Digital Identity eKYC and Remote Onboarding in Arab Countries

Arab Regional Fintech Working Group

No.
182
2022

صندوق النقد العربي
ARAB MONETARY FUND

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

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, eKYC and Remote Onboarding in Arab Countries

Arab Monetary Fund
April 2022

Acknowledgement

This policy guide was produced under the mandate of the Arab Regional Fintech Working Group (WG). The WG promotes the exchange of knowledge and expertise, strengthening the capacity of the Arab regulators, as well as building a network of Arab and international experts from the public and private sectors to promote the fintech industry and foster innovation.

The “Digital Identity, eKYC and Remote Onboarding in Arab Countries” paper was prepared by Nouran Youssef from the Arab Monetary Fund (AMF).

The document has benefited from valuable comments provided by the Arab Central Banks and Monetary Authorities members of the Arab Regional Fintech WG, and Harish Natarajan from the World Bank Group (WBG).

.

The opinions expressed in this policy paper are those of the authors from the Arab Regional Fintech WG members and do not necessarily reflect those of the entities they represent.

List of Abbreviations

AI	Artificial Intelligence
AML/CFT	Anti Money Laundering / Counter Financing Terrorism
APIs	Application Programming Interfaces
CDD	Customer Due Diligence
DFS	Digital Financial Services
DLT	Distributed Ledger Technologies
EMV Cards	Europay, Mastercard and Visa Cards
FI	Financial Institution
FSPs	Financial Service Providers
ML	Machine Learning
ML	Money Laundering
MNOs	Mobile Network Operators
TF	Terrorism Financing

TABLE OF CONTENTS

Introduction

Arab countries exerted lot of efforts to increase financial inclusion rates, which have already progressed since 2011, however more initiatives are needed to embrace digital financial inclusion; in order to enable the access and use of more tailored, affordable, and diversified financial activities. This is aiming to drive economic growth, reduce poverty as well as strengthen resilience to chocs such as job loss.

In the meantime, COVID 19 pandemic has accelerated Fintech and digital financial services (DFS) due to requirements of contactless and remote activities. Here, Digital ID plays a role at all stages of using financial services, since digital IDs allow for validation of a customer's identity with a higher degree of assurance, which in turn improve the reliability, security, privacy, and efficiency of identifying individuals in the financial sector. This is in addition to the significant decrease in customer onboarding costs.

Accordingly, regulators across the world are supporting the use of digital approaches and digital IDs by incorporating them into developing CDD & KYC requirements based on the risk assessment principle and risk-based approach. Applying a holistic digital ID framework and integrating it with CDD measures requires well designed policies and digital ID system design that fosters both inclusion and trust to mitigate several risks including technical challenges and risks of failure.

This paper elaborates on different approaches currently observed for ID verification in the financial sector. It discusses as well various challenges in adopting digital ID intensively in the financial sector including, but not limited to, the level of coverage of Legal ID, digital capabilities, pricing of the digital solutions, the efficiency and reliability of digital ID process, in addition to regulations governing the AML/CFT and identity frameworks.

In that space, Arab countries maintained various initiatives to adopt digital ID and eKYC/CDD frameworks in order to facilitate seamless financial activities, particularly remote onboarding following COVID-19 pandemic. These include, among others, adopting relevant regulatory frameworks, or amendments to existing regulations, testing new eKYC/CDD solutions within the regulatory sandbox, as well as validating the AMF/CFT compliance while assessing Fintech applications.

Furthermore, the paper draws some recommended actions for policy makers to enable Digital ID and CDD framework in a holistic and collaborative approach. The proposed set of considerations focus on five main policy areas coupled with their related implementing measures. These five building blocks are (i) the legal and regulatory framework supporting the usage of Digital ID by financial services providers (FSPs); (ii) identification of the full range of risks related to the usage of Digital ID by FSPs; (iii) adoption of consent mechanisms for customers; (iv) supporting collaboration with the private sector; and (v) ensuring a proper oversight framework for the Digital ID.

Drivers for Remote Onboarding in the Arab region

Onboarding represents the first customer interaction with the financial institution and will set the tone for the entire relationship. Technological advancements provide solutions to serve better the customer onboarding process, by making the identification and verification faster and matching the digital world, it promises improved experience for the users and better efficiency in the financial sector[1]. Moreover, the Covid-19 pandemic has accelerated the use of technology and the need for embracing digital financial services considering social distancing measures including increased need for customers' digital onboarding. These dynamics are relevant for the Arab region as well.

The extant Financial Action Task Force (FATF) standards governing the customer due diligence (CDD) and know your customer (KYC) requirements across the World, provides guidance on the responsible harnessing of the potential for technological solutions for CDD and KYC financial sector standards. Further the standards provide enough flexibility in applying a principle and risk-based approach to devising the CDD and KYC requirements. Many jurisdictions have leveraged these to formulate a tiered approach based on the risk assessment of specific types of transaction accounts and other contextual aspects. The features of the accounts in terms of maximum balance, types of transactions permitted are calibrated in line with the extent of the CDD and KYC processes performed. Regulators across the world are beginning to enable usage of digital approaches and digital IDs by incorporating them into this principle and risk-based approach. The increased focus on fostering greater use of digital payments in the context of the COVID-19 pandemic has given the emerging developments in many countries a major boost including in several Arab countries.

Fostering Financial Inclusion in the region

While it has been proved that financial inclusion reduces poverty rates and boosts economic growth, Fintech and digital financial services (DFS) play a major role in increasing financial inclusion rates in the Arab region due to the innovative remote methods in conducting financial activities, i.e. the ability to access, borrow, lend, insure, invest, transfer funds, and making or receiving payments.

Even though the Arab region is a young region, having 42 percent of its population between 15 and 40 years old, with 17% of the population fall between 15 and 24 years old, and this population is technology savvy; the region still needs to improve its digital capabilities to enhance access to formal financial services. This is also coupled with high unemployment rate, 13 percent on the average of the Arab countries, in addition to the high female unemployment rate reaching 21.4%, which counts for the double of the global rate.

All the above stress the need to bridge the financial inclusion gap by embracing Fintech and DFS as driver of the economy and remedy to efficient human resource allocation.

[1] / AMF. 2020. Digital Customer On-Boarding, e-KYC and Digital signatures in the Arab Region. February 2020.

Gaps related to Financial Inclusion in the Arab region

Arab countries rely on digital financial inclusion, considering the expansion of Fintech and digital financial services, to enable access to 63 percent of adult population in the region to formal financial services, in particular female, youth, micro small and medium sized enterprises[2].

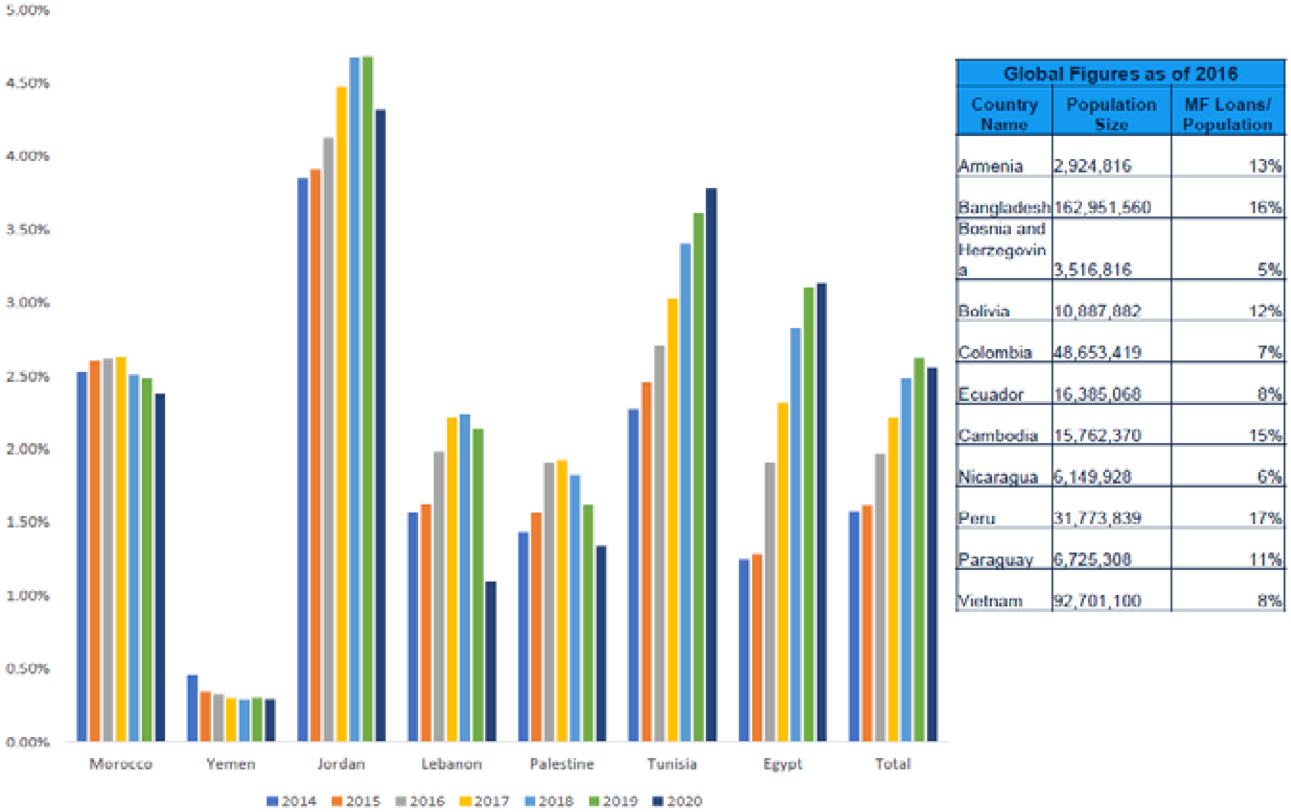
Despite the diversified initiatives conducted by Arab countries to enhance financial inclusion rates, which have already improved in general across the region in 2017 compared to 2014 and 2011, the region underperforms other world regions in access to both formal credit and savings. Where Arab countries in general achieved only 5% formal borrowing and 9% formal savings in 2017 compared to other regions like low-income countries which recorded 7% in borrowing and 11 % in savings in same year (Global Findex, 2017).

