and security audit and validation of the V-CIP application before rolling it out.

Further, if the FI proposes to utilize a digital KYC process, the FI shall develop an application which shall be made available at customer touch points for undertaking KYC of their customers and the KYC process shall be undertaken only through this authenticated application of the FIs. Among the various requirements which are to be complied with by the FI which using a digital KYC application, the following are included:

- The access of the digital KYC application shall be controlled by FIs and it should be ensured that the same is not used by unauthorized persons.
- The application shall be accessed only through login-id and password or live OTP or time OTP controlled mechanism given by FIs to its authorized officials. FI must ensure that the Live photograph of the customer is taken by the authorized officer and the same photograph is embedded in the customer application form (CAF).
- The application shall have the feature that only live photograph of the customer is captured and no printed or video-graphed photograph of the customer is captured. The background behind the customer while capturing live photograph should be of white colour and no other person shall come into the frame while capturing the live photograph of the customer.
- Once the above-mentioned process is completed, a One Time Password (OTP) message containing the text that 'Please verify the details filled in form before sharing OTP' shall be sent to the customer's own mobile number. Upon successful validation of the OTP, it will be treated as customer signature on CAF.
- The authorized officer shall provide a declaration about the capturing of the live photograph of the customer and the original document. For this purpose, the authorized

official shall be verified with One Time Password (OTP) which will be sent to his mobile number registered with the FI.

- Subsequent to all these activities, the Application shall give information about the completion of the process and submission of activation request to activation officer of the FI, and also generate the transaction-id/reference-id number of the process;
- On successful verification of all the information, the CAF shall be digitally signed by authorized officer of the FI who will take a print of CAF, get signatures/thumb-impression of customer at appropriate place, then scan and upload the same on the system. The Original hard copy may be returned to the customer.

Annex III

Survey Respondent Countries & Authorities

S. No	Name of Country	Name of Authority
1.	Lebanon	Banque Du Liban
2.	Egypt	Central Bank of Egypt
3.	Yemen	Central Bank of Yemen
4.	Jordan	Central Bank of Jordan
		Capital Market Authority of Jordan
5.	Kuwait	Central Bank of Kuwait
6.	Libya	Central Bank of Libya
7.	Mauritania	Central Bank of Mauritania
8.	Sudan	Central Bank of Sudan
9.	Bahrain	Central Bank of Bahrain
10.	Oman	Central Bank of Oman
11.	Palestine	Palestine Capital Market Authority "PMCA"
		Palestine Monetary Authority
12.	United Arab Emirates	Central Bank of United Arab Emirates
13.	Iraq	Central Bank of Iraq
14.	Morocco	Bank Al-Maghrib
15.	Saudi Arabia	Saudi Arabian Monetary Authority
16.	Tunisia	Central Bank of Tunisia/ Tunisian Financial Analysis Committee
17.	Qatar	Qatar Financial Intelligence Unit
		Central Bank of Qatar
18.	Algeria	Bank of Algeria

Annex IV

Survey Questions

صندوق النقد العربي
ARAB MONETARY FUND

Arab Regional Fintech Working Group

Survey for Digital Identity and e-KYC in Arab Countries

Arab Monetary Fund
September 2019

Survey for Digital Identity & e-KYC

Introduction

*This survey is intended to collect information on the current systems and practices followed within Arab countries related to management of identity of nationals/ residents and related to implementation of electronic Know Your Customer ('**e-KYC**') processes.*

This survey is intended to be filled up by Arab Central Banks and Monetary Authorities, Capital Market Authorities, Insurance Authorities in addition to the AML units in Arab countries.

While completing the survey, please note that the following terms have the definitions and meanings assigned below:

"Digital Identity" (or Digital ID) is a collection of electronically or digitally captured and stored identity attributes that uniquely describe a person within a given context and is used for electronic transactions, for example, common personal identity attributes include name, age, sex, place of birth, address, fingerprints, a photo, a signature, an identity number, date and place of registration, … etc.

Questions

1. Please list the name of your organization – Country, and the contact details as following:

Name	
Title	
Organization - Country	
Official Email	
Telephone number	+

2. Does your country have a national identification system? Please tick the appropriate box

   ☐ Yes ☐ No

3. Does your country have "**Foundational Identification System**" – i.e. is the identification system created primarily to provide **general identification** to the members of the population and is provided by (or on behalf of) the government?

