

Digital Customer On-Boarding, e-KYC and Digital signatures

- A study

Arab Monetary Fund - Regional Fintech Working Group

Technical workgroup publication



© 2019 Arab Monetary Fund
Arab Monetary AMF Building, Corniche Street, PO Box 2828, Abu Dhabi, UAE
Internet: <https://www.amf.org.ae>
All rights reserved.

This report is a product of the AMF Regional Fintech Technical Working group.

We encourage use for educational and non-commercial purposes. Dissemination of the contents of this report is encouraged for all end purposes. An attribution will be appreciated.

The findings, interpretations, and conclusions expressed in this volume do not necessarily reflect the views of the Directors or Executive Directors of the respective institutions of the AMF or the governments they represent and the AMF does not guarantee the accuracy of the data included in this work.

All product names, logos, brands, trademarks and registered trademarks referred in this document are property of their respective owners. All company, product and service names used are for identification purposes only. Use of these names, trademarks and brands does not imply endorsement.

All queries should be addressed to Arab Monetary Fund, Arab Monetary AMF Building, Corniche Street, PO Box 2828, Abu Dhabi, UAE 971 (2) 6171600; e-mail: nouran.youssef@amf.org.ae

Table of Contents

- 1. Acknowledgement 4
- 2. Executive Summary 5
- 3. Key definitions 9
- 4. Digital Identification 13
- 5. Customer Digital onboarding including KYC 19
 - 5.1 Practices across Arab countries – a broad flavour 25
 - 5.2 Customer Digital Onboarding - Practices across the World..... 30
- 6. Digital Signatures 33
 - 6.1 Use cases of Digital signatures - across Arab countries 37
 - 6.2 Use cases of Digital signatures - Global..... 43
- 7. Challenges facing e-kyc and digital on-boarding 45
- 8. Vendor landscape 49
- 9. Arab countries - Survey results 53
- 10. Concluding remarks 63
- 11. References 66

Table of Figures

- Figure 1 Impact of a Digital economy* 6
- Figure 2 Definition of Digital (From an application perspective)* 11
- Figure 3 Digital ID Interaction with Institutions* 16
- Figure 4 Digital ID Interactions* 16
- Figure 5 Digital ID system examples across the world* 17
- Figure 6 Customer Digital onboarding - Mobile (Schematic)* 23
- Figure 7 Customer Digital onboarding - Mobile using National Digital ID (Schematic)* 24
- Figure 8 Digital Signatures - How it works* 35
- Figure 9 Digitisation Index - Middle East countries* 53
- Figure 10 Digital potential by country %* 54
- Figure 11 Digitisation - Consumers are leading the charge - Middle east* 55
- Figure 12 Middle East Digitisation strategies - a few examples* 56
- Figure 13 Opportunities for enabling a Digital revolution* 64

1. ACKNOWLEDGEMENT

This study was delivered by the Arab Monetary Forum (AMF) Technical working group as part of the Regional Fintech Working group. This group consists of banking technologists, central bank regulators across the Arab countries and consulting firms.

This core AMF technical work group deliverable was led and lead authored by Saleem Ahmed – the UAE banking federation representative on the AMF Fintech working group with inputs from group co-members – Akshata Namjoshi of KARM Legal consultants, EY Research (Aatish Sankaran), Ghada Al Kharusi from the Central bank of Oman and Dorra Marrakchi from the Central bank of Tunisia. This document has also been peer reviewed by a wider team in the AMF coordinated by Nouran Yousef of the AMF.

All product names, logos, brands, trademarks and registered trademarks referred in this document are property of their respective owners. All company, product and service names used are for identification purposes only. Use of these names, trademarks and brands does not imply endorsement.

The report was launched at the AMF regional Fintech meeting in Abu Dhabi in December 2019 and was presented to the Arab countries representatives – regulators and technology leaders from the public and private sectors in a keynote presentation.

The findings, interpretations, and conclusions expressed in the paper and case studies are entirely those of the authors, they do not necessarily reflect the views of the Directors or Executive Directors of the respective institutions of the Arab Monetary Forum or the governments they represent. The AMF does not guarantee the accuracy of the data included in this work.

2. EXECUTIVE SUMMARY

In the financial services industry, the level of service offered to customers coupled with a strong branding are key to attract and retain their customers. Customers have come to expect from their financial institutions a high level of personalized service and personalized communications as they enjoy in other parts of their lives. Central bank regulations and regulations like PSD2 fosters competition between institutions. All these factors make customer loyalty a thing of the past and highlight the importance of the customer onboarding process.

Onboarding represents the first customer interaction for the financial institution and will set the tone for the entire relationship. A move from a lengthy and cumbersome paper-based process to a smooth, Omni-channel digital customer experience would be a true game changer (not to mention significant savings in process cost).

Customer onboarding encompasses the entire end-to-end process, from the time the customer is looking for information on a financial institution to the time his or her product (eg: bank account) is activated, as well as the follow-up activities performed by the financial institution to ensure a smooth start of the customer relationship (eg: first contact with a customer). Hence, this report covers both customer digital onboarding (bank account) and also the companion technology – digital signatures – as these two play a major role in ensuring the successful end-to-end customer onboarding is completed.

Every customer's onboarding journey is different but the experience of opening accounts with traditional financial institutions leads to many common friction points like being routed to different channels, the need to provide physical identification and long delays to access the account. Improving the customer onboarding experience should indeed be a priority for financial institutions. The account setup should be a formality and be completed in minutes, similar to other common services like Facebook.

Three characteristics of an identification system that matter most for financial services are a legal basis, uniqueness and the ability to exist in a digital format. Digital IDs are important to broaden public policy, especially for financial inclusion.

However, more fundamentally, the ability to prove one’s identity underlies the ability to access basic services and entitlements from healthcare through to pensions and agriculture subsidies to bank accounts. This is especially true for marginalized segments of society such as women, poor rural farmers, refugees and also extends to MSMEs (micro, small and medium enterprises). The importance of legal identity has been acknowledged by the international community through agreement of target 16.9 of the Sustainable Development Goals, which calls for all UN member States to “provide legal identity for all, including birth registration” by 2030.

The introduction of a regulated digital ID could potentially increase the adoption of financial services, furthering the financial inclusion agenda and supporting development goals. Digital ID lowers barriers by: a) making it easier for the unbanked to open a transaction account in conjunction with simplifying documentation requirements, b) enabling more cost-effective customer onboarding that can be conducted remotely and c) contributing to financial sector embedding by supporting the delivery of additional services to the individual.

This report first provides a context for digital ID and its various use cases across the spectrum of citizen interaction and then focuses on the customer digital on-boarding process adopted by financial institutions across the Arab countries, the emergence of digital signatures to bring in more system driven efficiencies into the system, the best practices across the globe in the arena of customer digital onboarding with relevant use cases highlighted, the various regulatory postures across the arab countries with respect to customer digital on-boarding and finally the challenges and key factors which impede wide spread adoption of these digital technologies. A

A digitised economy enjoys myriad economic and social benefits



Figure 1 Impact of a Digital economy

vendor landscape view is also presented for aiding readers to evaluate technology providers in this domain. There is indeed a great body of work done by the World bank group and the Global partnership for Financial Inclusion (GPII) in relation to the digital ID systems to increase efficiency, enhance effectiveness and enable new ways of conducting existing business processes in the financial sector apart from aiming to promote wider financial inclusion especially of marginalized segments of society such as women, poor rural farmers, refugees and also extends to MSMEs (micro, small and medium enterprises). This report complements this work by leveraging usage of Digital ID's in specific use cases of Customer digital on-boarding and digital signatures.



3. KEY DEFINITIONS

Authentication: The process of proving that a person is who they claim to be. Digital authentication generally involves a person electronically presenting one or more “factors” or “authenticators” to “assert” their identity—that is, to prove that they are the same person to whom the identity or credential was originally issued. These factors can include something a person is (e.g., their fingerprints), knows (e.g., a password or PIN), has (e.g., an ID card, token, or mobile SIM card), or does (e.g., their handwriting, keystrokes, or gestures).

Biometrics: Physical or behavioral attributes of an individual, including fingerprints, irises, facial images, gait, signatures, keystrokes, etc.

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. One-to-one (1:1) matching is a comparison against a single template (e.g., one stored on an eID card) and is typically used for authentication and verification.

Credential: A document, object, or data structure that vouches for the identity of a person through some method of trust and authentication. Common types of identity credentials include—but are not limited to—ID cards, certificates, numbers, passwords, or SIM cards. A biometric identifier can also be used as a credential once it has been registered with the identity provider.

Customer Due Diligence: FATF Recommendation 10 on CDD is based on four pillars, requiring: 1) identification and verification of customers, 2) identification and verification of beneficial owners, 3) understanding the nature and purpose of transactions, 4) monitoring the clients and their transactions on an ongoing basis.

Customer On-Boarding: The process of a financial services provider establishing a business relationship with a customer.

De-duplication: In the context of identification systems, it is a technique to identify duplicate copies of identity data. Biometric data—including fingerprints and iris scans—are commonly used to de-duplicate identities in order to identify false or inconsistent identity claims and to establish uniqueness.

Digital identity: A set of electronically captured and stored attributes and/or credentials that uniquely identify a person.

Digital identification (ID) system: An identification system that uses digital technology throughout the identity lifecycle, including for data capture, validation, storage, and transfer; credential management; and identity verification and authentication

Foundational identification system: An identification system primarily created to provide general identification and credentials to the population for public administration and a wide variety of public and private sector transactions, services, and derivative credentials. Common types of foundational ID systems include civil registries, national IDs, universal resident ID systems, and population registers.

Functional identification system: An identification system created to manage the identity lifecycle for a particular service or transaction, such as voting, tax administration, social programs and transfers, financial services, and more. Functional identity credentials— such as voter IDs, health and insurance records, tax ID numbers, ration cards, driver’s licenses, etc.—may be commonly accepted as proof of identity for broader purposes outside of their original intent, particularly when there is no foundational ID system.

Identification: The process of establishing, determining, or recognizing a person’s identity.

Identification (ID) system: The databases, processes, technology, credentials, and legal frameworks associated with the capture, management, and use of personal identity data for a general or specific purpose.

Identity: A set of attributes that uniquely identify a person.

Identity lifecycle: The process of registering, issuing, using and managing personal identities, including enrollment of identity data; validation through identity proofing and deduplication; issuing credentials; verification and authentication for transactions; and updating and/or revoking identities and credentials.

Identifiers: Unique data used to represent a person’s identity and associated attributes. A name or a card number are examples of identifiers.

KYC Registry: A KYC Registry refers to a centralized repository of CDD records of customers in the financial sector. It allows inter-usability of the CDD records across the sector with the objective to reduce the burden of producing CDD documents and getting those verified each time the customer creates a new relationship with a financial entity.

Legal identification (ID) system: Identification systems that register and identify individuals to provide government-recognized credentials (e.g., identifying numbers, cards, digital certificates, etc.) that can be used as proof of identity

Unique ID number (UIN): In the context of identification systems, a number that uniquely identifies a person—i.e., each person only has one UIN and no two people share the same UIN—for their lifetime. UINs are typically assigned after validating a person’s identity and statistical uniqueness through a process such as biometric deduplication. User: Individual or (system) process authorized to access an information system.