Digital channels can bridge this financing gap through reaching the un or underbanked population in the region, where 79% of young adults are unbanked, 72% of the poorest citizens can yet benefit from financial inclusion, 23% is the gap between women and men in access to services they currently need[3]. It also reported that almost 70% of adults lack access to formal credit due to their dependency on informal financial channels, mainly family and community, rather than formal financial institutions[4].

Another significant financial inclusion facet is the Micro Small and Medium-sized Enterprises (MSMEs) and the major role they play in supporting economic growth and reduction of unemployment. Although the MSMEs present 90% of the total entities operating in the Arab countries, and they contribute by more than 75 % to the gross domestic product, and constitute an interval of 10-49% in the employment rate, Arab countries achieve low rates of loans to the Micro Finance (MF) sector, since the percent of MF loans as a percent of population reaches almost 3 % on average; which stands behind other regions across the world as shown in the below.[5] This implies enhancing liquidity facilities and guarantees as main priorities of reforms areas to remove funding and liquidity challenges facing microfinance in the region[6].

[2] / AMF.2020. Annual Report of the Financial Inclusion for the Arab Region Initiative (FIARI), 2020.
[3]/ AMF.2019. Annual Report of the Financial Inclusion for the Arab Region Initiative (FIARI), 2019.
[4]/ Chehade et al. 2017. Financial Inclusion Measurement in the Arab World, Working Paper, CGAP and the Arab Monetary Fund's Financial Inclusion Task Force.
[5]/ Khaled, M. 2020. "Microfinance Roundtable: Call to action for Arab Stakeholders", IFC presentation, 20 May 2021.
[6] / AMF. 2021. Survey on "Discussing Policies Priorities in Microfinance" - FIARI, May 2021.

Figure 1. Micro Finance borrowers as a % of Population



Global Figures as of 2016		
Country Name	Population Size	MF Loans/ Population
Armenia	2,924,816	13%
Bangladesh	162,951,560	16%
Bosnia and Herzegovin a	3,516,816	5%
Bolivia	10,887,882	12%
Colombia	48,653,419	7%
Ecuador	16,385,068	8%
Cambodia	15,762,370	15%
Nicaragua	6,149,928	6%
Peru	31,773,839	17%
Paraguay	6,725,308	11%
Vietnam	92,701,100	8%

Source: IFC presentation at the Roundtable “Microfinance: Call to action for Arab Stakeholders” in May 2021.

Digital Financial Services

Mobile phone services cover approximately 65% of the population in the region. There are currently more people having mobile phone accounts than owning bank accounts. Mobile services accounted for 6% of the region’s GDP in 2019[7].

It is worth noting the progress expected in the mobile phone services market in the region over the next five years, where mobile broadband connections are expected to reach half a billion by 2021, subscription to mobile internet services are expected to exceed half of the population by 2023, and mobile connections will reach 700 million by 2025; which implies an average adoption rate of 80%[8].

In this context of acceleration in adoption of mobile telephony across the Arab region, Digital

[7]/ GSMA. 2020. The Mobile Economy Middle East & North Africa 2020. https://www.gsma.com/mobileeconomy/wp-content/uploads/2020/11/GSMA_MobileEconomy2020_MENA.pdf

[8]/ Ibid 7.

Financial Services (DFS)[9] have the potential to expand access to financial services in the region, thereby improving financial inclusion rates. Firstly, as they enable rapid and secure mean to distribute social transfers and financial support to vulnerable people, particularly in cases where movement around the country is limited or unsafe.

Second, DFS can also support alleviating challenges related to demand and supply sides, so as to deliver affordable and suitable financial services to the fragile segments of the population. For the demand side, DFS can overcome impediments emerging from the lack of documentation, volatile and small incomes, geographical barriers, as well as literacy and trust. On the supply side, DFS can eliminate many of the hurdles including the high operating costs, legacy business models, limited competition and innovation[10].

Digital ID as key enabler to fully harness the potential of DFS

Digital ID enables regulators to simplify the Customer Due Diligence (CDD) requirements and lower the cost for DFS providers, without compromising on safety and integrity[11] [12]. In response to the lack of adequate documentation available to the poor, many countries have adopted a tiered approach to CDD – wherein some basic accounts, including mobile money, can be opened with a reliable official identity document or, in some cases, even with a letter from a community leader.

The availability of an official ID that is universal, enables meeting the CDD requirements for the lower tiers very straightforward. The availability of a Digital ID simplifies the process further by enabling the verification to be done remotely or at an agent location and removing the need for maintaining paper records and copies. In Bangladesh, a recent study by Bangladesh Banki showed that eKYC would reduce the time to onboard a customer from 4-5 days to 5 minutes. Further, digital ID is increasingly becoming central to the effectiveness of fintech models like open banking. Open banking relies on strong customer authentication to secure customers' consent for accessing their data and accounts. Digital ID can be leveraged for developing an industry-wide common, strong customer authentication infrastructure instead of each institution developing their own.

All this however requires progress on expanding coverage of an official ID, enhance its digital capabilities and introduce suitable changes to regulations governing CDD to enable remote onboarding and digital ID frameworks.

[9] Digital financial services cover financial products and services, including payments, transfers, savings, credit, insurance and securities delivered via digital/electronic technology such as e-money (initiated either online or on a mobile phone), payment initiation services, payment cards, online lending and regular bank accounts.

[10]/ Pazarbasioglu, Ceyla et al. 2020. Digital Financial Services, WBG, April 2020.
https://pubdocs.worldbank.org/en/230281588169110691/Digital-Financial-Services.pdf

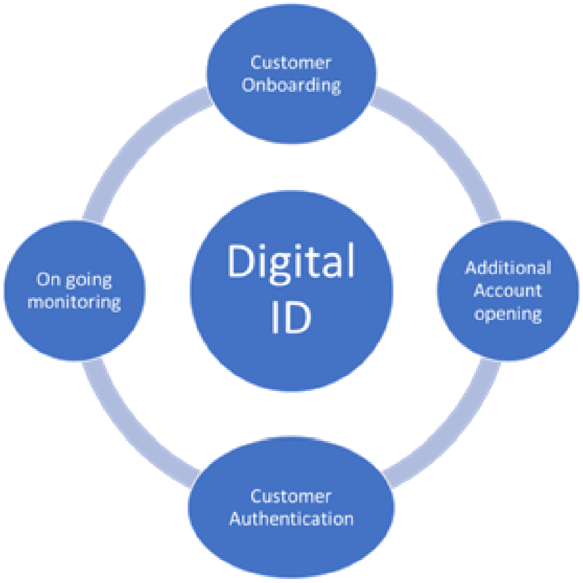
[11] Pazarbasioglu, Ceyla et al. 2020. Digital Financial Services, WBG, April 2020.