   If yes, proceed to question no. 4, otherwise please proceed to question no. 8

☐ Yes ☐ No

4. Is the "*Foundational Identification System*" (as mentioned in question no.3) for citizens only or is it for residents and citizens?

   ☐ Citizens only ☐ Citizens & Residents

5. Is the "*Foundational Identification System*" (as mentioned in question no.3) implemented in the country as a Digital ID system?

   If yes, proceed to question no. 6, otherwise please proceed to question no. 8

   ☐ Yes ☐ No ☐ In process

6. Please provide the percentage of the following:

Items	Percentage %
Citizens/residents in your country have currently the digital or electronic national ID	
Physical IDs vs. Electronic IDs	
Physical IDs vs. Electronic IDs by gender, i.e. male vs. female	

7. Do you presently collect biometric information as a part of the Digital ID system? For clarity, biometric information means "*Physical or behavioral attributes of an individual, including fingerprints, irises, facial images, gait, signatures, keystrokes, ... etc.*"

   ☐ Yes ☐ No ☐ In process

   Please provide Details:

   Fingerprints, irises, facial images, signatures.

   ……
   ……
   ……
   ……
   ……
   ……

8. Are there other systems of identification followed in the country like voters ID, driver's license, tax ID, ration cards, social security IDs, travel documents … etc.?

☐ Yes ☐ No

Please describe if any:

……
……
……
……
…

9. Which regulatory agency is the custodian of the information collected under the Identification System?

Please specify

……
……
……
……
…

10. Is there any regulation that governs the use of national ID data, i.e. data base?

☐ Yes ☐ No

Please list if any

……
……

11. Are there any regulations in place or being drafted related to e-signature?

☐ Yes ☐ No

Please list if any

……..

12. If there is a national data base, does it also capture financial transactions data?

☐ Yes ☐ No

If yes, please specify which type of data

……
……
……
……

13. Is the data base linked to credit bureaus?

☐ Yes ☐ No

14. Can financial institutions have access to the data base if they need to open accounts?

☐ Yes ☐ No

If yes, please list the type of financial institutions (banks, microfinance …etc.)

……
…

15. Are there any recognized private sector initiatives for creating a Digital ID system in your country including any system introduced by a consortium of banks?

☐ Yes ☐ No

16. What is the current scheme of KYC for banking and financial services including digital financial services in your country? Please describe if any

.....

17. Please describe current physical KYC process(es).

.....

18. Does your country have a fully operational e-KYC processes in place?

If yes, proceed to question no. 21, otherwise please proceed to question no. 19

☐ Yes ☐ No

19. Does your country have an e-KYC procedure in a pilot or implementation phase?

If yes, proceed to question no. 21, otherwise please proceed to question no. 20

☐ Yes ☐ No

20. Does your country have plans to implement e-KYC?

☐ Yes ☐ No

If yes, please specify when?

.....
.....
.....

21. Please describe the current status of e-KYC implementation plans – what is the process by which e-KYC (tiered KYC) is to be implemented, technical solutions assessed … etc.

.....
.....

22. For countries that have implemented or are implementing e-KYC, please list: which government entities were involved in the processes e.g. Central Bank, National Identity Authority, Ministries of Interior …etc.

……
……

how funding was secured for such initiative – e.g. budgeted, through aid, assistance…. etc.

……
……
……

23. Please summarise the legislative or regulatory framework that was introduced or applied/will apply in your country where an e-KYC solution has or is being introduced?

……
……

24. Is there any regulation in place related to data protection?

☐ Yes ☐ No

If yes, please specify

……
……
……
……

25. For countries that have or are introducing e-KYC, please identify whether there is any allowance for lower limit digital financial instruments which do not require KYC where, for example, a person may not have a form of national or electronic national identification

…… ……

26. For countries that have or are introducing e-KYC, please describe the technical physical store/vault for the document artefacts of the customer and the underlying technology – Blockchain, document management system …etc.

…… ……

27. Following question (26), will this store/vault be a central digital vault available for all banks to leverage and consume with customer consent, i.e. does not require the customer to provide documentation to every bank he intends to deal with.

☐ Yes ☐ No

28. Following question (26), as part of the e-KYC process, who are the entities who will contribute to this digital vault, e.g. Immigration and residency, Police? Please specify

……

……

……

……

29.Are Are such contributions captured at the time of Identity creation/update in the country?