Verification: The process of confirming or denying that a claimed identity is correct by comparing the credentials (something you know, something you have, something you are) of a person requesting access with those previously proven and stored and associated with the identity being claimed

Definition of digital from an application perspective

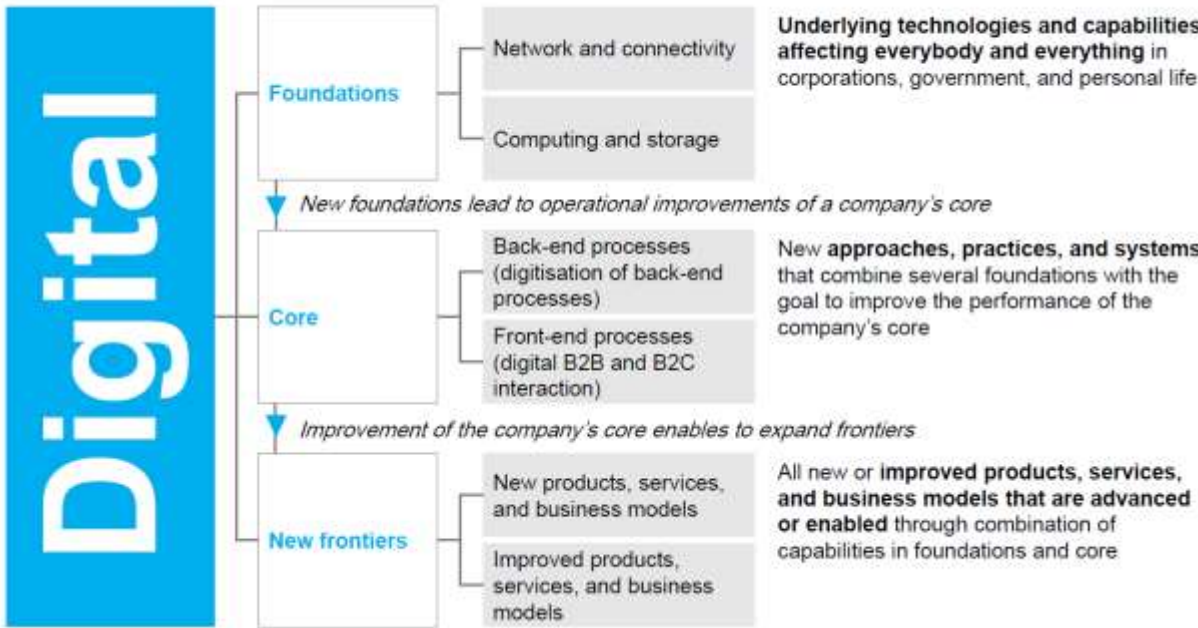


Figure 2 Definition of Digital (From an application perspective)



DIGITAL IDENTIFICATION



4. DIGITAL IDENTIFICATION

Before we commence analysis of the use cases of Customer digital on-boarding and digital signatures it is important to provide context on Digital ID's which are a pre-requisite element in any digital customer onboarding journey.

DIGITAL ID CAN UNLOCK VALUE BY PROMOTING INCLUSION, FORMALIZATION, AND DIGITIZATION

In an era of rapid technological change, digital identification provides a significant opportunity for value creation for individuals and institutions. Nearly one billion people globally lack a legally recognized form of identification, according to the World Bank ID4D database. The remaining 6.6 billion people have some form of identification, but over half cannot use it effectively in today's digital ecosystems. Individuals can use digital identification, or "digital ID," to be verified unambiguously through a digital channel, unlocking access to banking, government benefits, education, and many other critical services. Programs employing this relatively new technology have had mixed success to date—many have failed to attain even modest levels of usage, while a few have achieved large-scale implementation. Yet well-designed digital ID not only enables civic and social empowerment, but also makes possible real and inclusive economic gains—a less well understood aspect of the technology.

Digital ID is a foundational set of enabling technologies that can be pivotal in a wide range of digital interactions between individuals and institutions. Digital ID enables individuals to unlock value and benefit as they interact with firms, governments, and other individuals in six roles: as consumers, workers, microenterprises, taxpayers and beneficiaries, civically engaged individuals, and owners. Individuals benefit most as consumers from wider access to services, and as taxpayers and beneficiaries from time saved interacting with government. For example, digital ID could contribute to providing access to financial services for the 1.7 billion-plus individuals who are currently financially excluded, according to the World Bank ID4D Findex survey, and could help save about 110 billion hours through streamlined e-government services, including social protection and direct benefit transfers.

For institutions, gains could come from higher productivity, cost savings, and fraud reduction; for example, improving customer registration could reduce onboarding costs by up to 90 percent, and reducing payroll fraud could save up to \$1.6 trillion globally.

Unlike a paper-based ID such as most driver's licenses and passports, a digital ID can be verified remotely over digital channels, often at a lower cost and has the following attributes:

- Verified to a high degree of assurance. High-assurance digital ID meets both government and private-sector institutions' standards for initial registration and subsequent acceptance for a multitude of important civic and economic uses, such as gaining access to education, opening a bank account, and establishing credentials for a job. This attribute does not rely on any underlying technology. A range of credentials can be used to achieve unique high-assurance authentication and verification, including biometrics, passwords, QR codes, and smart devices with identity information embedded in them.
- Unique. With a unique digital ID, an individual has only one identity within a scheme, and every scheme identity corresponds to only one individual. This is not characteristic of most social media identities today, for example.
- Established with individual consent. Consent means that individuals knowingly register for and use the digital ID, with control over what personal data will be captured and how they will be used

Digital ID holds the promise of enabling economic value creation for each of these three groups by fostering increased inclusion, which provides greater access to goods and services; by increasing formalization, which helps reduce fraud, protects rights, and increases transparency; and by promoting digitization, which drives efficiencies and ease of use.

Digital ID benefits a wide range of individuals, from those who lack ID to those who have ID but cannot use it effectively in the digital world

Digital ID also unlocks new opportunity for the 3.4 billion individuals who have some form of high-assurance ID but limited access to the digital world.⁸ Moving from purely physical ID to digital ID programs, and creating digital infrastructure and applications that use digital ID for authentication, can enable these users to take advantage of the efficiency and inclusion benefits that digital interactions offer. Examples include more convenient services, such as e-government, and improved sharing of personal information, such as medical data. Digital ID can also provide the convenience of a multi-use form of identification, not a feature of many conventional national identity programs today. For example, as detailed in Exhibit 1, a 2016 study of 48 national identity programs found that very few could be used in a wide variety of sectors.⁹

Finally, good digital ID has the potential to benefit most of the 3.2 billion individuals who are already active in the digital world by facilitating greater user control of data, privacy protections, security for online interactions, and reduced friction in managing online accounts. In addition,

many of the 3.4 billion people who will become digitally active in the years to come stand to gain in the same ways. Individuals around the world have significant privacy-related concerns that high-assurance digital ID can address.

Forty or more national or non-national digital identity programs exist today - Roughly 1.2 billion people with digital IDs live in India alone, registered in the Aadhaar program, which began in 2009. Yet many digital ID programs have achieved low coverage levels, with the percentage of the population included as low as single digits, and most enable only a small fraction of the nearly 100 ways we have identified that digital ID can be used. As a result, most existing digital ID programs do not yet capture all potential value; additional opportunity exists for greater value creation.

Technology needed to expand digital ID exists and is growing ever more affordable

The opportunity for value creation through digital ID is growing as technology improves, implementation costs decline, and access to smartphones and the internet increases daily. The foundational digital infrastructure that supports digital ID grows in reach and drops in cost every day. More than four billion people currently have access to the internet, and nearly a quarter-billion new users came online. Africa is experiencing the fastest growth rates in internet usage, with a 20 percent increase each year. Meanwhile, the price of a smartphone, the primary entry point for access to the internet in many emerging markets is falling exponentially.

The technology needed for digital ID is now ready and more affordable than ever, making it possible for emerging economies to leapfrog paper-based approaches to identification. Biometric technology for registration and authentication is becoming more accurate and less expensive. For example, iris-based authentication technologies can give false acceptance rates as low as 0.2 percent and false rejection rates of 0.0001. The average selling price of a fingerprint sensor found in a mobile phone fell by 30 percent and falling. Bar codes on cards, which once stored only numerical data, can now secure signature, fingerprint, or facial data.

Digital ID has the potential to be used for good or for bad, and comes with risks even when intended for shared value creation

Digital ID, much like other technological innovations such as nuclear energy and even the ubiquitous GPS, can be used to create value or inflict harm. Without proper controls, digital ID system administrators with nefarious aims, whether they work for private-sector firms or governments, would gain access to and control over individual data. History provides ugly

examples of misuse of traditional identification programs, including to track or persecute ethnic or religious groups. Digital ID, if improperly designed, could be used in yet more targeted ways against the interests of individuals or groups by government or the private sector. Potential motivations could include financial profit from the collection and storage of personal data, political manipulation of an electorate, and social control of particular groups through surveillance and restriction of access to uses such as payments, travel, or social media. Thoughtful system design with built-in privacy provisions like data minimization and proportionality, well-controlled processes, and robust governance, together with established rule of law, are essential to guard against such risks.

Individuals and Institutions can benefit from Digital ID in a range of interactions

Digital ID can facilitate many types of interactions between two parties, most often individuals and institutions, producing benefits for both. Individuals can use identification to interact with businesses, governments, and other individuals in six roles: as consumers, workers, microenterprises, taxpayers and beneficiaries, civically engaged individuals, and asset owners (Exhibit 3). 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 residents; and as asset registers, interacting with individual asset owners. In this report we shall focus on the interaction of consumers with financial institutions for a) Streamlining registration and authentication b) e-KYC for financial service as highlighted in Figure below.