[12] G20. 2018. G20 Digital Identity Onboarding, WBG, 2018.
https://www.gpfi.org/sites/gpfi/files/documents/G20_Digital_Identity_Onboarding.pdf

Digital ID in financial sector

Digital ID plays a role at various stages when using financial services. It makes it (1) easier for the unbanked to open a transaction account which also enables efficient disbursement of social benefits, (2) enables cost-effective onboarding that can be done remotely by the FSP and (3) contributes to the deepening of the financial sector by supporting take-up of additional products and services.[13] Furthermore, digital IDs allow for validation of a customer's identity with a higher degree of assurance than those using manual or paper-based processes. In addition, with a Digital ID, such validation of customer's identity can -in many cases- be completed instantaneously[14]. Some studies have reported digital ID–enabled processes have the potential to reduce customer onboarding costs by up to 90 percent.[15]

Figure 2. Digital ID usage in financial services



[13] G20. 2018. G20 Digital Identity Onboarding, WBG, 2018. https://www.gpfi.org/sites/gpfi/files/documents/G20_Digital_Identity_Onboarding.pdf

[14] Currently some practices rely on verification of paper-based ID system and credential with a photo under remote account opening scenarios which allow for 'real-time' identity verification of the customer (e.g. by examining the credential and comparing the photo to the person presenting it), however the level of assurance would likely be lower than in the case of a digital ID system.

[15] McKinsey. 2019. Digital identification: A key to inclusive growth, April 2019. https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/digital-identification-a-key-to-inclusive-growth.

Digital ID use for onboarding:

The term digital ID is not a precise term as it encompasses a range of approaches through which one can prove his/her identity online. The G20 Digital Onboarding report issued in 2018[16] uses the following definition - A set of electronically captured and stored attributes and/or credentials that uniquely identify a person. A digital ID needs to have official recognition for it to be useful in the financial sector – perhaps in recognition of this, the FATF used the following definition in the guidance on digital ID issued in April 2020[17] – "Digital ID systems use electronic means to assert and prove a person's official identity online (digital) and/or in-person environments at various assurance levels."

Driven by the rapid growth in digital financial services which requires a better understanding of how individuals are being identified and verified in the world of digital financial services, the FATF released their Guidance on Digital ID[18] in 2020.

However, despite the active interest in developing Digital ID systems there are just a few countries that have effectively developed a comprehensive approach to Digital ID. Finally, in the absence of such measures, FSPs have developed systems that provide higher level of assurance through the adoption of e-KYC mechanisms that include supplementary data and external data sources.

The approaches currently observed in the financial sector for ID verification in the context of onboarding of a new customer can be broadly grouped into In-Person authentication and Remote authentication. These are discussed below.

In person authentication

This approach involves scenarios where the individual appears and presents ID credentials in person. The authentication process would depend on the features offered by ID systems. Broadly there could be two types of authentication – one based on capturing biometric attributes and matching against the ones captured during ID issuance process; and the other based on validating PIN or passcode issued against the ID. These authentications could be further grouped into online or offline – in the former case the biometric or PIN is transmitted online for authentication by a system and in the latter case the authentication can be completed entirely offline. The latter case necessarily require availability of a physical credential, often in the form of a chip card.

Remote authentication

Remote authentication approaches as the name suggests involve the authentication process being carried out remotely without the person having to visit any particular location physically. Five different remote authentication options have been observed.

[16] https://documents.worldbank.org/en/publication/documents-reports/documentdetail/362991536649062411/g20-digital-identity-onboarding

[17] http://www.fatf-gafi.org/media/fatf/documents/recommendations/Guidance-on-Digital-Identity.pdf; p. 19

[18] Guidance on Digital ID: https://www.fatf-gafi.org/publications/fatfrecommendations/documents/digital-identity-guidance.html

- **Online validation of biometric**: In this approach using devices conforming to the standards based on which biometrics were captured during registration are used by the individual to capture and transmit the biometric to ID verification service provider through the financial institution. The financial institution would in general embed this within its system and processes. A variant of this could be offline validation of captured biometric against recorded biometric in a physical credential – for e.g. chip in an ID card and the result then communicated online.

- **Online validation using PIN/Password:** This is broadly similar to the biometric approach, the difference being use of PIN/Password instead of biometric. The PIN/Password can be a static or dynamic. The latter would involve unique code transmitted by the ID service provider to a pre-registered device or generated by the individual using a device/software configured and synchornised with the ID service provider.

- **Online validation using digital certificates**: This approach involves asserting identity using digital certificates that has been issued to the individual by the financial service provider or other eligible institutions. A simple version of this process could be for the individual to simply sign the onboarding application digitally and transmitting that to the financial service provider. Other approaches involve using digital certificate in a challenge-response process. The digital certificate could be provisioned in a variety of devices.

- **Verification of ID and online matching against physical ID**: This is observed in country contexts where the ID verification service is only able to validate the demographic attributes like name, address, and date of birth but not biometrics or PIN/Passcode. The individual is asked to provide the details in the physical ID credential and also present oneself on a video recording holding the physical ID credential. The ID service provider then programmatically compares the photo in the physical ID credential with the video captured of the individual and further validates the ID information against the ID system. The financial service provider is provided a response on the level of confidence in the authentication of the individual.

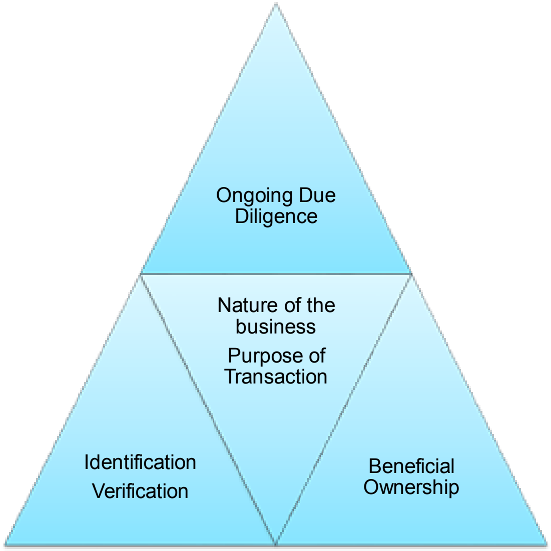
- **In person verification combined with online validation of ID documents produced**: This simple hybrid approach requires the individual to present oneself in person with a physical ID credential. The details in the ID credential are then validated online. This approach validates the authenticity of the ID credential but relies on visual inspection of say the photo in the ID credential, to ascertain whether the individual presenting the ID is the same individual.

Digital ID and FATF regulations

During account opening, a customer is required to provide information necessary though not necessarily ID credentials to establish identity so that the FSP can carry out one of the customer due diligence (CDD) dimensions. The term CDD is frequently interchanged with Know your Customer (KYC) although CDD entails more requirements that just identifying the customer -or the one that on a legitimate basis acts on its behalf- and verifying such identification. Amongst authorities and financial service providers there is a preference for formal or officially recognized proof of identification through strictly speaking as per the FATF standards other approaches that can lead to same outcome would be acceptable as well.

As per the illustration below, FATF Recommendation 10 entails 4 dimensions consisting of (i) identifying the customer and verifying the customer's identity, (ii) identifying the beneficial owner, (iii) understanding the purpose and nature of the business relationship and, (iv) conducting ongoing due diligence on the business relationship ensuring consistency of risk profile, source of funds, and knowledge of the customer by the Financial Institution (FI). However, for the purpose of this note the focus will be on the identification and verification dimension of CDD, recognizing that all other dimensions are relevant.

Figure 3- Dimensions of CDD under Recommendation 10



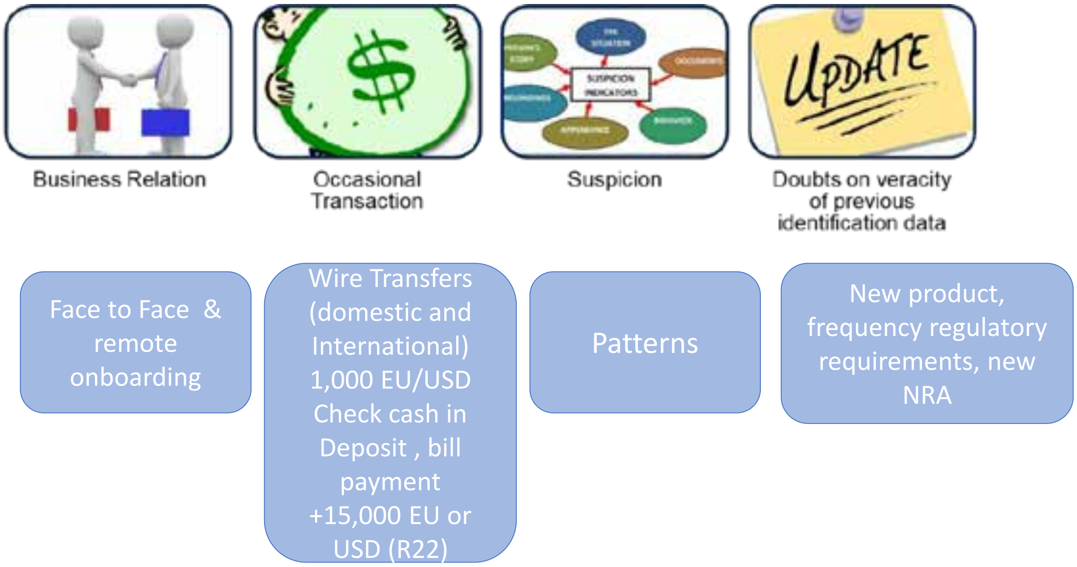
Furthermore, recommendation 10 of the FATF establishes that Financial institutions (FIs) should be prohibited from keeping anonymous accounts or accounts in obviously fictitious names. Also, FIs should conduct CDD under the following circumstances (see Figure 4 below)