☐ Yes ☐ No

30. Can the customer upload and/ or amend documents in this vault?

☐ Yes ☐ No

31. What is the technical mechanism for banks to access this vault during the e-KYC process?

……

……

32. For countries that have or are introducing e-KYC, have you considered the usage of Digital Signatures in the following:

ID authentication		
Document signing		

If yes, please elaborate the use cases in which you seek to introduce digital signatures

……

……

33. Regarding Digital signatures, is your country actively amending the law of the land to allow the use of digitally signed documents/artefacts are having legal status?

☐ Yes ☐ No

If yes, please elaborate the use cases allowed and those which are excluded

……

……

34. For countries that have or are introducing e-KYC, have you considered the use of banks to be an additional vehicle for authenticating and onboarding customers to the central/federal digital identity repository?

☐ Yes ☐ No

If yes, please elaborate the mechanism of such delegated onboarding

……

…

35. For countries that have or are introducing e-KYC, please elaborate your security architecture covering aspects of Data Confidentiality, Data Governance, Data Provenance, Geographical Presence of customer confidential data, Treatment of Cloud infrastructure …etc.

……

36. For countries that have or are introducing e-KYC, has any special considerations been considered with respect to the General Data Protection Regulation (GDPR)

☐ Yes ☐ No

If yes, please describe such considerations

……

…

37. Please list potential types of risks that may emerge from the application of e-KYC:

☐ Cyber security ☐ Operational ☐ Compliance

☐ IT ☐ Data Protection ☐ Others

If others, please specify

38. Is there any misuse of the e-KYC implementation such as fraud, Manipulation, ….etc.?

☐ Yes ☐ No

If yes, please summarize the cases

…… ……

39. What are the precautionary measurements applied to prevent any misuse of the e-KYC? Please describe

…… ……

40. Please mention any Digital ID and e-KYC system implemented in any country (including outside the Arab region), which you would like to be covered as a case study in the report.

…… ……

Please fill in the survey and revert it back to the Technical Secretariat of the Arab Regional Fintech Working Group by October 15th, 2019 via email: FintechWG@amf.org.ae; governors@amf.org.ae;

In case of any queries, please contact the Arab Regional Fintech WG Technical Secretariat through the following contacts:

Email:	FintechWG@amf.org.ae; nouran.youssef@amf.org.ae; Amal.Masrieh@amf.org.ae; rasha.elashy@amf.org.ae;
Direct Office:	+971 2 6171477
Mobile:	+971 505604585
Tel:	+971 2 6171574
Fax:	+971 2 6326454

Thank you
Arab Monetary Fund

Reference List

Abraham et al. (2017). *State of Aadhaar Report 2016- 2017*. https://static1.squarespace.com/static/5b7cc54eec4eb7d25f7af2be/t/5bc5357e652dea4073286a35/1539650996433/State-of-Aadhaar-Ch3-Legal.pdf accessed on November 19, 2019.

Aminova M. (2019). *Entrepreneurship and Innovation Ecosystem in 22 Arab countries: The Status Quo, Impediments and the Ways Forward*, (Telecommunication Development Bureau (BDT) in November 2018 – April 2019). Available at https://www.itu.int/en/ITU-D/Regional-Presence/ArabStates/Documents/events/2019/Reports19/Entrepreneurship%20and%20Innovation%20in%20Arab%20Region_Final%20report.pdf accessed on 17 November 2019.

Atick J. (2014). *Digital identity: The essential guide*. ID4Africa Identity Forum, 2014, available at http://www.id4africa.com/main/files/Digital_Identity_The_Essential_Guide.pdf accessed on November 17, 2019.

Bahrain News Agency (2019). *BENEFIT launches first eKYC project in Arab World*. February, 2019, available at https://www.bna.bh/en/BENEFITlaunchesfirsteKYCProjectinArabWorld.aspx?cms=q8FmFJgiscL2fwIzON1%2BDnjwKS5lgF8vEgrzLWh3IgA%3D accessed on November 19, 2019.

BankID.com (2019). *This is BankID*. Available at https://www.bankid.com/en/om-bankid/detta-ar-bankid accessed on November 17, 2019.

Cavallo et al. (2016). Saving for development: How Latin America and the Caribbean can save more and better. *InterAmerican Development Bank*, June 2016. Available at https://publications.iadb.org/publications/english/document/Saving-for-Development-How-Latin-America-and-the-Caribbean-Can-Save-More-and-Better.pdf accessed on November 17, 2019.