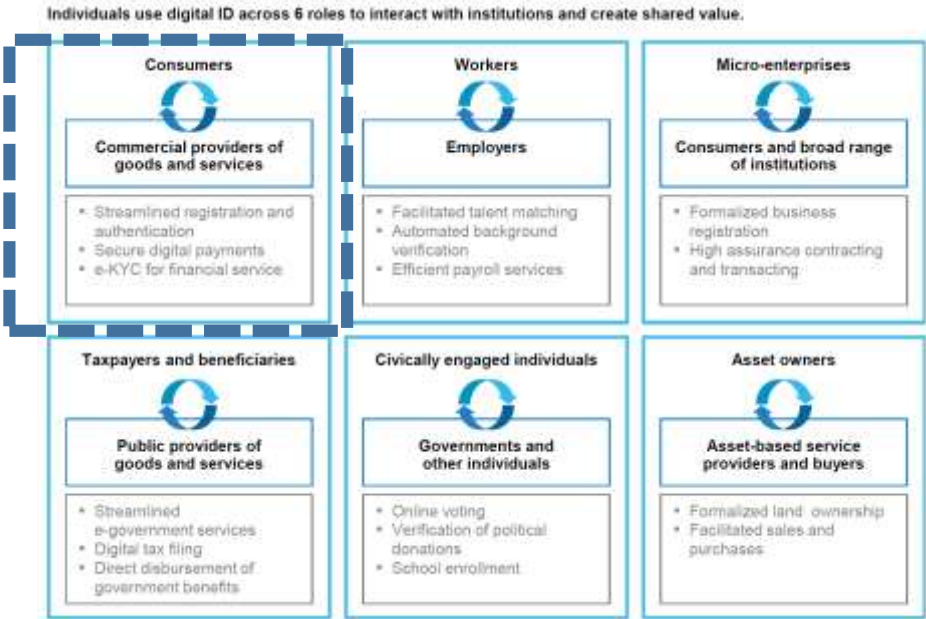
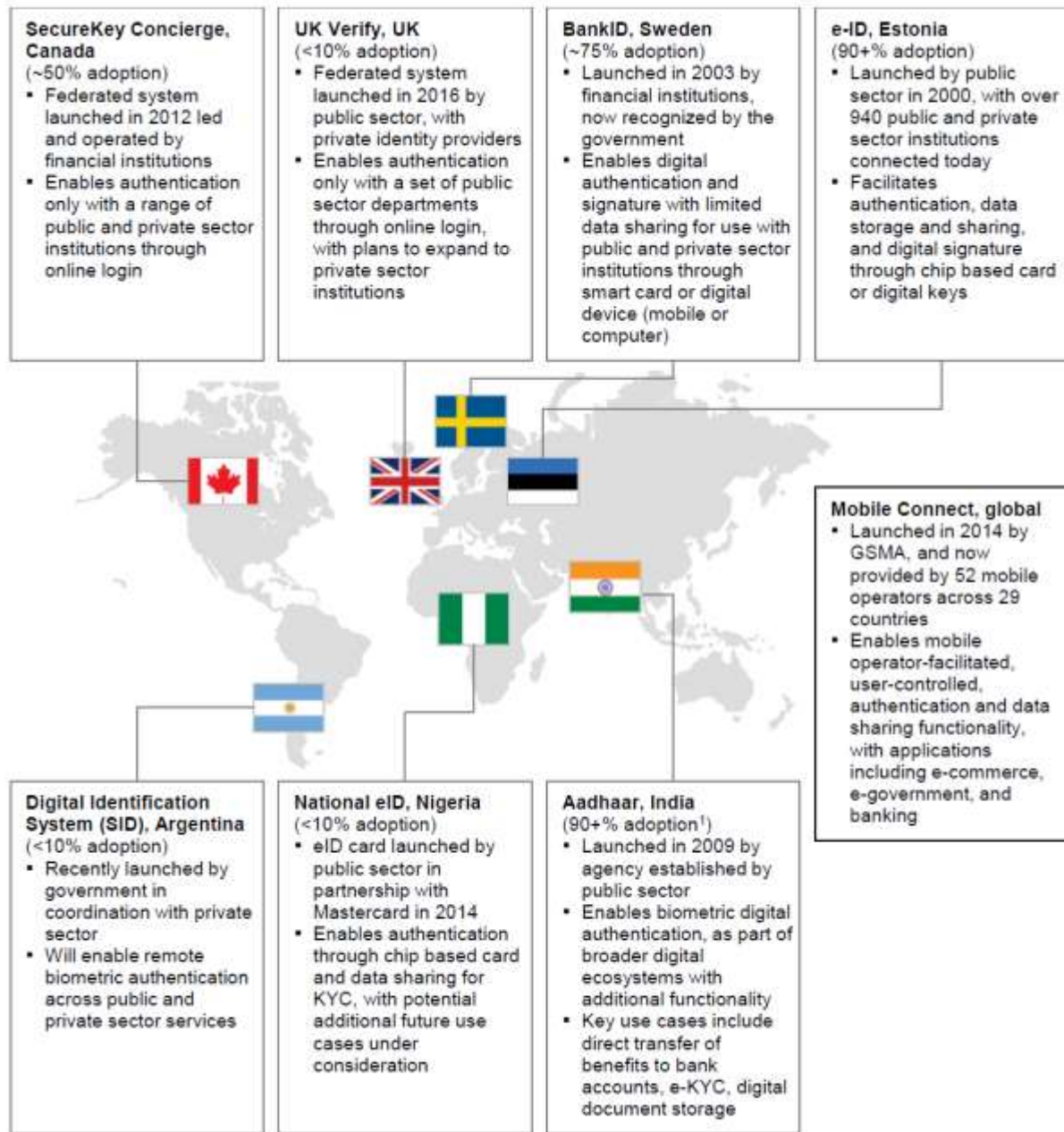


Figure 4 Digital ID Interactions

A variety of digital ID systems currently operate around the world.

Examples of digital ID systems can be found in Argentina, Canada, Estonia, India, Sweden, and the United Kingdom



¹ Adoption figures reflect data from the Unique Identification Authority of India (UIDAI) as of January 2019.

SOURCE: GSMA.com; BankID.com; Securekeyconcierge.com; Gov.uk; E-estonia.com; Argentina.gob.ar; Nimc.gov.ng; Uidai.gov (updated as of 1/2/2019); McKinsey Global Institute analysts

Figure 5 Digital ID system examples across the world

DIGITAL ONBOARDING



5. CUSTOMER DIGITAL ONBOARDING INCLUDING KYC

Customer onboarding including KYC procedures have been more stringent and need to be implemented in the first stage of any business relationship when enrolling a new customer. In response to the worldwide anti money laundering compliance requirements, set out by regulatory standards like FATF, KYC checks has been put in place to protect the financial sector against the misuse of financial products against money laundering and financing of terrorism.

The current processes of customer onboarding done by financial institutions involves collecting ID documentations such as national ID, or passport for residence and non-residence, and the verification is done against other independent data sources. Then compliance checks are made to ensure on going monitoring of the accounts to check the intended purpose of opening an account and if any suspicious activities or transactions are taking place. Verifying the sources of funds is essential prior to customer onboarding in many jurisdictions. Clients checks are made against regular watch lists or regulatory blacklists. This process of customer onboarding is done using a manual infrastructure to carry out KYC processes and may be unsustainable for monitoring AML, as noted in a recent report by FATF, “the information provided by third party service providers can be out of date or incomplete” (Jee, 2019).

For financial institutions to ensure that they know the clients well, they will need to perform customer due diligence during onboarding. This traditional onboarding process claims to be very time consuming for clients, customers expect the process to be faster and easier.

Digital on-boarding

Technological advancements provide solutions to better the customer onboarding process, by making the identification and verification more fast to match the fast pace of the digital world, it promises improved experience for its users and better efficiency in the financial sector.

Digital onboarding aims to ease the process of onboarding customers. For instance, instead of visiting an agent in person to open an account, customers may instead do so by phone or on a computer.

Digital Identification can be achieved through a set of electronic attributes, such as the use of biometrics. There are various options for biometric verification like fingerprints, Iris or even voice recognition or by having a multifactor authentication measures. The identification measures of clients happen remotely through electronic means (“DIGITAL KYC PROOF-OF-CONCEPT WHITE-PAPER”, 2019).



Specific case: Onboarding experience with N26

Number 26 ("N26") is a bank created in 2013 in Germany that allows customers to run their entire financial life from their smartphone. N26 processes the entire account opening in less than 10 minutes, and offers the possibility to withdraw cash from any ATM and receive real time push notifications after every transaction. Moreover, customers can send and receive money instantly to and from other N26 users. As of August 2017, the bank was available in 17 European countries, and claimed it had 500 000 customers, with 1500 new clients per day on average.

N26 announces a full online onboarding in less than 10 minutes, including ID verification and anti-impersonation performed via live video chat. Customers are guided through the process on a simple and clear interface:

- Fill in the online application form by entering personal details
- Provide personal legal data (e.g. tax country)
- Verify your identity and collect your ID document via a video chat with a video agent, available in multiple languages
- Receive an SMS with a unique code to pair your smartphone to your bank account

The fast success of this fully digital bank highlights that many customers are ready to change to new players when the experience of change is satisfying, and the level of services provided afterwards at least equal to that of traditional financial institutions.

The onboarding process represents the first interaction a customer has with a financial institution. This is a unique opportunity to create long-term loyalty. Moreover, it is the starting point enabling the digitization of other digital financial services such as online loans, insurance or investments.

Re-designing existing onboarding processes is a complex activity that involves many processes, providers and systems. The complexity increases due to customers' high expectations of top-notch user experience (UX) and their demand for omni-channel use. A customer-centric approach during the design phase should make it easier to achieve these goals. Today, numerous FinTech and non-FinTech providers are able to assist with both end-to-end and standalone solutions. Even if most of the underlying technology has a proven-track record, financial institutions still need to assess integration feasibility (i.e. considering specific internal constraints) and local legal requirements. Indeed, some of these requirements can be unclear and require special attention. For instance, photo/video identification and electronic signature requirements (e.g. advanced vs qualified according to eIDAS regulation), AML/CTF background checks and underlying customer due diligence duties need a specific focus.

Without compromising on AML/CFT requirements and with such technological solutions customer digital onboarding can be achieved, the onboarding process can be streamlined and hence the client experience will be more flexible. Clients will have to download an app, scan the national ID/passport, then take a selfie as a second mean of authentication and finally submits the request online without the need to be present at a branch. All is achieved in a non-face to face manner.

For instance, Paraguay now allows customers to register by taking a picture of their ID card and a picture of themselves and sending the two in together. Thailand introduced regulations in 2016 for remote customer onboarding, which have been interpreted to include registering via

video call. In Mexico, customers can open Level 1 and Level 2 accounts either via mobile phone



Digital Onboarding enables a new and personalized customer experience by simplifying the access to financial services while reducing processing time and cost for financial institutions due to optimized processes



or online, subject to additional ID verification and monitoring procedures by providers, which must be authorized by their supervisory authority with feedback from the Ministry of Finance. Finally, Malaysia's central bank, Bank Negara Malaysia, has laid the regulatory groundwork for e-KYC services for the money services business (MSB) industry, with a particular view toward streamlining the KYC process for users of online and mobile remittance services. The regulations permit the MSB industry to conduct remote onboarding of users through the use of video calls and 'selfies' (using facial recognition technology).

Customer experience is one of the most important success factors of the onboarding process. Financial institutions use more and more customer-centric methodologies to redesign the customer experience.

Customers need to see the onboarding process as a single process, no matter how many channels they use. To avoid losing customers during the process, the onboarding strategy must offer cutting-edge personalized experiences that accompany the customer during the onboarding process across multiple channels.

In the banking industry, 38 percent of customers stated user experience (UX) as the most important criterion when choosing a digital bank, and 26 percent stated the easy enrollment and login is the most important one.

To start implementing a new onboarding process, financial institutions need to consider their overall business architecture.

Customer onboarding encompasses the entire end-to-end process, from the time the customer is looking for information on a financial institution to the time his or her product (eg: bank

account) is activated, as well as the follow-up activities performed by the financial institution to ensure a smooth start of the customer relationship (eg: first contact with a customer). The goal is to ensure a valuable onboarding for the financial institution, not only by developing a new mobile app or website.

Some specific steps of the digital onboarding process require dedicated technologies.



In the banking industry, 38% of customers stated user experience (UX) as the most important criterion when choosing a digital bank

Deloitte, Inside Magazine Issue 16, Part 01 From a Digital perspective

Onboarding is a specific process that requires identifying customers and verifying their identity with high level of security and low level of risk, as required by KYC and AML regulations. Technologies like OCR, photo, facial and video recognition, automatic recognition of country identification documents (such as passports).

The role of electronic signatures is very important because of their key ability to complete the legal contractual engagement between the customer and the financial institution and seamlessly and paperless manner without the need for physical engagement between the two entities.

Financial institutions will need to integrate the required applications seamlessly to guarantee a great customer experience.

E-KYC is a process in which approved entities query a digital ID system to or verify their customers' identities. A growing number of developing countries are either implementing e-KYC or developing regulations and utilities to support its use.