(i) Establishing business relations (i.e. onboarding of new clients);

(ii) Carrying out occasional transactions above 15,000 USD-EUR; or

(iii) Electronic Transfers based on interpretative note (IN) R16[19]; For cross-border wire transfers countries may adopt a *de minimis* threshold not higher that 1,000 USD/EUR where information on name of originator, beneficiary and account number is required but verification is not necessary.
(iv) Suspicion of illegal activity of Money Laundering (ML) or Terrorism Financing (TF);or
(v) When the FI has doubts about the veracity or adequacy of previously obtained customer identification data

Figure 4- Illustration of scenarios that require CDD Measures under FATF Recommendations


UpDATE
Business Relation
Occasional Transaction
Suspicion
Doubts on veracity of previous identification data
Face to Face & remote onboarding
Wire Transfers (domestic and International) 1,000 EU/USD Check cash in Deposit , bill payment +15,000 EU or USD (R22)
Patterns
New product, frequency regulatory requirements, new NRA

FATF standards are applicable for both traditional and digital financial services. In many developing countries the primary pathway to financial inclusion is often via a mobile wallet or e-money account or basic bank accounts. Therefore, the enrolment process -including identification of customers- of Mobile Network Operators (MNOs) and at agent locations is very relevant to onboard customers on basic transaction accounts.

Digital ID systems have the potential to improve the reliability, security, privacy and efficiency of identifying individuals in the financial sector, to the benefit of both customers and regulated entities. However, they also present a variety of technical challenges and risks of failure. Well-designed policies and digital ID system design that fosters both inclusion and trust are fundamental to mitigating such risks and guarding against challenges.

[19] R16 establishes that FIs are required to collect accurate originator information and beneficiary on cross-border wire transfers and domestic wire transfers including serial payments and cover payments.

Integrating new technologies in CDD/KYC measures

Innovative technology promotes financial inclusion considering enabling more financially excluded segments and to provide robust AML/CFT framework. Since innovative technologies can improve data collection, processing and analysis processes, they can best support compliance with AML/CFT requirements and mitigate effectively the related risks from one hand, from the other hand, they enhance regulatory and supervisory authorities' mandate and support overcoming AML/CFT challenges.

While use of new technologies can improve risk assessments, onboarding practices, reporting and governance processes for regulated entities, it can also help detecting suspicious activities in a timely manner. Similarly, these technologies can strengthen supervision based on informed oversight and real-time monitoring.

Adoption of diversified technologies can enhance all stages of AML/CFT processes, whether use of Artificial intelligence (AI) and machine learning (ML), or Application Programming Interface (APIs), or even the Distributed Ledger Technology (DLT).

For instance, AI and machine learning solutions can eliminate human intervention and automatically monitor, process and analyze suspicious and illicit activities. In addition, they can produce more accurate and comprehensive and updated assessments of ongoing customer due diligence and customer risk in real time. AI and ML techniques are also relevant for the image recognition and liveness detection used in some identification methods. Further, the Application Programming Interface (APIs) solutions allow direct communication between supervisory authorities and regulated entities and their customers, as well as communications among regulated entities, and between them and their customers, which accelerate alerts and reports follow ups.[20] Moreover, DLT and Blockchain technologies allow for different ways of managing digital identities, as they provide innovative solutions for identity authorization, verification and personal data management. It would follow a decentralised model of ownership, management, representation and attestation of the identity.[21]

In addition, monitoring CDD procedures can be improved by managing transactions via a single ledger shared between many institutions, or via interoperable ledgers, in addition, transaction data can be better stored and traceable. The distribution of transaction data between several institutions provides better input in identifying suspicious transaction patterns. This would imply significant cost savings for financial institutions, better experience for customers and higher quality of data. Here, financial institutions in China draw a leading example, where they use DLT to share watch lists or red flags depending on the level of confidentiality permitted by the system[22].

[20]/ FATF. 2021. Opportunities and Challenges of new technologies for AML/CFT, July 2021. https://www.fatf-gafi.org/media/fatf/documents/reports/Opportunities-Challenges-of-New-Technologies-for-AML-CFT.pdf
[21]/ AMF.2021. Strategies for adopting DLT/ Blockchain Technologies in Arab Countries, August 2021.
[22]/ Ibid 21.

Furthermore, the innovative technologies play major role in enhancing internal assessments, internal reporting and supervisory capacity via the Regtech/Suptech solutions to fulfill the AML/CFT obligations and supervise their compliance. As Regtech solutions can enable the collection and shaping of high velocity, diverse types and large volumes of data in a fast and integrated manners for a smooth automated extraction of actionable data. Also, Regtechs can ensure the "check" role via its feedback loop that identifies if reports have been submitted correctly, accurately, on time and to the correct supervisor.[23]

Challenges with remote onboarding

There are several challenges in adopting digital ID intensively in the financial sector. This section discusses the key challenges.

Coverage of Legal ID: As noted before for a digital ID to be useful in the financial sector there are needs to be official recognition of the underlying ID –i.e. the digital features need to be built on top of some form of legal ID or alternatively the Digital ID itself is either recognized by the Government or certified by a government recognized entity[24]. The limited penetration of legal ID could be a major challenge in broader adoption of digital ID in the financial sector.

Digital capabilities: Even when the legal ID has universal or near universal coverage, the digital capabilities offered by the legal ID could be limited and that could also pose challenges. However as noted in the earlier section, even in the absence of digital features, some solutions can be developed as long as the ID has legal backing and is widely accepted as reliable. The key digital capabilities of legal ID that could be particularly relevant are: (i) ability for online or offline authentication; and (ii) ability to validate critical attributes of the ID online. Presence of even one of these features can be adequate.

Process efficiency and reliability: For digital ID to be useful the process needs to be efficient for both the FSP and the customer and there must be a very high degree of confidence in the reliability of the overall process.

Pricing: In many cases, the digital ID solutions are provided by some external entity – either in the public sector or industry utility or as a contracted service from a service provider. Irrespective of who provides the service, these would likely be provided on commercial terms. The pricing will need to be low relative to the overall cost of alternative processes and relative to the expected returns from the particular consumer's relationship.

Regulation: The AML/CFT regulations have a significant impact on how the onboarding and

[23/] Ibid 21.

[24] FATF, April 2020

customer verification procedures are designed. In some jurisdictions, regulations can be very prescriptive on what forms of ID are acceptable and in what mode. Regulations pertaining to consumer protection, data protection and privacy and outsourcing could also have a bearing- For example, consumer protection measures might necessitate a particular mode of securing consent from customer; data protection and privacy regulations might have a bearing on what data can be sought from the customer and what information can be shared by other institutions; and outsourcing regulations might specify if and what aspects of the KYC and CDD processes can be outsourced.

Different countries' experiences in deploying ID systems

As mentioned earlier, allowing electronic means to verify identity foster remote onboarding, and boost CDD procedures, then, remove barriers to financial inclusion by getting into official system more people from various vulnerable segments.

Moreover, a digital identity would minimize weaknesses in human control measures, allow for live transactions monitoring (whenever the digital identity has been accessed), provide a more user-friendly experience and save costs.

The below table illustrates different countries' experiences to promote digital identity and verifications systems of such identities. It also shows the remote signing in and respective approaches of integration with CDD/KYC requirements.