Cavoukian, A. (2011). *Privacy by Design: The 7 foundational principles*. Available at https://iab.org/wp-content/IAB-uploads/2011/03/fred_carter.pdf accessed on November 20, 2019.

Capgemini, "*KYC Utility: why should you consider it?*" available at https://www.capgemini.com/2019/07/kyc-utility-why-should-you-consider-it/ accessed on December 22, 2019

Clark J. and Daly C. (2019). *Digital ID and the Data Protection Challenge*. World Bank. Available at http://documents.worldbank.org/curated/en/508291571358375350/Digital-ID-and-the-Data-Protection-Challenge-Practitioners-Note accessed on November 20, 2019.

Council of EU (2019). *Interoperability between EU information systems: Council Presidency and European Parliament reach provisional agreement*. May 2019. Available at

https://www.consilium.europa.eu/en/press/press-releases/2019/05/14/interoperability-between-eu-information-systems-council-adopts-regulations/ accessed on November 14, 2019.

Counter Currents Collective (2017). *Right to Privacy: Judgement Highlights and Full Judgement*. August, 2017, available at https://countercurrents.org/2017/08/right-to-privacy-judgement-highlights-and-full-judgement accessed on November 19, 2019.

DAWN Newspaper (2018). *Unregistered mobile phones to become unusable after 20th: PTA*. Available at https://www.dawn.com/news/1438714/unregistered-mobile-phones-to-become-unusable-after-20th-pta accessed on November 20, 2019.

Desai et al. (2017). *Ten Principles on Identification for Sustainable Development*. World Bank, February 2017, available at http://blogs.worldbank.org/ic4d/ten-principles-identification-sustainable-development accessed on November 17, 2019.

Desai, V., Diofasi, A. and Jing L. (2018). *The global identification challenge: Who are the 1 billion people without proof of identity?* World Bank, April 2018. https://blogs.worldbank.org/voices/global-identification-challenge-who-are-1-billion-people-without-proof-identity accessed on October 20, 2019.

Digital Transformation Agency. *Benefits of joining the digital identity ecosystem*. Available at https://www.dta.gov.au/our-projects/digital-identity/benefits-joining-digital-identity-ecosystem accessed November 17, 2019.

Economic Times (2018). *What's valid and what's not: Everything you need to know about Aadhaar verdict*. September 2018, available at economictimes.indiatimes.com/articleshow/65961427.cms?from=mdr&utm_source=contentofinterest&utm_medium=text&utm_campaign=cppst accessed on November 19, 2019.

E-Estonia (2018). What we learned from the eID card security risk. May 2018, available at https://e-estonia.com/card-security-risk/ accessed November 19, 2019.

E-Estonia.com. E-identity: Id-card, available at https://e-estonia.com/solutions/e-identity/id-card, accessed on November 19, 2019.

E-Estonia.com. E-identity: Mobile-id, available at https://e-estonia.com/solutions/e-identity/mobile-id, accessed on November 19, 2019.

E-Estonia.com. E-identity: Smart-id, available at https://e-estonia.com/solutions/e-identity/smart-id, accessed on November 19, 2019.

Republic of Estonia's Information system authority. ROCA vulnerability and eID: Lessons learned. Available at https://www.ria.ee/sites/default/files/content-editors/kuberturve/roca-vulnerability-and-eid-lessons-learned.pdf accessed on November 19, 2019.

El Sawy N. (2019). Financial institutions gear up to integrate UAE Pass. *The National*, September 2019, available at https://www.thenational.ae/business/money/financial-institutions-gear-up-to-integrate-uae-pass-1.915602, accessed on November 19, 2019.

FATF-GAFI (2019). *Draft Guidance on Digital Identity*. November, 2019, available at https://www.fatf-gafi.org/media/fatf/documents/publicconsultation/Digital%20ID-public-consultation-version.docx accessed on November 20, 2019.

FATF-GAFI (2019). *Draft Guidance on Digital Identity*. November, 2019, available at https://www.fatf-gafi.org/media/fatf/documents/publicconsultation/Digital%20ID-public-consultation-version.docx accessed on November 20, 2019.

FATF, *International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation*. FATF, Paris, France in 2012-2019. Available at https://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%202012.pdf accessed on November 11, 2019.