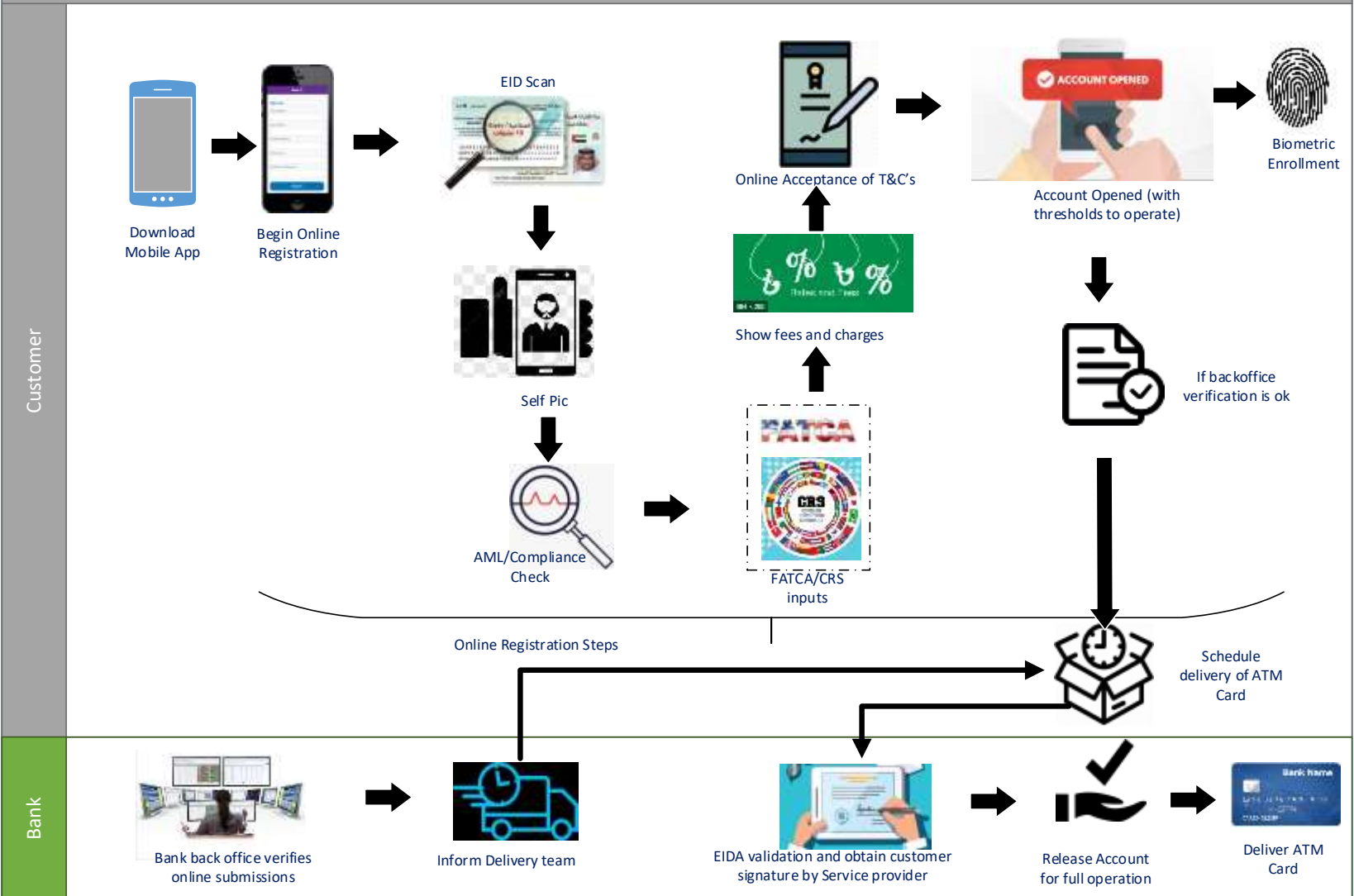
Digital onboarding and eKYC in the Arab countries:

For example, an e-KYC utility has been developed in Abu Dhabi, in order to provide a centralized location where customer identification and verification can be performed once, rather than several times by different entities for a same customer.

This solution based on blockchain technology with an immutable audit trail, seamless and secure information sharing, data privacy compliant, use of digital signatures, and with a customer consent model that has several benefits for all stakeholders.

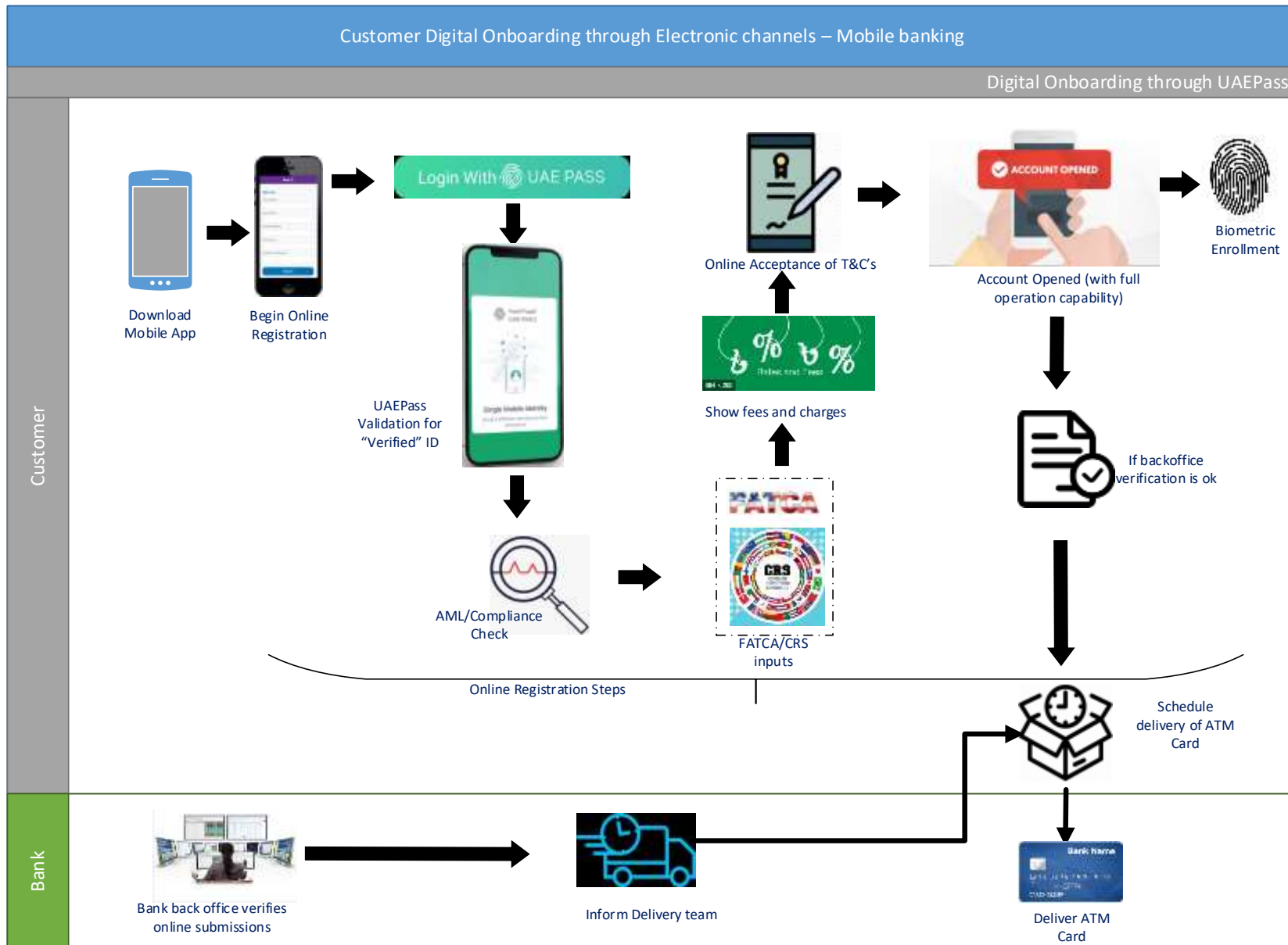
Customer Digital Onboarding through Electronic channels – Mobile banking

Standard Digital Onboarding



Customer digital onboarding in banks typically involve a verification of digital identity followed by banking specific customer due diligence measures. Mobile First strategy is adopted by many banks and neo-banks. The customer experience is very seamless and the customer is provisioned with an account number within minutes. Three banks in the UAE have such digital on-boarding mechanisms in place (Emirates NBD, Mashreq and ADCB) and AlAwwal bank in KSA have also introduced such innovation

Figure 6 Customer Digital onboarding - Mobile (Schematic)



Digital ID verification through pre-verified national digital identity programs - in the alongside figure, UAE's National identity program UAEPASS provides verification of digital identity using its mobile app. Citizens and residents are encouraged to enrol into the UAEPass program which allows for banks and others to on-board customers without the need for them to visit the branch.

Figure 7 Customer Digital onboarding - Mobile using National Digital ID (Schematic)

5.1 Practices across Arab countries – a broad flavour

The need for digital onboarding and e-KYC has been validated across the GCC countries by various regulatory authorities. However, the maintaining of a strong regulatory framework remains essential.

e-KYC and robust digital onboarding practices are a central topic of discussion and interest amongst GCC regulators. During the FinTech Abu Dhabi Summit 2018, a regional regulators roundtable was held that saw multiple regulators in attendance from the region including the FSRA, Central Bank of UAE, Securities and Commodities Authority of UAE, Dubai Financial Services Authority, Central Bank of Bahrain, Banking Control Commission of Lebanon, Capital Markets Authority of Kuwait, Capital Markets Authority of Saudi Arabia, and Saudi Arabian Monetary Authority, to discuss the necessary conditions for setting up an environment conducive to innovative technologies but still compliant with regulations.

In terms of digitally onboarding customer and eKYC central banks of Saudi Arabia, Oman, Qatar, Morocco, Libya, Lebanon, Egypt, Jordan, Yemen, Palestine, UAE, Sudan and Kuwait all have plans to implement eKYC. Most countries in the Arab region are working on creating a national eKYC platform by performing studies and updating regulations that will enable eKYC, but are still in their initial stages.

While Bahrain has a fully operational eKYC platform to digitally onboard its clients. They are working towards it by phases as follows:

- The eKYC is currently at its *initial stage* where all the Financial Institutions have access to the eKYC platform for retail customers. The platform has been launched and is live since April 30th 2019.

The eKYC 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.

The eKYC platform is connected with World Check One for screening against Anti Money Laundering, Politically Exposed Persons and Terrorist Financing.

The eKYC platform is on cloud-blockchain environment.

- *Phase 2* of the project is working in process to include APIs for seamless digital onboarding and integration with the financial institutions 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.

In the UAE, 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. With the launch of the UAE PASS, such process can be further enhanced when authenticating an individual.

The Payment institutions in Tunisia however, are currently the only institutions allowed by the regulation to use the e-KYC process for the identification of their clients who hold limited payment accounts by a threshold in terms of account balance and transactions and providing that the account opening procedures are based on secure technological process ensuring the verification of the authenticity of the ID documents and the confidentiality of client's personal data. The banks are not yet authorized to deal with this process. The Central Bank of Tunisia has implemented a regulatory sandbox to support Fintech in the development of new digital financial solutions including the e KYC process. Tunisia's e-government vision is also to provide a unique identifier for citizen and company.

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

Some key developments and examples are illustrated below.

fenergo:



Fenergo partners with BENEFIT to Create National eKYC Utility in E

Fenergo, a leading provider of digital Client Lifecycle Management (CLM) solutions for financial institutions, announced that it will be working with Bahrain's Electronic Network for Financial Transactions (BENEFIT) in designing and implementing the world's first national Know Your Customer (KYC) utility that incorporates blockchain technology. Blockchain-integrated utility will support more than 380 financial institutions to improve customer experience and drive KYC efficiencies across Bahrain.

The National Bank of Bahrain has joined the National eKYC (Know Your Customer) platform mandated by the Central Bank of Bahrain (CBB).

NBB was the first bank in the Kingdom to join the platform, which will be used by all financial institutions to simplify client onboarding and KYC maintenance requirements electronically.

The eKYC platform is a cloud-based/blockchain hybrid solution that provides financial institutions with the ability to retrieve and process client KYC and other data from the related bodies including Bahrain's Information & eGovernment Authority (IGA) and will also include international screening without the need for a physical presence, document verification or authentication. NBB has been successfully transacting on the platform since it went live on 30 April 2019.