Table 1 – Digital ID Systems worldwide and integration with CDD/KYC measures

Countries	Digital ID System	Remote Signing in Method	Integration with CDD/KYC requirements	Identity verification	Additional Measures
Brazil	National Digital Identification (NDI): using biometric attributes, such as fingerprints, based on social security number as the main proof of ID for Brazilians	Biometric attributes, such as facial recognition, short videos, in addition to fingerprints	Brazil Central Bank (BCB) Open Data Portal. The platform allows customers with authenticated digital ID to remotely open & manage banks accounts	Used behavioral, geographical and biometric techniques for ID verification.	The BCB launched, in collaboration with other financial regulators, an information sharing platform based on blockchain techniques.
Bangladesh	National Identity Database (NID) includes biometric information. Smart national ID cards includes 10 fingerprints and iris biometric features. Mobile network operators developed a biometric identity system via SIM cards that can be verified against national identity database.	Biometrics used by agent banking to onboard consumers through scanning the fingerprints.	Biometrics attributes are used to verify identity against national database.	Biometrics used to verify identity against national identity database.	Government provided refugees from Myanmar identity by registering them biometrically and integrating them into the national database.
India	Unique digital IDs (Aadhaar), a 12-digit number issued to all India residents. Aadhaar uses demographic information and biometric data, i.e. fingerprints, iris and face	Digital onboarding by integrating the Aadhaar ID, bank accounts. This is in addition to the planned integration with mobile payment systems, namely United	Integrating Aadhaar system with e-KYC service to enable service providers to verify individual information through Aadhaar number.	The CDD data is shared with regulated entities in a real time upon customers' consent. A Central KYC records registry (CKYCR) is	Aadhaar Enabled Payment Systems (AEPS) is used in distributing of government benefit transfers using

	recognition; which permit identity verification and authentication.	Payment Interface (UPI), Bharat Interface for Money (BHIM), and Aadhaar Enabled Payment Systems (AEPS).		used as shared database across the financial sector.	Aadhaar authentication.
Nigeria	The National Identification Number (NIN), is an eleven digits number that uses individual's biometric and demographic identity data to one secure, digitally accessible number on the National Identity Database.	The Bank Verification Number (BVN) methodology: a Unique Individual Identifier. It uses biometric features, namely fingerprints, facial recognition, and a digital signature.	The BVN is a Unique identification number linked to centralized verification system that is hold by the Central Bank of Nigeria, can be used by all financial institutions in Nigeria. The BVN is operated by Nigeria Interbank Settlement System (NIBSS)	The BVN as a centralized biometric data base used by all financial institutions in Nigeria, in addition, it is accessible by mobile money operators and law enforcement agencies.	The e-ID card is a physical token that can be used to authenticate individual identity across many public & private services. It can only be issued to Nigerians registered into the National Identity System and Legal Residents who have attained the age of 16 years and above.
Peru	National ID (DNI): Personal Unique Identity Number; and an electronic ID (e-DNI). Which is biometric and allows for digital signature and faster processing of information.	e-DNI is a biometric card using fingerprint.	Tiered KYC system, where three tiers exist depending on the product, which vary between money, simplified deposit accounts, and the general tier. This is in addition to the enhanced	e-DNI serve as base for authentication in the mobile connect platform (BiM) for mobile transactions including access to websites and applications.	National Payment Platform "BiM". BiM is an interoperable mobile money system.

			tier if the person is politically exposed[25].		
Pakistan	NADRA's (National Database and Regulation Authority) digital ID uses biometrics to ensure Unique ID numbers for Pakistani citizens above 13 years old. The unique 13 digits number is based on a Computerized National Identity Card (CNIC).	The Computerized National Identity Card (CNIC) is used for opening accounts, receiving remittances, in different government programs and with private sector.	Biometric information linked to the CNIC are used to validate NADRA's identity.	The NADRA's digital ID is used for identity verification by validating basic biometric information linked to the CNIC. PTA (Pakistan Telecom Authority) and MoIT (Ministry of Information Technology) introduced the Biometric Verification System (BVS) that requires cell phones' owners to biometrically verify their ID against the NADRA database.	The CNIC facilitated various G2P payments. Also, the electronic Credit Information Bureau (eCIB) allowed credit information linked to CNIC via NADRA verification and authentication online process.
Russia	National biometric database to identify both citizens and foreign nationals via face recognition and fingerprints.	The Bank of Russia developed the digital biometric identification system, using face and voice recognition data, to enable financial services remotely.	Unified System of Identification and Authentication (USIA), a centralized database of identity information to enhance verification and customer due diligence	The Unified Biometric System, together with the Unified System of Identification and Authentication (USIA), are used to ensure reliable customer	

[25]/ AFI. 2019. KYC Innovations, Financial Inclusion and integrity in selected AFI member countries, AFI Special Report, March 2019.

			under FATF's risk-based approach.	identification and verification	
Singapore	**SingPass** (Singapore Personal Access), is the national digital ID system, and a platform that provide access to over 340 government agencies and private sector services. **SingPass Mobile**, is a mobile application that allows users to log in to SingPass with their fingerprint, facial recognition or a 6-digit passcode.	SingPass enables its holders to conduct transactions seamlessly and securely with public and private sectors' digital services via biometric verification to authenticate themselves. Financial institutions can use Myinfo, which allows SingPass users to auto-fill selected personal details onto forms online, to streamline customer on-boarding, with the customer's explicit consent. Myinfo business is an extension of Myinfo that includes corporate data.	Biometric authentication technology permits secure identity verification when accessing diverse range of government and commercial services.	Various digital initiatives like the SingPass Mobile, MyInfo and MyInfo Business are using biometrics, such as facial recognition and fingerprints, in addition to QR code for login, verification, authentication, as well as digital signature.	The Singapore Government is currently developing a National Digital Identity (NDI) platform, as an extension from the SingPass authentication system. The NDI serves as a secure and trusted digital credential, as well as a platform for authentication, authorization and consent.

Sources: AFI, 2019. WBG, G20, 2018. MAS, 2020. https://www.singpass.gov.sg; and authors' illustration.

Current landscape in the Arab region

Many Arab countries have adopted diversified initiatives to embrace digital identity and/or eKYC/CDD frameworks. These efforts have been accelerated during 2020 to cope with COVID-19 repercussions.

As part of the COVID-19 response, Arab countries exerted various efforts to enable eKYC and digital ID frameworks, to support the access to financial services. The ongoing focus on promoting Fintech developments, which also rely on digital ID, has provided a further impetus. Six Arab countries - UAE, Bahrain, Tunisia, Saudi Arabia, Oman, Palestine - reported deploying digital ID arrangements to improve Fintech adoption in their national markets according to the Fintech survey of Arab countries –FinxAr – conducted in 2021.

In addition to harnessing the opportunities coming from digital ID, Arab countries also see digital ID as a means to effectively address Money Laundering / Financing of Terrorism (ML/FT) risks. According to the FinxAr survey, ten Arab countries, representing 83% of the Arab countries respondents to this question, recognize ML/FT risks as potential challenge related to Fintech activities; which requires response from regulatory and supervisory authorities to mitigate such risks.

Figure 5- Perceptions on ML/FT Risks related to Fintech activities

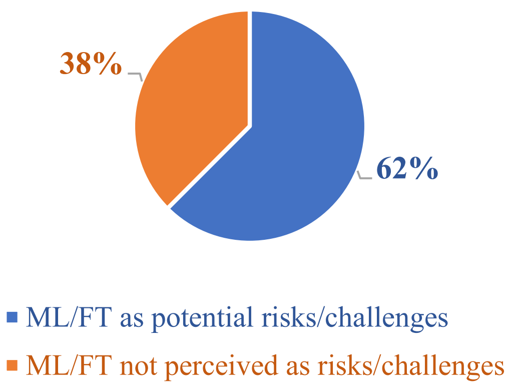


Table 2- Arab regulators' Responses to ML/FT risks related to Fintech activities

Countries	Arab regulators' Responses to ML/FT risks related to Fintech activities
Jordan	Offering AML/CFT instructor to Fintech companies under the sandbox.
Bahrain	Enhancing capabilities of the national eKYC platform using APIs and Cloud, and its integration to the banking systems & and smart phone applications; as well as expending its scope to all businesses.
Kuwait	Strengthening Fintech companies' compliance with AML/CFT measures.
Qatar	Check AML/CFT compliance by committee member when approving Fintech applications.
Egypt	Simplified eKYC rules – experimenting "Valify" eKYC solution in the sandbox.

This has motivated a range of initiatives – for example amendments to existing regulations, testing new eKYC/CDD solutions within the regulatory sandbox, and checking the AMF/CFT compliance while assessing Fintech applications. Jordan, UAE, Bahrain, Palestine, Kuwait, and Egypt focus their reactions to ML/FT risks related to Fintech activities through adapting the regulatory framework, in addition, Egypt went for requiring testing new eKYC/CDD solutions in the regulatory sandbox. Qatar included an AML/CFT expert in the committee that evaluates all Fintech applications[26]. Table 3 summarizes the Digital and eKYC initiatives across the Arab region.