FATF, "*Public consultation on FATF draft guidance on digital identity"* available at https://www.fatf-gafi.org/publications/fatfrecommendations/documents/consultation-digital-id-guidance.html accessed on December 9,2019

Fenergo (2019). *Fenergo Partners with BENEFIT to Create National eKYC Utility in Bahrain*. PR Newswire, May 2019, available at https://www.prnewswire.com/ae/news-releases/fenergo-partners-with-benefit-to-create-national-ekyc-utility-in-bahrain-850186014.html accessed on November 19, 2019.

Financial Inclusion Insights Program (2014). *Digital Pathways to Financial Inclusion.* Tanzania, Wave 1 in November 2014, available at http://finclusion.org/uploads/file/reports/FII-Tanzania-Wave-One-Wave-Report.pdf accessed on November 15, 2019.

Finda Systems (2018). *Digital KYC proof-of-concept white-paper 1: Overview of the Digital KYC authentication system*. November 2018, available at https://findasystem.com/download/KPI%20FINDA%20FSTI%20POC%20paper%201%20-%2019Nov2018.pdf accessed on November 19, 2019.

Fintech Futures (2019). *Regional KYC utilities: genesis of global collaboration on shared compliance platforms*. Available at https://www.fintechfutures.com/2019/11/regional-kyc-utilities-genesis-of-global-collaboration-on-shared-compliance-platforms/ accessed on November 19, 2019.

FSB (2015). *Report to the G20 on actions taken to assess and address the decline in correspondent banking*. Available at https://www.fsb.org/2015/11/report-to-the-g20-on-actions-taken-to-assess-and-address-the-decline-in-correspondent-banking/ accessed on November 12, 2019.

FSB, "*FSB Action Plan to Assess and Address the Decline in Correspondent Banking: Progress Report*" , May 2019 at https://www.fsb.org/wp-content/uploads/P290519-1.pdf accessed on December 22, 2019

Gasser U. (2015). *Interoperability in the Digital Ecosystem*. July 6, 2015. Available at https://ssrn.com/abstract=2639210 or http://dx.doi.org/10.2139/ssrn.2639210 accessed on November 13, 2019.

GDPR. *General Data Protection Regulation*. Available at https://gdpr-info.eu/ accessed on November 20, 2019.

Gemalto (2019). Nigerian national ID program: An ambitious initiative. Available at https://www.gemalto.com/govt/customer-cases/nigeria-eid accessed on November 19, 2019.

GLEIF, "*Introducing the Legal Entity Identifier (LEI)"* available at https://www.gleif.org/en/about-lei/introducing-the-legal-entity-identifier-lei accessed on December 11,2019

GSMA, World Bank and Security Identity Alliance (2016). *Digital Identity towards Shared Principles for Public and Private sector Co-operation*. Available at https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2016/07/Towards-Shared-Principles-for-Public-and-Private-Sector-Cooperation.pdf accessed on November 14, 2019.

GSMA (2017). *Aadhaar: Inclusive by design: A look at India's national identity program and its role in the JAM trinity*. March 2017, available at https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2017/03/gsma-aadhaar-report-270317.pdf accessed on November 19, 2019.

ICAR (2018), *The unique digital identity will be crucial for worldwide social and economic development*. Available at https://www.icarvision.com/en/the-unique-digital-identity-will-be-crucial-for-worldwide-social-and-economic-development accessed 28 October 2019.

Id4africa.com (2019). *Interoperability in African Governments: Digital Identity as an Enabler*. Available at http://www.id4africa.com/2019_event/presentations/InF11/4-Chimezie-Emewulu-Seamfix.pdf accessed on November 13, 2019.

International Telecommunication Union (2018), *Digital Identity Road Map Guide*, available at https://www.itu.int/en/ITU-D/ICT-Applications/Documents/Guides/Digital_Identity_Roadmap_Guide-2018-E.pdf accessed on November 12, 2019.

International Telecommunications Union (2019). *Unique, Legal and Digital: Three Characteristics of ID Crucial to Financial Inclusion*. Available at https://news.itu.int/unique-legal-digital-id-financial-inclusion/ accessed 28 October 2019.

Institute of International Finance "IIF" (2019). *Digital Identity: Key Concepts*. July 2019. Available at https://www.iif.com/Portals/0/Files/content/Regulatory/iif_digital_id_07022019.pdf accessed on November 12, 2019.

Klapper et al. (2017). *The Global Findex Database: Measuring Financial Inclusion and the Fintech Revolution*. World Bank, available at https://globalfindex.worldbank.org/ accessed on November 18, 2019.