1st Industry e-KYC Utility Project with UAE Financial Institutions concluded

ADGM has announced the conclusion of the first phase of the industry Electronic-Know-Your-Customer (e-KYC) utility project.

The e-KYC project, launched in March 2018, was an FSRA-led collaboration with a consortium of the UAE's major financial institutions. The objective was to develop a proof-of-concept (PoC) to test operational and technological models of the e-KYC utility. In consultation with consortium members, the FSRA also developed a governance framework and business model on which the e-KYC utility can operate on an inclusive and sustainable basis.

Notable highlights and potential benefits observed from the project include:

- Consortium members can successfully share and validate simulated KYC documentations and data updates about the client on the prototype in a secure environment, supported by blockchain technology
- Data quality and compliance standards can be assured with respect to applicable KYC requirements. Clear guidelines and pre-requisites will have to be identified for any member that qualifies as a contributor of KYC records or information to the utility.
- Individual clients can be empowered to decide how their personal data can be shared in the utility, enabling conformance with data protection requirements. In addition, serve as an effective incentive for clients to keep their data accurate and updated.
- An ownership structure of the KYC utility that assures safe custody of customer information and operates on a non-profit mandate will foster trust across stakeholder group.



Mint reveals digital customer on-boarding solution

Mint Middle East, has developed a digital customer onboarding solution integrated with the Emirates Identity Authority.

The Emirates Identity Authority is the government agency, which manages the national biometric ID database in UAE for real-time and instant customer identification (eKYC).

By employing eKYC technology in the UAE market, Mint is aligning their strategy with the Government's push for financial transparency, thus ensuring compliance with regulatory requirements and reducing the possibility of fraud. Mint's technology offers a secure, scalable solution that enables real-time validation of biometrics and Emirates ID to identify the customers.

Moreover, the eKYC solution also provides a new revenue opportunity, as it offers the proprietary eKYC service to Mint's financial institution partners. Mint aims to drive adoption of the Mint mobile app, and facilitate its position as a provider of mobile-enabled financial services in partnership with licensed financial institutions.



Acuant, Codebase launch eKYC solution in GCC region

Acuant and Codebase Technologies Digibanc have joined forces to provide the Gulf Cooperation Council region with a digital identity and eKYC solution called Digibanc Identity.

The GCC region includes Saudi Arabia, Kuwait, the United Arab Emirates, Qatar, Bahrain, and Oman.





The goal of the partnership is to provide a strong customer focused solution to industries heavily focused on their customers and are looking to provide more engaged customer experience. With Digibanc Identity, organizations can lower their customer acquisition costs, operating expenditures, onboarding times, and physical location footfalls.

Digibanc Identity has already been deployed for a large-scale regional bank in the GCC providing them with regulatory compliance and increased customer satisfaction.

Digibanc Identity aims to establish itself as the benchmark technology for institutions for the verification and onboarding of their customer base on a global scale starting with the GCC and South Asian Regions.

5.2 Customer Digital Onboarding - Practices across the World

Following are examples of best practice in digital onboarding being adopted Globally including pure play digital banks

			
<p>Digital KYC App, 'KYZO' launched FRSLABS, a fintech startup has launched a digital KYC App- 'KYZO' which used OCR and computer vision technology to extract the ID details and pre-fill an identity form for later use by the Customer.</p> <p>The documents in KYZO stays in the customer's phone (encrypted) and never transferred or backed up to cloud, putting to rest the threat of mass hacking, leaks and privacy concerns. At the point of sharing KYC (say to open a Bank Account), the customer simply scans the unique QR generated by the Bank, consents to share the identity data and authenticate using a PIN. The data seamlessly transfers to the Banker's App. The data transfer is done offline such that no network connectivity is needed making it convenient to work even in place with limited network.</p>	<p>The fifth largest bank in Thailand deploys facial recognition</p> <p>Bank of Ayudhya, commonly referred to as Krungsri, has introduced biometric facial recognition technology for verifying the identities of people as they open a deposit account.</p> <p>This news follows a report last month which said that 10 participants testing facial recognition for eKYC checks in a Bank of Thailand test were ready to exit the regulatory sandbox. The use of facial recognition for eKYC requirements was approved by Thailand's cabinet in 2018 to promote financial inclusion.</p> <p>The biometric technology is now available for customers visiting Krungsri branches and facial recognition for eKYC will be deployed to open accounts on mobile devices by the end of the Q2 of 2019.</p>	<p>CBL adopts electronic KYC to distribute hard currency allowance</p> <p>The Tripoli-based Central Bank of Libya (CBL) has adopted an electronic Know Your Customer (e-KYC) system for this year's round of disbursing the annual hard currency allowance.</p> <p>Applicants for the allowance must ensure that their mobile phones are registered in their names and linked to their National ID Number.</p> <p>The adoption of an e-KYC system by the Tripoli CBL, a paperless Know Your Customer process, wherein the identity and address of the subscriber are verified electronically, is seen as an attempt to reduce corruption and provide a speedier and more efficient distribution system for the annual hard currency allowance.</p>	<p>Financial service provider bKash has launched electronic KYC app so that customers can open their account by themselves.</p> <p>The eKYC app would allow customers to open their bKash account with instant activation only scanning National ID and taking photo without any documents. Using Optical Character Recognition (OCR) to collect data from NID, face detection technology, and cross matching data with Election Commission (EC) database, the app is making the whole system more integrated and less operational complexity.</p> <p>As such, in this system, the respective fields of the eKYC form are filled up by an automated scanning process OCR to extract information from the NID. After that, a photo is taken directly by the mobile phone and all the information are cross matched with EC database. Proper verification follows then, so that the system will automatically register the customer account and send confirmation message to both the eKYC app user and the new customer.</p> <p>Currently agents of bKash care, bKash center, and distributors are the ones registering new customers using this interactive app, bKash plans to render this solution directly to the customers so that they can open accounts by themselves.</p>



BANK NEGARA MALAYSIA
CENTRAL BANK OF MALAYSIA



The rise of e-KYC

While the KYC process is typically done face-to-face or over the phone, some banks innovate by introducing electronic Know Your Customer (e-KYC), an electronic and paperless method of conducting the KYC process remotely, through a mobile application. For example, The **Bank of Negara Malaysia (BNM)** will introduce e-KYC as its latest innovation. Its solution will be applied to ease large remittances and is expected to be finalized in October.

Under this framework remittance provider are permitted to verify a customer's identity via video calls, selfies and social media on top of the databases maintained by the National Registration Department, telecommunication companies and sanctions lists issued by credible sources.

Another example is **Kakao bank**, a successful online bank in Korea with a customer centric approach. Kakao bank implemented an e-KYC solution so that customers can open an account in 7 minutes which is significantly less time than it would take at a traditional bank branch.



Tata Mutual Fund launches 'Video KYC'

Tata Mutual Fund has launched "video KYC" as a digital solution to continue paperless know your customer (KYC) verification. Video KYC requires an investor to update their details and upload identity proof i.e. PAN card, address proof, photograph, a cancelled cheque, and signatures on the AMC's website.

On uploading all documents, the investor is required to start real-time video recording using the front camera on his/her smartphone or computer and display a hard copy of all the documents for five seconds each. Investors have to say 'Hi' followed by the investor's name at the end of the video recording.



Overcoming the "Know Your Customer" hurdle with e-KYC

India's Aadhaar program has rightly captured the world attention for its innovativeness and rapid growth. Aadhaar assigns each registrant a unique 12-digit ID number linked to minimal personal information (name, gender, date of birth, and a digital photo) and biometric information (fingerprints and iris scans) that can be used for authentication.

Since the Unique Identification Authority of India (UIDAI) issued the first Aadhaar ID, more than 1.2 billion people (90% of the population in India) have enrolled in the program. Aadhaar-based e-KYC allows customers to electronically provide their demographic and personal information to financial providers, who can verify it in real time.

One Ministry of Finance official estimated that moving from paper-based KYC to e-KYC in India reduced the average cost of verifying customers from \$15 to \$0.50. But the use of Aadhaar for KYC has also raised privacy concerns which lead the UIDAI to decide to suspend financial service providers and from conducting e-KYC.

Then the lesson to learn for other countries who want to conduct e-KYC is the importance of establishing a legal framework for digital ID and its use by third parties.



DIGITAL SIGNATURES



6. DIGITAL SIGNATURES

Banking transactions are increasingly moving from face-to-face to digital platforms – ATMs, kiosks, smartphones, tablets, and online – and while this trend has significantly enhanced customer convenience and driven down salary expenses, it has introduced its own costs and risks.

Some banking transactions such as account openings, loans, mortgages, and investments haven't participated in the digital revolution because of customer signature requirements, which typically require physical documents be mailed, couriered, or faxed between the parties. Whether or not a physical handshake occurs, the customer must acknowledge acceptance of the terms of the transaction by signing the document. The introduction of electronic signatures (e-signatures) into these processes is proving to deliver significant and quantifiable results in terms of reduction in cost, speed of transaction completion, and enhanced customer satisfaction.

USA and The G20 countries have all enacted legislation that recognizes digital signatures as equivalent to hand-written ones. Usually these need to be produced according to specific requirements (such as the European Union Directive on Electronic Signature); however, any digital signature can be used to identify the confirming user, system or organization.

Additional countries that accept digital signing include Bermuda, Colombia, Ghana, Guatemala, Malaysia, Moldova, New Zealand, Peru, the Philippines, Switzerland, and Uruguay.

In the Middle east, the UAE is enacting legislation to make digital signatures legal across a wide variety of use cases and is powered by their UAEPass digital identity platform.

What is a digital signature?

“While systems vary from provider to provider, the general idea behind them is the same,” writes, you upload a document – Word or PDF, or even an image file – to an online service, then tag it with special annotations where signatures eventually need to go. The service sends this marked-up file to your specified recipients, who then ‘sign’ it with a few clicks, either with stock cursive fonts or with a scrawl they draw with a mouse (or finger using a tablet) on the fly. When finished, the signed file is sent back.

A digital signature is an electronic signature that can be used to authenticate the identity of the sender of a message (either encrypted or plain text) or the signer of a document, and to ensure that the original content of the message or document that has been sent is unchanged. Digital signatures are easily transportable, cannot be imitated by someone else, and can be automatically time-stamped. ESRA defines it as a signature method that uses a digital certificate process, with a private key to sign and encrypt the document and a public key to unencrypt and authenticate the signature. Digital signatures require that a trusted third party (usually a digital certificate provider, such as VeriSign, Entrust, or Thawte) verifies facts about the signer's identity and issues the digital certificate to that signer.

Some of the key banking processes that can leverage digital signature services include:

- Product offerings to customers;
- Account opening;
- Signature cards;
- Standing orders;
- Exemption orders;
- Loan documents;
- Investments;
- Mortgage origination and closing; and
- Operational support materials, such as appraisals, disclosures, and employment verification.