Table 3- Arab countries Initiatives related to Digital Identity and eKYC

Countries	AML/CFT legislations	eKYC regulations	eKYC arrangement	Digital ID regulation	Digital ID arrangement
Jordan	✓	Instructions for Regulating KYC Procedures and dealing with him electronically.	See JoPacc project study case		
UAE	✓		UAE Blockchain KYC Platform		"UAE Pass" app. for digital ID & signature, through a smartphone-based authentication.
Bahrain	✓		National eKYC platform		
Tunisia	✓		"Kaoun" an eKYC solution. "Hannibal platform" Regtech solution for cross-border foreign currencies.	Unique Identifier for both citizens and companies.	Digital Onboarding using (OCR) technology
Algeria	✓				Digital biometric ID card for e-government services

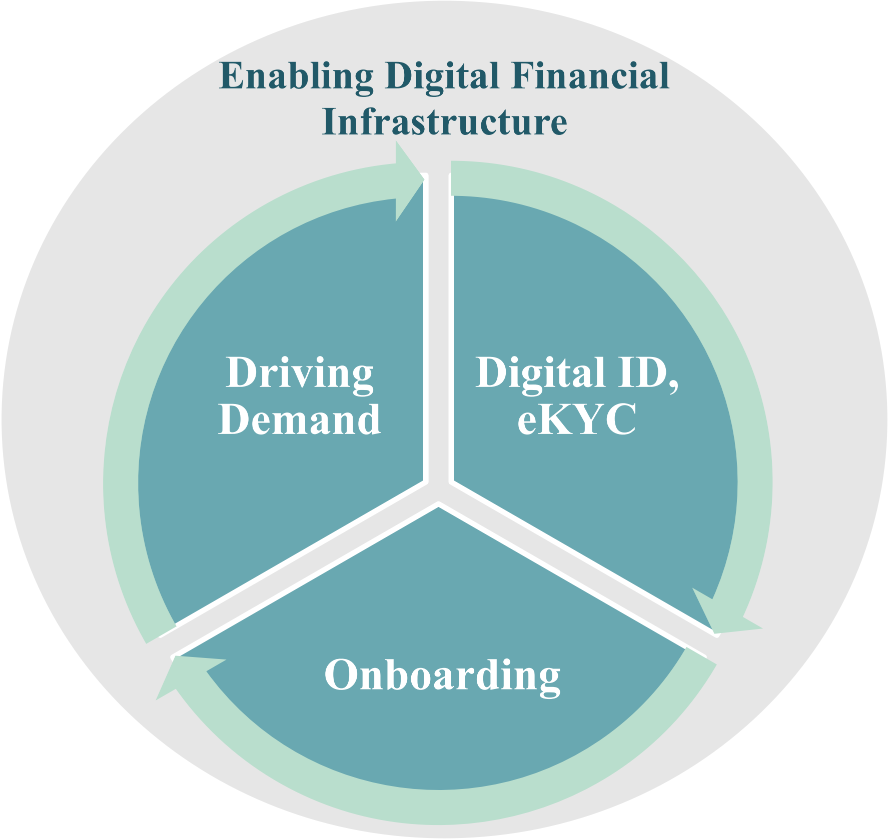
[26]/ Arab countries contributions to the "FinxAr" survey (Fintech Index for the Arab Region).

KSA	✓	eKYC protocols applied to all financial institutions (including fintechs within the regulatory sandbox[27])	eKYC procedures as financial market infrastructure		
Sudan	✓				
Iraq	✓			Digital ID instructions	Qi cards (biometric pre-paid cards)
Oman	✓	Simplified eKYC			
Kuwait	✓			Kuwait mobile civil ID application “Hawyati“	
Qatar	✓	In process	Checking AML/CFT when approving Fintech solutions	In process	
Egypt	✓	Simplified eKYC procedures for individuals & merchants.	Under testing within the regulatory sandbox		
Morocco	✓	Simplified remote onboarding for payment institutions and merchants. - Banks proceed eKYC for account opening			

This has also been reflected in putting in place the proper legal and/or regulatory regime governing the AML/CFT and CDD measures, where six Arab Countries, namely Bahrain, Tunisia, Saudi Arabia, Oman, Egypt, as well as Morocco, have specific regulations for simplified or electronic KYC/CDD.

[27]/ AMF. 2021. Responses to the survey for Fintech Index for the Arab Region “FinxAr”, 2021

Figure 5- Illustration of interconnection between digital onboarding and driving demand



Source: Author Illustration.

Regarding the current infrastructure supporting customers' remote onboarding such as digital ID system, and/ or eKYC procedures, two Arab countries employ both arrangements, which are UAE, and Bahrain; while four other Arab countries, namely Tunisia, Saudi Arabia, Oman and Egypt; adopt simplified or eKYC procedures to accommodate remote onboarding. Kuwait has deployed digital ID system. Central Bank of Iraq is currently working with a leading development financial institution to initiate eKYC project.

A high-level stocktaking of recent trends regarding the digital ID and eKYC in Arab countries is presented below..

In **Jordan**, the Central Bank of Jordan (CBJ) issued special instructions for "Regulating Know your Customer Procedures and dealing with him electronically", which permit banks and electronic payment and money transfer companies to register their clients electronically through applying the requirement specified in these instructions. These requirements involve the minimum procedures banks and Payment Service Providers (PSPs) must apply to verify and authenticate persons who intend to open an account remotely. Instructions are targeting only natural persons at this stage and will be extended to legal persons when the infrastructure of Jordanian market get mature enough and satisfy CBJ assurance levels.

The UAE adopted in 2019 a national digital identity/ID for the UAE, UAE-PASS, and is a foundational pillar in the country's journey towards digital transformation. It enables citizens, residents and visitors to create a secure digital identity that can be used to seamlessly access all public and private digital services in the country from the mobile app and using a single credential. With UAE-Pass, customers can also digitally sign transactions and documents using their digital certificates. Moreover, UAE-Pass will provide customers with a digital vault that allows them to request, share and store all their government issued credentials/e-documents securely in their mobile phones[28].

UAE-Pass is built on a national secure public key infrastructure, and it utilizes the country's identity systems as trust anchors. It is due to this level of security that CBUAE endorsed the usage of UAE-Pass for banking and financial institutions for customers' onboarding process.

Another development in UAE, the UAE Blockchain KYC Platform; which reflects a collaborative ecosystem transforming ease of doing business, remote onboarding and compliance. The platform allows seamless registration and onboarding as well as better compliance, enforcing a Single Version of Truth across the ecosystem. It also adheres to key UAE federal laws regarding data privacy, implementation of AML Law, as well as blockchain technology regulation.

The initial set of institutions on the platform are Mashreq Bank, Dubai Financial International Center (DIFC), ENBD, Emirates Islamic, HSBC, ADCB, CBD, RAKBANK, and Dubai Economic Department (DED); and second wave of banks are in the process of joining the platform. The ecosystem will be governed by a consortium of members, whereas CBUAE and Smart Dubai will oversee network formation and architecture as well as ecosystem governance and compliance standards.

Moreover, **Kuwait** have applied in 2020, an ID authentication and verification through the mobile and QR code via "Hawyati" application. Issued by the Public Authority for Civil Information (PACI). The Kuwait Mobile ID application provides citizens and expats in Kuwait a digital representation of their Civil ID through a simple download and update of their details into the application. The digital Civil ID aims to provide a portable mobile based Civil ID for identity verification, authenticating government and non-government e-Services such as renewing driver's license, in addition to a trusted Digital Signature of electronic documents and transactions[29]. By late 2020, Hawyati has attracted more than 960,000 users, including individuals, private businesses and government institutions[30].

In **Oman,** the central bank of Oman has permitted banks to digitally onboard their clients through simplified eKYC for mobile wallets and prepaid cards[31].

[28]/ AMF. 2021. The Arab Region Fintech Guide, the CBUAE contribution to the guide survey, June 2021.
[29]/ PACI. 2020. https://hawyti.paci.gov.kw/English
[30]/ KUNA. 2020. Kuwait News Agency, 2 December 2020.
https://www.kuna.net.kw/ArticleDetails.aspx?id=2942695&language=en
[31]/ AMF. 2020. Digital Customer On-Boarding, e-KYC and Digital signatures in the Arab Region, February 2020.

While **Iraq** used the biometric ID data, fingerprints[32], for offline customer authenticity at the pre-paid cards of the public sector payments “Qi cards”, where approximately seven million Iraqis can receive salaries and welfare benefits through their Qi cards. It worth mentioning that Qi cards are arranged through the International Smart Company (ISC)which is working on replacing the Qi cards with EMV standards cards. The strategy of Central Bank of Iraq in digital ID and e-KYC is depending on interoperability concepts and establishing an eKYC pool. So that to issue clear concepts which depend on sharing of the information of national ID, establishing an e-KYC entity, and issuing the digital onboarding instructions for digital banking services.

Similarly, **Algeria** has launched a digital biometric ID card in 2016, which allows digital access to government services such as passport issuance, tax collection, as well as voting registration[33].