Lyman T. and De Koker L. (2018). *KYC Utilities and Beyond: Solutions for an AML/CFT Paradox?* Available at https://www.cgap.org/blog/kyc-utilities-and-beyond-solutions-amlcft-paradox accessed on November 19, 2019.

Makin P. and Martin C. (2018). *The Biometric Balancing Act in Digital Finance*. CGAP, available at https://www.cgap.org/blog/biometric-balancing-act-digital-finance, accessed on November 19, 2019.

Mohap (2019). *UAEPASS: User Guide; Version 1.0*. Available at https://www.mohap.gov.ae/Documents/Banner/UAEPASS_User_Guide_1.0.pdf accessed on November 19, 2019.

Namita Viswanath , Savithran Ramesh, "*India: The Supreme Court's Aadhaar Judgement And The Right To Privacy*", available at http://www.mondaq.com/india/x/744522/Data+Protection+Privacy/The+Supreme+Courts+Aadhaar+Judgement+And+The+Right+To+Privacy accessed on December 23,2019

Natarajan H. (2018). *G20 Digital Identity Onboarding*. World Bank Group, available at https://www.gpfi.org/sites/gpfi/files/documents/G20_Digital_Identity_Onboarding.pdf accessed on November 12, 2019.

NIMC (2019). *How to enroll Adults*. Available at https://www.nimc.gov.ng/how-to-enrol-adults/ accessed on November 19, 2019.

NIMC (2019). *Nigerians Embrace the Mandatory Use of NIN*. Available at https://www.nimc.gov.ng/nigerians-embrace-the-mandatory-use-of-nin/ accessed on November 19, 2019.

OECD (2018). *Embracing Innovation in Government: Global Trends 2018; Aadhaar. India*. Available at https://www.oecd.org/gov/innovative-government/India-case-study-UAE-report-2018.pdf accessed on November 19, 2019.

Parashar, A. and Chandra, A. (2017). *Central KYC: What it means for investors and institutions*. PWC, 2017, https://www.pwc.in/assets/pdfs/financial-service/central-kyc.pdf accessed on November 19, 2019.

Perlman L. (2018). *The Digital Financial Services Primer*. Available at http://www.citicolumbia.org/wp-content/uploads/2018/11/DFS-primer-for-publication.pdf accessed on November 19, 2019.

Regulation (EU) 2019/818 of the *European Parliament and of the Council* of 20 May 2019 on Establishing a framework for interoperability between EU information systems in the field of police and judicial cooperation, asylum and migration and amending Regulations (EU) 2018/1726, (EU) 2018/1862 and (EU) 2019/816.

Sapkale Y. (2019). *Aadhaar data breach largest in the world, says WEF's Global Risk Report and Avast*. February, 2019, available at https://www.moneylife.in/article/aadhaar-data-breach-largest-in-the-world-says-wefs-global-risk-report-and-avast/56384.html accessed on November 19, 2019.

Sen S. (2019). *A Decade of Aadhaar: Lessons in implementing a foundational ID system*. May, 2019, available at https://www.orfonline.org/research/a-decade-of-aadhaar-lessons-in-implementing-a-foundational-id-system-50464/ accessed on November 19, 2019.

The Wolfsberg Group. *The Wolfsberg Frequently Asked Questions on Risk Assessments for Money Laundering, Sanctions and Bribery & Corruption*. Available at https://www.wolfsberg-principles.com/sites/default/files/wb/pdfs/faqs/17.%20Wolfsberg-Risk-Assessment-FAQs-2015.pdf accessed on November 20, 2019.

UIDAI "Unique Identification Authority of India" (2018). *Enhancing Privacy of Aadhaar Holders – Implementation of Virtual ID, UID Token and Limited KYC.* Available at https://uidai.gov.in/images/resource/UIDAI_Circular_11012018.pdf accessed on November 19, 2019.

United Nations (2015). *Transforming our world: the 2030 Agenda for Sustainable Development*. Available at https://sustainabledevelopment.un.org/post2015/transformingourworld accessed on November 17, 2019.

UN High Commissioner for Refugees "UNHCR" (2017). *Principles on Identification for Sustainable Development: Toward the Digital Age.* February 2017, available at: https://www.refworld.org/docid/59db4aaa4.html accessed 6 November 2019.