The terms “electronic signature” and “digital signature” are used interchangeably in the banking domain, but in each case refer to digital signature technology that adheres to cryptographic public key infrastructure (PKI) standards. Figure below depicts the three-step digital signature process

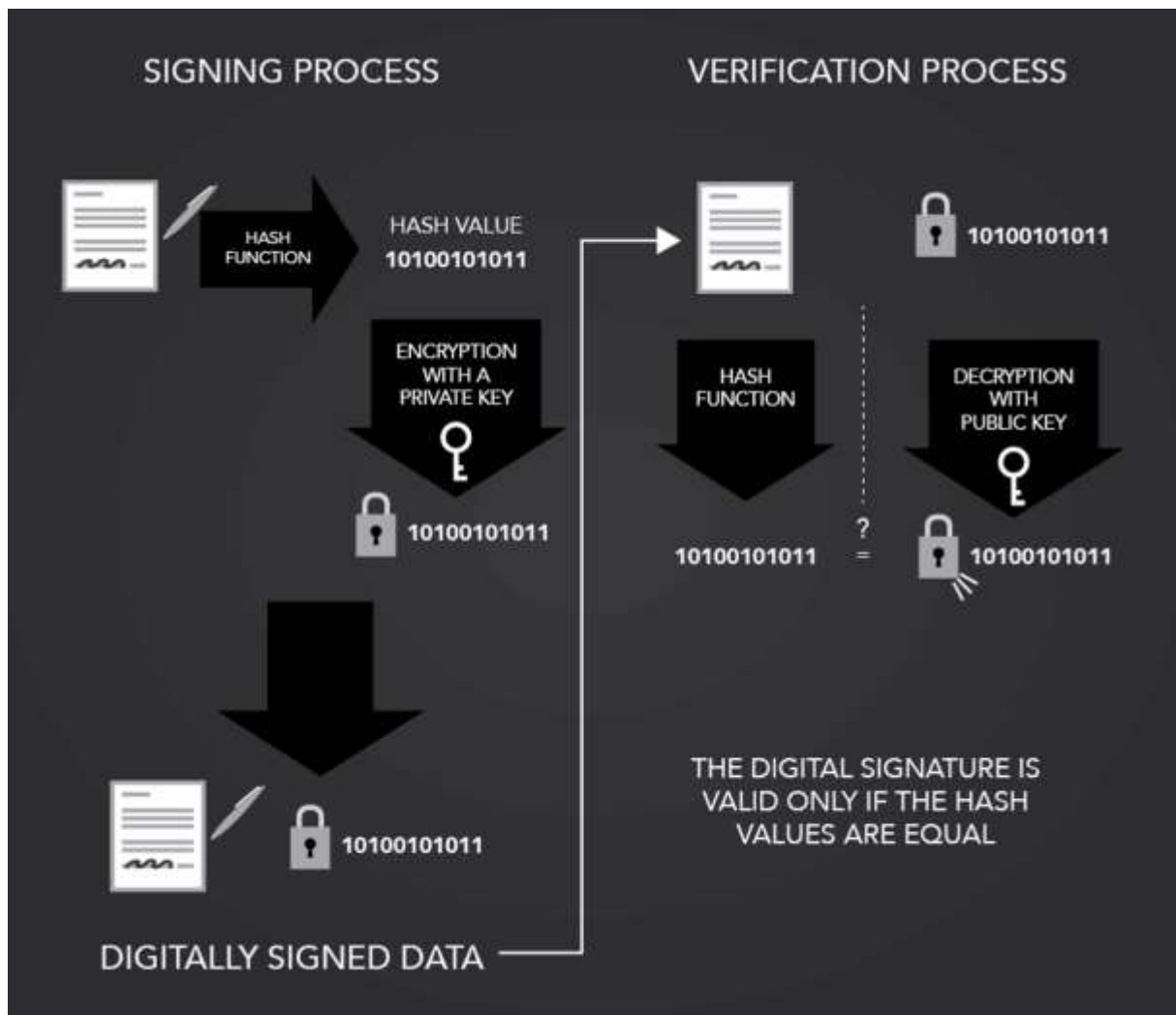


Figure 8 Digital Signatures - How it works

Incorporated into the digital signature process is a registration authority, which acts as the verifier for the certifying authority before a digital signature certificate is issued to a requestor. They process user requests, confirm their identities, and induct them into the user database. A certifying authority is a trusted third party willing to verify the identity of entities and their association with a given key, and issue certificates attesting to that identity.

E-signatures deliver:

Authentication. Digital signatures are used to authenticate the source of messages. The ownership of a digital signature key is bound to a specific user, so a valid signature shows that the message was sent by that user.

Integrity. In many scenarios, the sender and receiver of a message need assurance that the message has not been altered during transmission. Digital signatures provide this feature by using cryptographic message digest functions.

Non-repudiation. Digital signatures ensure that the sender who has signed the information cannot at a later time deny having signed it.

Key benefits of e-signatures

Cost reduction. A study by Ombud estimates e-signature solutions help enterprises save an average of \$20 per document, “reducing turnaround times by up to 80 percent and seeing ROIs over the next five years that can top \$50 million.” Study authors add that to achieve these savings, businesses must integrate e-signature technologies with other internal technologies and business processes.

Banks are taking advantage of e-signatures to reduce their operational costs. For example, HDFC Bank, Citibank, and ABN Amro Bank (cited in this *Economic Times* article) are using the technology in respect of statements of accounts for savings, current and credit cards, and electronic contract notes for equity brokerage transactions – cutting down on paper and time and improving the customer experience. The authors estimate the per-unit cost of sending paper account statements at around seven times that of digital signatures. Across millions of statements, this translates to immediate savings of 86 percent.

Royal Bank of Canada* indicates that about 8,000 wealth management and investment advisors use e-signatures to complete mutual fund, GIC, and other investment transactions. It further estimates it saves \$8 million annually by shaving 82,000 staff hours (equal to about 41 full-time employees) while reducing document errors by an astonishing 75 percent.

**Source: Doxim Fall Roadshow: Accelerating Customer Experience.*

Enhanced security. A paper document can be modified after being signed by an unauthorized person, but as counterfeiting e-signatures is virtually impossible, the integrity of the data is assured. Also, the probability of losing a digital copy is much lower compared to paper-based documents. All types of data, such as photos or audio files, can be digitally signed, which protects the copyright of these materials. A timestamp can be attached to the digital signature, ensuring that the document was signed at a specific date and time.

Faster service delivery. “Customers can receive the digitally signed documents electronically much faster – on their request or on execution of trade – compared to paper documents,” Munish Mittal, EVP and head of the technology solutions group at HDFC Bank told the *Economic Times*. “As long as the customer’s mail box is not full, delivery is guaranteed, which is a major advantage over paper mail/courier receipt tracking.”

User convenience. Customers are able to process signatures from any computer, tablet, or smartphone. No external devices (hardware token, e-identification card) are needed and there is no need to install any software.

Environmentally friendly. Paper savings alone will prove to be a significant advantage to the environment when banks substantially migrate from paper to digital documents.

The take-up of digital signatures services is still relatively small in banking. However, the opportunity for significant cost savings, inherent security, increased global legal acceptance, and the rapid acceptance of SaaS-based solutions incorporating mobile technology will fuel continued growth into the future.

6.1 Use cases of Digital signatures - across Arab countries

United Arab Emirates

Electronic Signature has been recognized by law in the United Arab Emirates since 2006, with the passage of the Electronic Commerce Law.

Court admissible: Yes; General Business use: Yes; E-Signature legal model: Open

eSignature Legality Summary

Under UAE law, a written signature is not necessarily required for a valid contract – contracts are generally valid if legally competent parties reach an agreement, whether they agree verbally, electronically or in a physical paper document. To prove a valid contract, parties sometimes have to present evidence in court. Leading digital transaction management solutions can provide electronic records that are admissible in evidence, under UAE laws, to support the existence, authenticity and valid acceptance of a contract.

[1] An AES is an “advanced electronic signature”, a type of electronic signature that meets the following requirements: (a) it is uniquely linked to the signatory; (b) it is capable of identifying the signatory; (c) it is created using means that are under the signatory’s sole control; and (d) it is linked to other electronic data in such a way that any alteration to the said data can be detected.

[2] A QES is a specific digital signature implementation that has met the particular specifications of a government, including using a secure signature creation device, and been certified as ‘qualified’ by either that government or a party contracted by that government.

Use Cases for Standard Electronic Signature (SES)

Use cases where an SES is typically appropriate include:

- HR documents, such as supplemental employment contracts (i.e., not employment contracts filed with UAE authorities), non-disclosure agreements, employee invention agreements, privacy notices, benefits paperwork and other new employee onboarding processes
- commercial agreements between corporate entities, including non-disclosure agreements, purchase orders, order acknowledgements, invoices, other procurement documents, sales agreements, distribution agreements, service agreements
- consumer agreements, including new retail account opening documents, sales terms, services terms, software licenses, purchase orders, order confirmations, invoices, shipment documentation, user manuals, policies
- service agreements
- termination notices
- software license agreements
- certain intellectual property licenses and transfers such as trademark licenses and assignments

Use Cases for Other Types of Electronic Signature (e.g. Digital Signature, AES QES)

Use cases where an electronic signature other than SES may be required include:

UAE law does not distinguish between the types of contracts/transactions that can be effectuated by SES, AES and/or QES. Therefore, those transactions that can be effectuated by the use of SES can also be effectuated with AES or QES and vice versa.

Use Cases That Are Not Typically Appropriate for Electronic Signatures or Digital Transaction Management

Set out below are use cases that are specifically barred from digital or electronic processes or that include explicit requirements, such as handwritten (e.g. wet ink) signatures or formal notarial process that are not usually compatible with electronic signatures or digital transaction management.

- Notarization or handwritten - documents with formal notarization requirements
- Notarization - family law contracts (marriage, divorce, wills, etc.) (Electronic Commerce Law, Article 2)
- Notarization or handwritten - deeds of title to real property (Electronic Commerce Law, Article 2)
- Notarization or handwritten - negotiable instruments (Electronic Commerce Law, Article 2)
- Notarization or handwritten - transactions involving the sale, purchase, lease (for a term of more than 10 years) and other disposition of real property and the registration of other rights relating to real property (Electronic Commerce Law, Article 2)
- Notarization or handwritten - employment agreements which must be filed with the Ministry of Labor or a Free Zone Authority in the UAE
- Notarization or handwritten - securitization documents
- Notarization or handwritten - termination notices
- Notarization - corporate articles

- Notarization or handwritten - any other documents or transactions exempted by special provision of law

Local Technology Standards

As an open, technology-neutral country, the United Arab Emirates have not created specific technical requirements, procedures or practices to implement a QES (Qualified Electronic Signature, or an electronic signature issued by an accredited organization of 'Electronic Attestation Certificates' as defined by local law). Therefore, no practical application of QES exists locally, although the law can be interpreted to imply the existence of a QES.

KSA

Electronic Signature has been recognized by law in Saudi Arabia since 2007, with the passage of the Electronic Transactions Law. However, the Electronic Transactions Law is applicable only to certified electronic transactions, which are not yet available to private parties.

Court admissible: Yes; General Business use: No; E-Signature legal model: Tiered

eSignature Legality Summary

Under Saudi law, a written signature is not necessarily required for a valid contract - contracts are generally valid if legally competent parties reach an agreement, whether they agree verbally, electronically or in a physical paper document. Article 5 of the Electronic Transactions Law specifically confirms that contracts cannot be denied enforceability merely because they are concluded electronically. To prove a valid contract, parties sometimes have to present evidence in court. It may be difficult to prove verbal contracts or electronic contracts formed by email or simple click-through arrangements.

Use Cases for Standard Electronic Signature (SES)

Use cases where an SES is typically appropriate include:

Parties can use DocuSign to create valid contracts and documents of any kind provided they are not subject to a specific statutory form requirement. Such contracts if contested will be subject to the judge's vast discretionary power. Possible use cases include agreements that do not require notarization.

Use Cases That Are Not Typically Appropriate for Electronic Signatures or Digital Transaction Management

Use cases that are specifically barred from digital or electronic processes or that include explicit requirements, such as handwritten (e.g. wet ink) signatures or formal notarial process that are not usually compatible with electronic signatures or digital transaction management.

- Notarization – real property title deed transfer
- Notarization – granting a power of attorney
- Notarization – signing the Articles of Association of a company with limited liability and any amendments thereof



DMCC has implemented E-signature

DMCC is the first Free Zone in the UAE to offer electronic signatures. Keeping up with Dubai Smart Government initiative, DMCC is always keen to continuously introduce state-of-the-art technology and solutions with the aim of enabling DMCC members to execute signature requirements on a range of documents online, from any device in any location in a safe and secure way.