Most recently, **Tunisia** have issued in May 2020 a government decree setting the technical specifications of the Citizen's Unique Identifier, providing a unique identifier for both citizens and companies, which was in accordance with Tunisia’s e-government vision. Also, the Central Bank of Tunisia has implemented a regulatory sandbox to support Fintech in the development of new digital financial solutions including the eKYC process[34].

Another development is “Kaoun”, which is a Tunisian eKYC solution that enables the remote onboarding for banks’ customers, which is tailored to each partnering bank. The respective process comprises of digitizing the three steps: identification, verification and authentication[35].

On a related development, the Tunisian Financial Intelligence Unit (Tunisian Committee for Financial Analysis), launched in January 2021 a Regtech solution “Hannibal platform” to track the cross-border transport of foreign currencies[36].

Morocco made significant progress to cater for remote onboarding, where Bank Al-Maghrib, in collaboration with the National Financial Intelligence Unit and the National Commission for Personal Data Protection (CNDP), issued a regulatory framework governing the online opening of bank and payment accounts in April 2020. This framework allows banks and payment institutions to open accounts remotely for individuals and companies in compliance with FATF recommendations, in particular recommendations n°10 and n°15 related to customer due diligence and new technologies respectively. It worth noting that the CNDP, the General Directorate of National Security (DGSN) and Bank Al-Maghrib have launched a project aiming to establish a national digital identity.

[32]/ QiCard. 2021. https://qi.iq/english/about-us

[33]/ Riley et al. 2020. Digital Financial Services in the MENA, Abt Associates Inc.

[34]/ Central Bank of Tunisia. 2021. FinxAr, Fintech Index for the Arab Region, Survey, March 2021. Government Decree No. 2020-312 of May 15, 2020. Government Decree-no. 2020-312.

[35]/ Chehade. Nadine. 2020. Fintechs Across the Arab World, CGAP, December 2020.

[36]/ Central Bank of Tunisia, 2021. FinxAr, Fintech Index for the Arab Region, Survey, March 2021. https://www.ctaf.gov.tn/data/uploads/pdf/6036f145745426.90813774.pdf

Selected Arab Countries' Case Studies

Bahrain National eKYC Platform[37]

Bahrain eKYC Platform is the first of its kind in the region to be implemented at a national level using state of art technologies of AWS Cloud Computing, Blockchain and advanced sets of APIs to serve the needs of eKYC in the market.

The eKYC platform was launched in April 2019 to address the gaps and pain points of KYC across the financial sector, fulfill the regulatory requirement and facilitate digital onboarding. The financial institutions are now able through the eKYC platform to electronically authenticate the client, fetch up to date KYC data, screen against AML/ CFT lists and perform risk-based KYC for individuals and corporate clients at a feasible cost. Thus, it is an enabler for digital banks as well as other fintech companies and any other financial institution to offer their services digitally and serve their clients remotely. The integration capabilities make it convenient to integrate with core systems and electronic channels, enhance customer experience, reduce fraud, and streamline the full onboarding journey therefore acquiring new clients.

The eKYC service represents a successful collaboration between The BENEFIT Company, which operates systems for various other Fintech and electronic financial transactions' service in Bahrain (the eKYC operator), the Information and eGoverment Authority (the eKYC Biometric Identity Authenticator and Data Provider), under the supervision of the Central Bank of Bahrain (CBB) who is leading and regulating eKYC. It leverages the National infrastructure of citizens and resident's data repository with the Information and eGoverment Authority and extend it to the financial sector for the purpose of KYC upon customer consent, and allows sharing the KYC data among financial institutions through the Blockchain.

This eKYC service introduced in Bahrain prior to COVID19 pandemic was timely and helped the financial sector cope with some of the challenges posed by the pandemic.

Egypt Simplified eKYC Measures[38]

The Central Bank of Egypt (CBE) has been taking proactive steps towards digital transformation for the last couple of years and was keen to implement several key initiatives to promote usage of digital financial services (DFS) and to bolster the growth of digital transformation.

In July 2019, the CBE announced the opening of its Regulatory Sandbox first cohort with a theme e-KYC for digitally onboarding e-wallets' customers to facilitate the seamless provision of financial and banking services to citizens, and thus ensuring access of a wider segment of underserved population.

This led to the emergence of "Valify", a digital ID solution, which enables customers' digital onboarding in three steps consisting of information extraction, facial recognition and

[37]/ The Benefit Company, 2021. Bahrain eKYC Platform, presented to the Arab Monetary Fund, June 2021.

[38]/ Central Bank of Egypt. 2021. Egypt Simplified eKYC Measures, presented to the Arab Monetary Fund, June 2021.

authentication[39]. "Valify" is still under testing within the CBE sandbox.

Soon after, the Covid-19 outbreak highlighted the increased need for customers' digital onboarding and the CBE had a swift reaction to the repercussions of the crisis; aiming to facilitate conducting financial transactions digitally and thereby contributing to reducing the spread of the virus. Consequently, on March 15, 2020 the CBE issued an circular allowing banks to verify mobile wallet customers' identity by any electronic means that the bank deems appropriate (exceptionally for six months), including but not limited to, obtaining his/her national number and mobile phone number in an electronic way and verifying the customer's ownership of the mobile phone number used during the registration process via the National Telecommunication Regulatory Authority (NTRA) platform.

To maintain a balanced approach between achieving financial inclusion and providing the measures necessary for safe banking, new simplified Customer Due Diligence (CDD) procedures were issued including the following:

- Fewer required documents to verify a customer's identity (only an ID is needed to open an account).
- Less data to conduct domestic mobile transfers.
- Offer the possibility to update customer data and documents electronically.
- Permit certain categories of service providers to conduct CDD procedures according to a set of prerequisites, i.e. agent banking.

Additionally, in coordination with the Egyptian Money Laundering and Terrorist Financing Combating Unit (EMLCU), the CBE issued guidelines to all banks to apply new simplified procedures to open banking accounts for the self-employed and owners of micro-sized projects; aiming to progress towards higher financial inclusion rates and encouraging more citizens to open bank accounts.

Jordan Payments and Clearing Company (JoPACC) e-KYC/ CDD Project[40]

The Jordan Payments and Clearing Company (JoPACC) is currently designing a project to adopt a national e-KYC/ CDD platform aiming to enable all residents and citizens of Jordan to access financial services remotely and securely. This is in addition of employing a unified platform for individuals and businesses, facilitating the ability of financial institutions to digitally obtain KYC information required by the Central Bank of Jordan (CBJ), so that to ensure rightful, harmonized, and up-to-date data across financial institutions in Jordan, reducing the risk of financial crime, and improving Jordan's financial market soundness.

This will allow remote customer verification and authentication, creating a usable and trustable digital financial identity; while permitting the sharing of customer's profile with entitled participants, from the financial institutions, upon obtaining the customer's immutable and traceable consent.

[39]/ Chehade, Nadine. 2020. Fintechs Across the Arab World, CGAP, December 2020.
[40]/ JoPACC. 2021."JoPACC eKYC and eCDD Platform Overview", presented to the Arab Monetary Fund, June 2021.

The Platform will provide participants with the below services enabling the remote onboarding and access of their services to the clients.

1) Genuineness Check

Utilizing the camera of the client's mobile phone, the platform will verify the genuineness of the scanned document based on the applicable security marks along with the validity and relevance of the Machine Readable Zones (MRZ) of the document.

2) Data Capturing and Validation

Data capturing will be performed to extract all data in the document and perform initial validation of the data against the data retrieved from data providers where applicable.

3) Liveness Check and Image Matching

i. Liveness Check

Using the selfie captured via customer's mobile phone camera, the platform will validate the liveness of the individual and detect any attempts of presentation attacks.

ii. Image and Document Matching

The selfie captured during the liveness check will be matched against the image captured from the scanned identification document and with the image residing at the Data Provider (such as CSPD), subject to the availability of images at the Data Provider.

4) Biometric Recognition

Facial image biometrics will be captured and will be securely stored to allow for the biometric-based authentication of individual customers who have successfully passed the onboarding process based on matching with a percentage score.

5) Customer(s) Consent(s) and Data Access

Prior to allowing participant's access to any KYC data, the platform will request and capture the immutable customer consent. Access to customers’ KYC data will be provided to participants based on the participant tier and consent.

Additionally, all KYC data updates will be published to participants who have access to the data.

6) KYC Data Sharing

The collected KYC data will be shared with the participant based on their tier as a signed form.