United Nations System (2018). Personal Data protection and Privacy principles. December 2018, available at https://www.unsystem.org/personal-data-protection-and-privacy-principles accessed on November 20, 2019.

United Nations. *UN Legal Identity Agenda*. Available at https://unstats.un.org/legal-identity-agenda/ accessed on November 12, 2019.

Veridium (2019). *What is Two-Factor Authentication (2FA)?* Available at https://www.veridiumid.com/two-factor-authentication-2fa/ accessed on November 19, 2019.

White al. (2019). *Digital identification A key to inclusive growth*. McKinsey. Available at https://www.McKinsey.com/~/media/McKinsey/Business%20Functions/McKinsey%20Digital/Our%20Insights/Digital%20identification%20A%20key%20to%20inclusive%20growth/MGI-Digital-identification-Executive-summary.ashx accessed October 28, 2019.

Woodsome J. and Pisa M. (2019). *Overcoming the Know Your Customer hurdle: Innovative solutions for the mobile money sector*. GSMA, 2019, available at https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2019/02/Overcoming-the-KYC-hurdle-Innovative-solutions-for-the-mobile-money-sector.pdf accessed on November 19, 2019.

Woolley R. (2019). *KYC Utilities: The Promised Silver Bullet for Nordic Banks?* Finextra, 2019. Available at https://www.finextra.com/blogposting/17839/kyc-utilities-the-promised-silver-bullet-for-nordic-banks accessed on November 19, 2019.

World Economic Forum (2016). *A Blueprint for Digital Identity: The role of financial institutions in building Digital Identity*. http://www3.weforum.org/docs/WEF_A_Blueprint_for_Digital_Identity.pdf accessed on November 19, 2019.

World Bank (2017). *Technical Standards for Digital Identity*. ID4D, 2017. Available at http://pubdocs.worldbank.org/en/579151515518705630/ID4D-Technical-Standards-for-Digital-Identity.pdf accessed on November 14, 2019.

World Bank (2018). *World Development Indicators*. Available at http://datatopics.worldbank.org/world-development-indicators/ accessed on November 18, 2019.

World Bank Group's Identification for Development (ID4D) initiative (2018). *The Global ID4D Dataset*. https://datacatalog.worldbank.org/dataset/identification-development-global-dataset accessed on October 20, 2019.

World Bank (2018). *The Global Findex Database 2017*. https://globalfindex.worldbank.org accessed on November 17, 2019.

World Bank (2018). *Technology Landscape for Digital Identification*. Washington, DC: World Bank License: Creative Commons Attribution 3.0 IGO CC BY 3.0 IGO in 2018. Available at https://openknowledge.worldbank.org/bitstream/handle/10986/31825/Technology-Landscape-for-Digital-Identification.pdf?sequence=1&isAllowed=y accessed on November 12, 2019.

World Bank Group (2018). *G20 Digital Identity Onboarding*. Available at https://www.gpfi.org/sites/gpfi/files/documents/G20_Digital_Identity_Onboarding.pdf accessed on November 12, 2019.

World Bank Group (2019). *ID4D Practitioner's Guide*, (October 2019). Available at http://documents.worldbank.org/curated/en/248371559325561562/pdf/ID4D-Practitioner-s-Guide.pdf accessed 12 November 2019.

World Bank (2019). *Public Sector Savings and Revenue from Identification Systems: Opportunities and Constraints*. Available at http://documents.worldbank.org/curated/en/745871522848339938/Public-Sector-Savings-and-Revenue-from-Identification-Systems-Opportunities-and-Constraints.pdf accessed on November 15, 2019.

Zelazny F. (2012). The Evolution of India's UID Program: Lessons Learned and Implications for Other Developing Countries. *Center for Global Development Policy Paper 008*. Washington, D.C, available at https://www.cgdev.org/sites/default/files/1426371file_Zelazny_India_Case_Study_FINAL.pdf accessed on November 19, 2019.

Copies of publications issued by the Arab Monetary Fund may be requested from:

Arab Monetary Fund

P.O. Box 2818

Abu Dhabi, U.A.E.

Tel. : (+9712) 6215000

Fax : (+9712) 6326

E-mail: publications@amfad.org.ae

***Available in PDF format at: www.amf.org.ae**

http://www.amf.org.ae

صندوق النقد العربي
ARAB MONETARY FUND

أمانة مجلس محافظي المصارف المركزية ومؤسسات النقد العربية