DMCC has partnered with DocuSign, the global standard for Digital Transaction Management with more than 100 million users in 188 countries around the world to facilitate the e-signature process in a secure and easy way.

Yes, e-signatures under UAE Law are as binding as physical signing and DMCC has partnered with DocuSign, the global standard for Digital Transaction Management. Generally speaking, e-signatures are recognized under the laws of most of the GCC countries provided they satisfy certain requirements. Although this is positive, the formal recognition of e-signatures as evidence of a binding contract has yet to be tested in the courts in the region.

It is important to ensure when using e-signatures in any jurisdiction that once an e-signature has been affixed to a document, the document is incapable of being amended and the e-signature cannot be removed. Only an e-signature solution which satisfies this requirement will provide a reliable audit trail in the event that the validity of the e-signature is challenged.



Turkey: QNB Finansbank rolls out digital signatures in branches

QNB Finansbank, a subsidiary of QNB Group and one of the top five privately owned banks in Turkey, has launched digital signatures for account opening and loans in the bank's branches.

Customers can use the digital signature in the branches on a small tablet application that is customer-facing and integrates wirelessly (4G/LTE) with the teller's desktop solution. Then, the data is uploaded automatically to the relevant systems, including the core platform.

Also, this smart screen is used to present real-time customized campaign offers. The solution was first piloted in a handful of branches to see the customer response. In late 2016, 1,200 Samsung Android tablets were bought – two for each branch. The roll out process is still in progress.

6.2 Use cases of Digital signatures - Global



Aadhaar eSign

Aadhaar eSign is an online electronic signature service in India to facilitate an Aadhaar holder to digitally sign a document. The signature service is facilitated by authenticating the Aadhaar holder via the Aadhaar-based e-KYC (electronic Know Your Customer) service.



American Bank Systems, IMM to provide digital lending platform for community banks

IMM, an eSignature provider for financial institutions, has partnered with American Bank Systems (ABS) to provide digital lending platform that leverages signing capabilities for community banks. The eSignature provider will integrate IMM eSign with ABS' CoPilot Loans, CoPilotDeposits Origination Software, BankManager Tracking and Imaging solutions enabling community banks to electronically process loan and account opening transactions from origination to closing to electronic filing, all in a digital environment. ABS also provides technology solutions that help assess, monitor and lower compliance risk of financial institutions. The integration of IMM eSign with ABS' CoPilot and BankManager automates the entire loan and account opening process. Additionally, customers can access and sign important documents electronically, at a time and place that is most convenient to their schedule.



Deutsche Bank introduces digital signatures for corporates

Deutsche Bank has announced the implementation of a digital signature feature to speed up account openings for its corporate clients. The bank says document and contract signing remains one of the most important and frequent processes between banks and its clients and until today involves a high degree of manual processing. Deutsche Bank's first corporate client to incorporate DocuSign as a solution was US-based Honeywell. Clients can use the signature to open accounts, sign documents and buy products from the bank. The solution is available to corporate and institutional clients in the US, the UK, Germany, Belgium and the Netherlands. Deutsche Bank clients in Asia-Pacific and Middle East will be able to use DocuSign in order to implement digital signature in 2019, according to bank officials.



Cryptomathic, SwissSign launch e-signature solution for European banks

Cryptomathic has announced the launch of its centralised e-signature solution for Qualified Electronic Signatures (QES), in partnership with SwissSign. Utilising the combined solution for QES, banks and other institutions operating in Switzerland and the EU can now deliver an end-to-end digital customer experience by introducing digital signatures that carry the same legally binding status as those that are hand-written. The solution is deployable across all common digital channels including web browsers and mobile applications. The central signing solution utilises an organisation's existing authentication infrastructure to deliver QES, allowing organisations to reduce costs, enhance agility, enable digitalisation and minimise liability risks.



CHALLENGES FACING CUSTOMER DIGITAL ONBOARDING



7. CHALLENGES FACING E-KYC AND DIGITAL ON-BOARDING

According to the 2017 Global Findex Survey, the lack of documentation was the primary barrier to access to financial services cited by 26 percent of unbanked individuals in low income countries. Beyond extending legal ID in order to address these gaps, the introduction of a legal, digital ID could potentially increase the adoption of financial services, furthering the financial inclusion agenda and supporting development goals.

Digital ID lowers barriers by: a) making it easier for the unbanked to open a transaction account in conjunction with simplifying documentation requirements, b) enabling more cost-effective customer onboarding that can be conducted remotely and c) contributing to financial sector embedding by supporting the delivery of additional services to the individual. Governments are adopting electronic means of cash transfer to streamline processes and prevent leakage. Digital IDs can substantially strengthen the efficiency and effectiveness of the state in providing critical services such as Government to Person (G2P) payments and supporting the provision of humanitarian aid. A legal digital ID for those forcibly displaced not only provides them with a sense of identity but also supports efficient benefit distribution reducing fraud and duplication while allowing them to participate in the real economy.

The fourth industrial revolution presented many opportunities for the financial sector such as eKYC solution for ease of availing financial services and although these solutions facilitate the process of on boarding banking client's regulators and financial institutions alike are facing several challenges which have been identified in the section below.

According to a survey by Thomson Reuters that was conducted on KYC challenges, the survey reveals that there are no global common standards for applying KYC regulations in corporations and that is a key challenge. The lack of consistency in KYC Requirements of banks make it difficult for corporations to on-board within a country or across countries. Standard setters like FATF, Wolfsburg and the Financial Stability Board have very general KYC requirements and this causes a lack of convergence amongst regulatory bodies. The survey also found that 12 per cent of companies said they had changed banks because of KYC issues. Survey respondents

were drawn from the UK, Germany, South Africa, the U.S., Australia, Hong Kong, Singapore and France (Thomson Reuters,2017).

Above all, regulatory bodies like FATF require financial institutions to perform a Risk Based approach on all their clients, products/services provided, delivery channels and across geographical location, that are vulnerable to money laundering and financing of terrorism risk and they consider non face-to-face transactions as high risk which requires FI to undergo Enhanced due diligence (EDD). To satisfy the EDD process, banks may require additional identification documents, the data and information availability of customers being on boarded may be scattered within different stakeholders and this may trigger connectivity constraints in terms of verification purposes.

A main challenge in terms of eKYC requirements is the verification of clients' permanent address, this remains the issue of mostly the unbanked clients who lack the basic identification requirements to avail financial services. Refugees in specific face more difficulties satisfying KYC requirements because they do not have formal ID card and proof of residence. It remains a challenge for regulators to proof that refugees have proper identity requirements. As stated in a report published by World Bank ID4D 2017 Global dataset, universally (17.7 per cent) of the world's population remain without access to official KYC ("Helix Institute of Digital Finance", 2019).

The requirement that all KYC documents must be kept up to date is an ongoing challenge to most corporations and clients. In terms of corporation, they are obliged to inform their banks of any changes in executive managers and shareholders in order for banks to proper do their risk assessments. The responsibility of continuously updating the requirements falls primarily on the client/corporation but it is also the responsibility of the bank to make the process easier (Thomson Reuters, 2016)

Digital ID systems may be prone to abuse by terrorist, criminals and other bad actors. The challenges that may occur is due to the method of which the proofing of verification is done

through, over the internet, hence the risk of hacking and failure tend to be high. Cyber-attacks can happen at any time if the system lacks proper safeguard mechanisms to address them.

The authentication process of CDD may also be misused. The vulnerabilities relating to authenticating of a customer identity may be abused without the knowledge of the client. Phishing attacks for example may trick the clients into sharing their passwords, government ID numbers and other credentials in an attempt to impersonate the ID of the person for fraudulent for criminal reasons/attempts. This raises the attention of data protection and the privacy challenges, countries that do not have proper data protection laws and proper risk mitigates in place could be at a very high risk of cyber security attacks.

While the use of biometrics as a second buffer of authentication may be thought of as a safe option. But there are many weaknesses that may arise during the authentication process. In terms of face recognition, facial factors may be unreliable due to similarities in face expressions, and or other factors such as change in hairstyle, makeup may end up with a false reporting of facial expressions. If there is a failure in capturing right biometric and authenticating it, this may cause financial exclusion if and when there is no switch to an alternative mechanism for authentication.

Since digital ID systems are present online, through a mobile phone and with the use of an internet connection, there may be challenges relating to the soundness of the connectivity. Such connectivity issues may disrupt the on boarding process of clients, especially if the use or model of the mobile phone does not capture the required basics for on boarding.



VENDOR LANDSCAPE



8. VENDOR LANDSCAPE

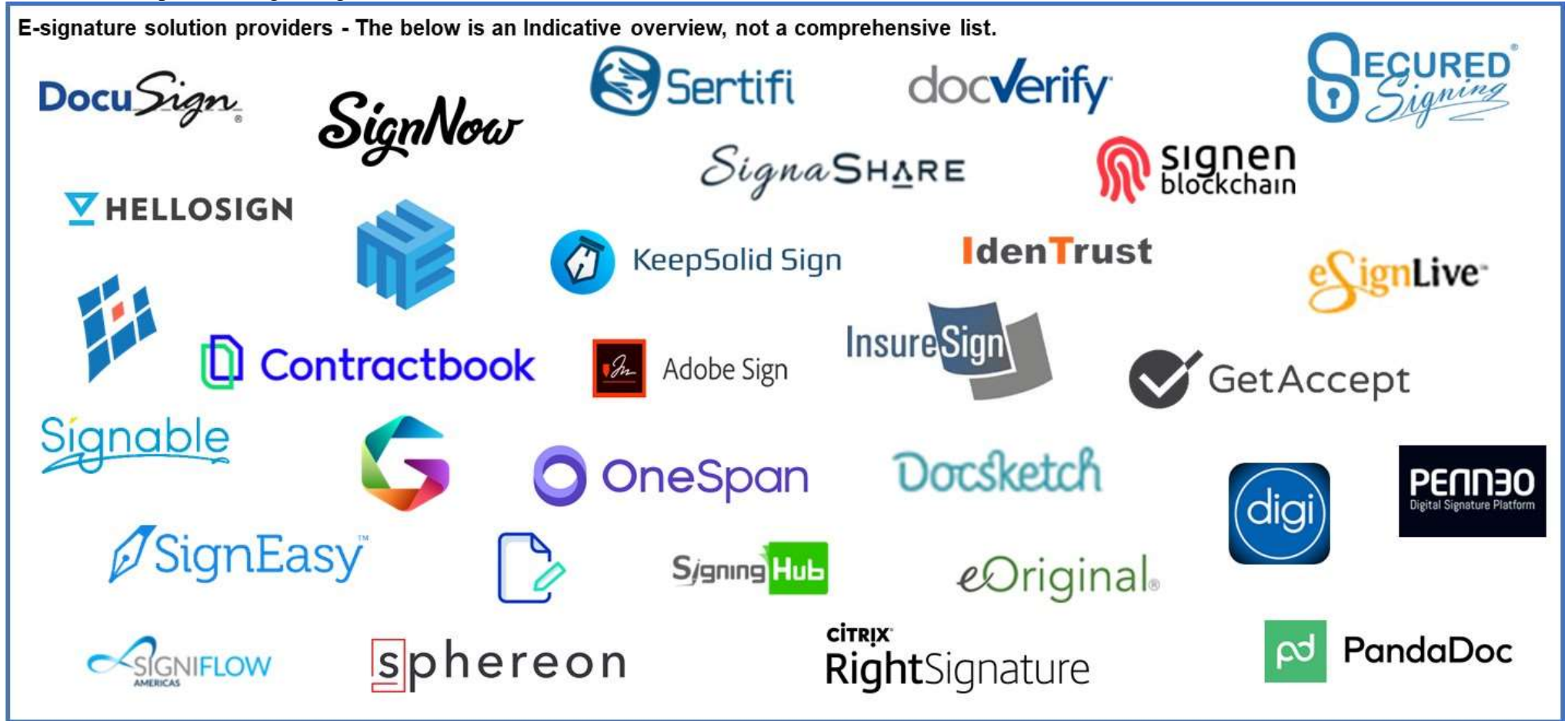
Vendor landscape in the customer digital on-boarding is categorised in the below table

The below is an Indicative overview – Not a comprehensive list.