Policy recommendations and the way forward:

The G20 Digital ID on-boarding paper highlighted seven policy considerations. In brief they include (i) Ensure an integrated identity framework, (ii) Appropriateness of the regulatory Framework; (iii) Establish a reliable oversight model to include stakeholders beyond the traditionally regulated financial institutions; (iv) Build authentication and service delivery systems that protect user privacy; (v) Establish clear and well-publicized procedures for citizen redress; (vi) Support and empower development of private sector led services to leverage the legal ID infrastructure for building out digital layers; (vii) closely monitor emerging development and technologies.

Moreover, the "Digital Identity and e-KYC Guidelines for the Arab Region" imply set of policy actions within same directions in addition to the following: (i) Establish a 'risk-based' CDD regime which balances the AML/CFT objective and financial inclusion objectives; (ii) Prioritize integrity of user data and facilitate processes and procedures for minimalistic sharing of the information during CDD; (iii) Provide regulatory clarity, remove barriers and foster enabling regulatory environment for innovation which may provide newer solutions for CDD; (iv) Create benchmarks and standards for use of any 'non-government' backed identity systems; (v) Ensure complete, accurate and better integrated databases that can be utilized for customer identification and verification purposes. Furthermore, the guidelines propose formulating transnational frameworks for interoperability and levels of assurance being implemented across Arab countries[41].

The Financial Inclusion Global Initiative (FIGI) Digital Identity working group elaborated on five policy considerations that are specifically relevant to financial sector regulators looking to accelerate the use of digital ID for expanding access and uptake of financial services.
Each policy consideration includes several suggested implementing approaches and highlights relevant case studies. These approaches are intended to help countries assess and implement key policies necessary to access and use digital ID in the financial sector, with the understanding that these approaches will need to be adapted to fit the needs of each specific country-context.

[41]/ AMF. 2020. Digital Identity and e-KYC Guidelines for the Arab Region, March 2020. https://www.amf.org.ae/en/publications/digital-identity-and-e-kyc-guidelines-arab-countries

Table 3- Summary of Policy Considerations and Implementing Measures

Policy considerations	Implementing measures
1. The legal and regulatory framework supports the usage of Digital ID by FSPs	Foster dialogue between different agencies and actors
	Develop clear guidelines or regulations allowing the appropriate, risk-based use of digital ID systems
	Consider if a Simplified CDD (SCDD) would be appropriate based on a risk-based analysis
	Assess if the existing legal and regulatory framework cover the usage of Digital ID and e-verification of customers identity
	Harmonize CDD requirements
	Develop KYC requirements stem from an outcome perspective focusing on financial integrity
	Increase awareness of risk-based approach within a collaborative approach among stakeholders
	Adopt technical standards to the usage of Digital ID
	Support the usage of e-KYC solutions, to be technology-neutral, and consider being in line with the risk-based approach
	Guidelines on non-face to-face account opening
	Support usage of Suptech solutions to enhance AML/CFT supervision
	Guidelines on the role that e-signatures
	Mitigate exclusion risks for those that do not have a digital ID
2. Identify the full range of risks related to the usage of Digital ID by FSPs	Data Governance
	Privacy by design
	Conduct a Data Protection Impact Assessment
	Encourage data minimization, whereby FSPs only collect the minimal amount of data required for the intended purpose
	Mitigate fraud-related threats
	Establish guidelines on legal and technical requirements for cyber-resilience and cyber incidents.
	Establish protocols for incident responses when there is a data breach

3. Adopt consent mechanisms for customers	Build easy-to-understand consent mechanisms
	Data Controllers to be able to proof the capture of consent and expiry of consent
	Handle disputes for errors in consent management
4. Support Collaboration with the private sector	Establish a platform (such as a working group) for collaboration and dialogue
	Consider the supportive role that MNOs can play in ID enrollment and verification.
	Ability for private sector to build on top of, or supplement foundational infrastructure and resources
	Encourage the use of collaborative platforms and APIs to support identity management including interoperability, efficient data exchange, and data portability
	Develop robust procurement guidelines and support open design standards
	View emerging technologies and applications as an opportunity but recognize its potential risks to regulatory objectives
	Consider the use of regulatory "sandboxes", as an approach to better understand the risks and benefits of new approaches and identify approaches to responsibly harness them.
5. Oversight Framework for the Digital ID	Establish clear institutional mandates
	Transparent, proportionate and equitable framework
	Establish an independent oversight body

References

AFI. 2019. KYC Innovations, Financial Inclusion and integrity in selected AFI member countries, AFI Special Report, March 2019.

AMF. 2020. Digital Customer On-Boarding, e-KYC and Digital signatures in the Arab Region. February 2020. https://www.amf.org.ae/en/publications/digital-identity-and-e-kyc-guidelines-arab-countries

AMF. 2021. The Arab Region Fintech Guide, the CBUAE contribution to the guide survey, June 2021. https://www.amf.org.ae/en/publication/arab-regional-fintech-working-group

AMF.2021. Strategies for adopting DLT/ Blockchain Technologies in Arab Countries, August 2021. https://www.amf.org.ae/en/publication/strategies-adopting-dltblockchain-technologies-arab-countries

AMF. 2021. Responses to the survey for Fintech Index for the Arab Region "FinxAr", 2021

Central Bank of Egypt. 2021. Egypt Simplified eKYC Measures, presented to the Arab Monetary Fund, June 2021.

Central Bank of Tunisia. 2021. FinxAr, Fintech Index for the Arab Region, Survey, March 2021. Government Decree No. 2020-312 of May 15, 2020. Government Decree-no. 2020-312.

Central Bank of Tunisia, 2021. FinxAr, Fintech Index for the Arab Region, Survey, March 2021. https://www.ctaf.gov.tn/data/uploads/pdf/6036f145745426.90813774.pdf

Chehade et al. 2017. Financial Inclusion Measurement in the Arab World, Working Paper, CGAP and the Arab Monetary Fund's Financial Inclusion Task Force.

Chehade. Nadine. 2020. Fintechs Across the Arab World, CGAP, December 2020.

Digital financial services cover financial products and services, including payments, transfers, savings, credit, insurance and securities delivered via digital/electronic technology such as e-money (initiated either online or on a mobile phone), payment initiation services, payment cards, online lending and regular bank accounts.

FATF. 2020. Guidance on Digital ID, March 2020. https://www.fatf-gafi.org/publications/fatfrecommendations/documents/digital-identity-guidance.html.

FATF. 2021. Opportunities and Challenges of new technologies for AML/CFT, July 2021. https://www.fatf-gafi.org/media/fatf/documents/reports/Opportunities-Challenges-of-New-Technologies-for-AML-CFT.pdf

AMF.2019. Annual Report of the Financial Inclusion for the Arab Region Initiative (FIARI), 2019.

AMF.2020. Annual Report of the Financial Inclusion for the Arab Region Initiative (FIARI), 2020.

AMF. 2021. Survey on "Discussing Policies Priorities in Microfinance"- FIARI, May 2021.

GSMA. 2020. The Mobile Economy Middle East & North Africa 2020. https://www.gsma.com/mobileeconomy/wp-content/uploads/2020/11/GSMA_MobileEconomy2020_MENA.pdf

G20. 2018. G20 Digital Identity Onboarding, WBG, 2018. https://www.gpfi.org/sites/gpfi/files/documents/G20_Digital_Identity_Onboarding.pdf

JoPACC. 2021."JoPACC eKYC and eCDD Platform Overview", presented to the Arab Monetary Fund, June 2021.

Khaled, M. 2020. "Microfinance Roundtable: Call to action for Arab Stakeholders", IFC presentation, 20 May 2021.

KUNA. 2020. Kuwait News Agency, 2 December 2020.
https://www.kuna.net.kw/ArticleDetails.aspx?id=2942695&language=en

MAS. 2020. Monetary Authority of Singapore, Singpass, 2020. https://www.singpass.gov.sg.

McKinsey. 2019. Digital identification: A key to inclusive growth, April 2019.
https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/digital-identification-a-key-to-inclusive-growth.

PACI. 2020. The Kuwaiti Public Authority for Civil Information, Mobile Based Civil ID.
https://hawyti.paci.gov.kw/English

Pazarbasioglu, Ceyla et al. 2020. Digital Financial Services, WBG, April 2020.
https://pubdocs.worldbank.org/en/230281588169110691/Digital-Financial-Services.pdf

QiCard. 2021. https://qi.iq/english/about-us

Riley et al. 2020. Digital Financial Services in the MENA, Abt Associates Inc.

The Benefit Company, 2021. Bahrain eKYC Platform, presented to the Arab Monetary Fund, June 2021.

http://www.amf.org.ae

صندوق النقد العربي
صندوق النقـد الـعربـي
ARAB MONETARY FUND

مجلس محافظي المصارف المركزية ومؤسسات النقد العربية
Council of Arab Central Banks and
Monetary Authorities Governors