Onboarding / Identity Verification / Online Authentication		Onboarding / KYC risk assesment	
Identity Document verification 	Biometric Identification (behavioral and physical) 	E2E Onboarding / Due Diligence / risk Assessment 	

Vendor landscape in the digital signatures is shown in the below table

E-signature solution providers - The below is an Indicative overview, not a comprehensive list.



Some vendor details pertinent to digital on-boarding and e-KYC solutions are elaborated in the below table.

 <p>REFINITIV, a global provider of financial markets data and infrastructure, is set to expand its suite of financial crime solutions into the wealth industry as increased scrutiny from regulators and the demand for a more frictionless client experience from investors drive the need for more digital KYC and onboarding processes. The push into the Wealth and Advisory segments is set to expand on Refinitiv's World-Check Risk Intelligence and the company's expertise in delivering trusted data into client workflows using the cloud and API technology. Traditional wealth onboarding is paper centric and cumbersome, new technologies offer opportunities to streamline this process, while improving the customer experience and decreasing risk. Refinitiv will help Wealth Managers to simplify their day-to-day risk management, onboarding and monitoring decisions through the latest innovations in AI and cloud computing, combined with its market leading data and KYC solutions such as World-Check.</p>	 <p>TRUSTDOCK, Japan's only provider of e-KYC / identity verification APIs has announced new investment from STRIVE, 500 Startups Japan, Sony Innovation Fund, Mitsubishi UFJ Capital, Mizuho Capital, and SMBC Venture Capital. With the investment, TRUSTDOCK will accelerate its efforts to build a social infrastructure by offering digital identity that is compliant with laws and regulations in different industries, including the e-KYC requirements of Japan's new Anti-Money Laundering Act. KYC as a Service "TRUSTDOCK" is Japan's only API service for e-KYC/identity verification. By only embedding APIs, it ensures KYC that is compliant with different laws including the Act on Prevention of Transfer of Criminal Proceeds, Mobile Phone Misuse Prevention Act, Secondhand Articles Dealer Act, Worker Dispatching Act, Online Dating Site Regulation Act, Private Lodging Business Act, etc.</p>	 <p>AI has been identified as the most effective solution in terms of cost and time to automate KYC processes by managing and screening high volumes of customer profiles and transactions, learning from and adapting to changing environments and by automating repetitive tasks. Fineksus is an AI software managing the KYC processes for financial institutions as HSBC, ING Bank and Bank of China. Their program involves the identification and verification of customers, the customer's screening before onboarding, the risk calculation of customers based on dynamically-defined rules of risk categories, etc.</p>	 <p>Virginia-based biometrics and identity assurance software company Daon, and France based CTMS, a digital onboarding and anti-fraud specialist have entered in a partnership agreement in France and other French-speaking countries. CTMS has been providing document and Identity fraud solutions to banks and Financial Institutions, their diverse clientele also includes administrations, social agencies and businesses in France, Africa and abroad. This partnership is expected to enable CTMS to leverage and deliver Daon's biometric technologies in the space of KYC and onboarding solutions to financial institutions and other industries in France.</p>	 <p>Deutsche Bank selects Finantix's solutions for fueling KYC processes. In order to accelerate its client onboarding and KYC process, Deutsche Bank Wealth Management selected the AI-powered KYC solution, Finantix. Finantix provides multi-language, Natural Language Processing (NLP) and AI-powered technology for regulatory requirements. Finantix will help the bank to automate their current data collection, ensure rigorous compliance checks while making better use of their human talent in analyzing and investigating the results, and finally, will improve the quality of the bank's controls and risk management. Finantix classifies all available individual or company KYC accessible data and content in different formats. The solution also allows for screening for adverse news and background information as well as for carrying out detailed risk assessments.</p>
--	---	---	---	--



ARAB COUNTRIES REGULATORY SURVEY

9. ARAB COUNTRIES - SURVEY RESULTS

The extent of digitization drives the government and its citizen’s interactions with the various sectors. Mckinsey created a digitization index comparing the extent of digitization across the middle east countries as illustrated in below infographic.

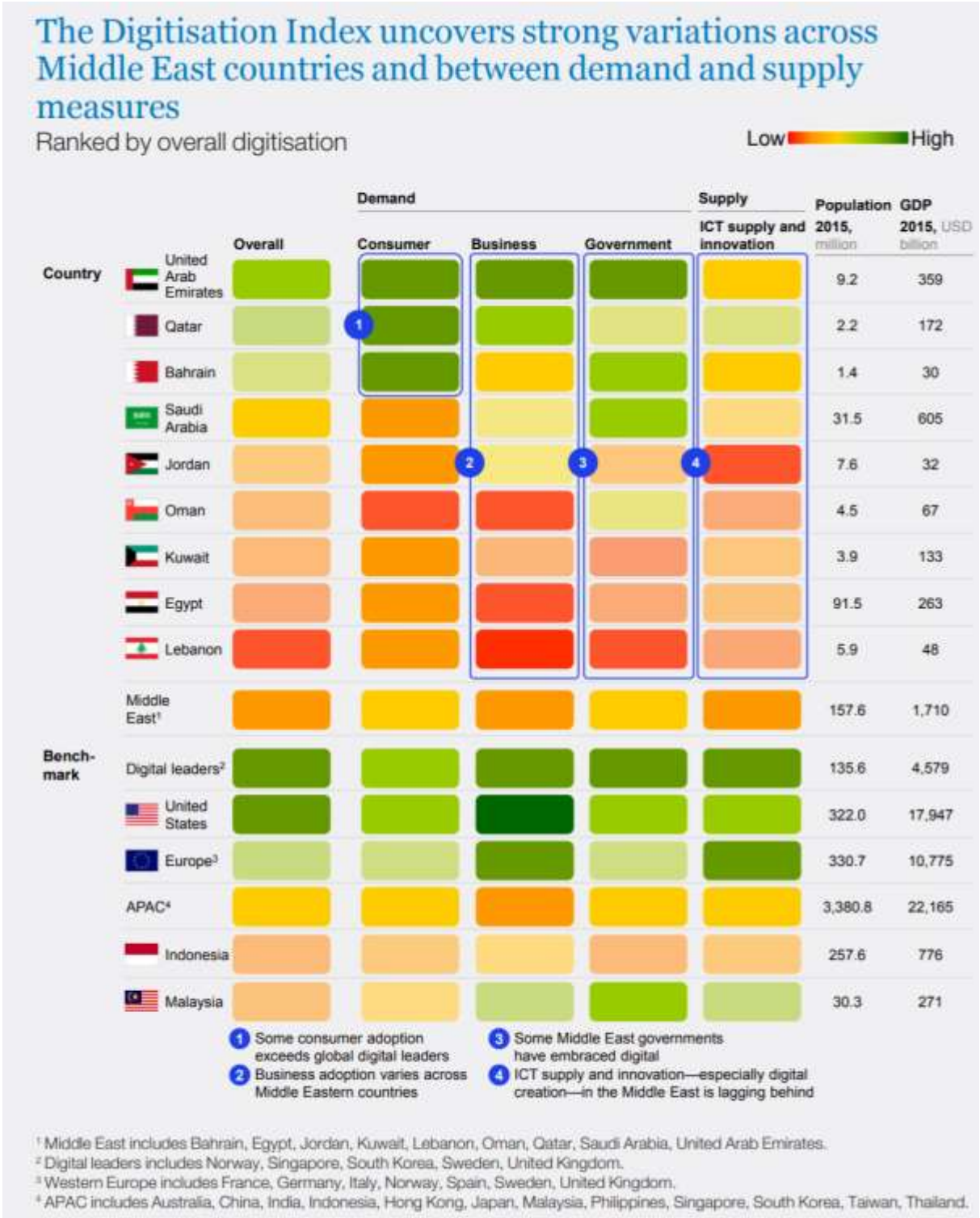
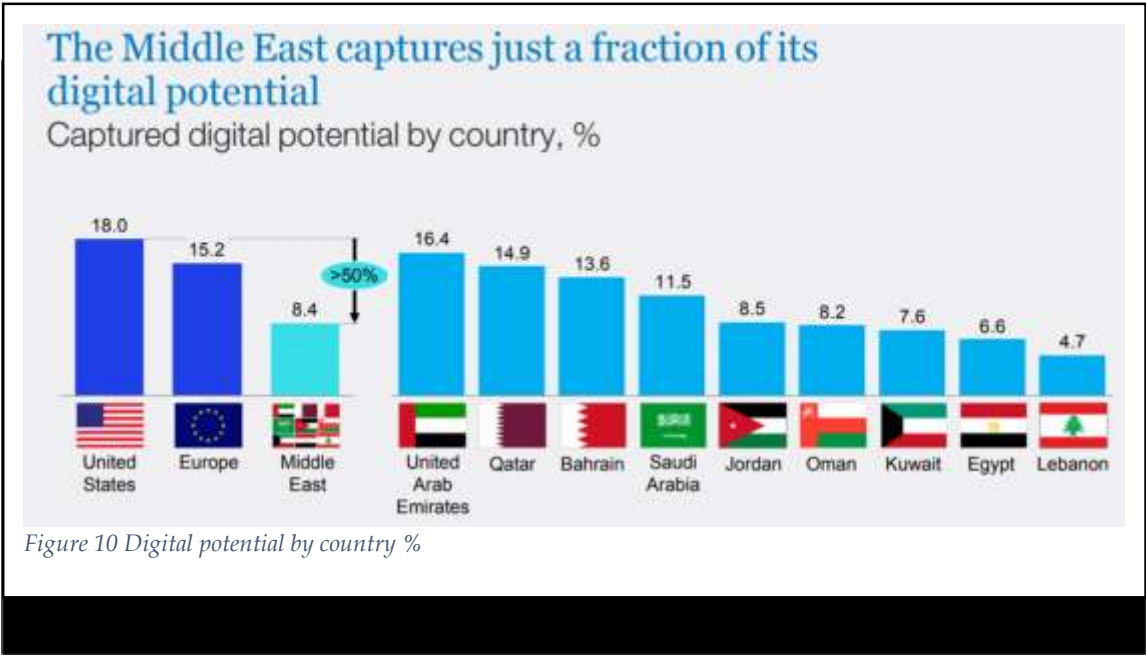


Figure 9 Digitisation Index - Middle East countries

Based on a recent survey that has been conducted by the Regional Fintech Working Group of the Arab Monetary Fund, a total of 24 respondents from the Arab countries including central banks, capital market authorities and AML/CFT units from the Arab region has participated actively in attending the survey on Digital ID and e-KYC. The main findings will be highlighted under.

With regards to the current physical KYC processes, the majority of responses received from the Arab countries including Saudi Arabian Monetary Authority, Central bank of Tunisia, Central bank of Oman, Central Bank of Algeria, Central Bank of Qatar, claim that the client onboarding is done generally by having financial institutions obtain KYC information from their clients in accordance with relevant laws, regulations and guidelines that are mostly based on FATF standards and the like. All the collected information then gets verified using independent reliable sources that retrieve the data from the concerned government bodies. Financial institutions frequently update the KYC process based on each client’s risk profile.



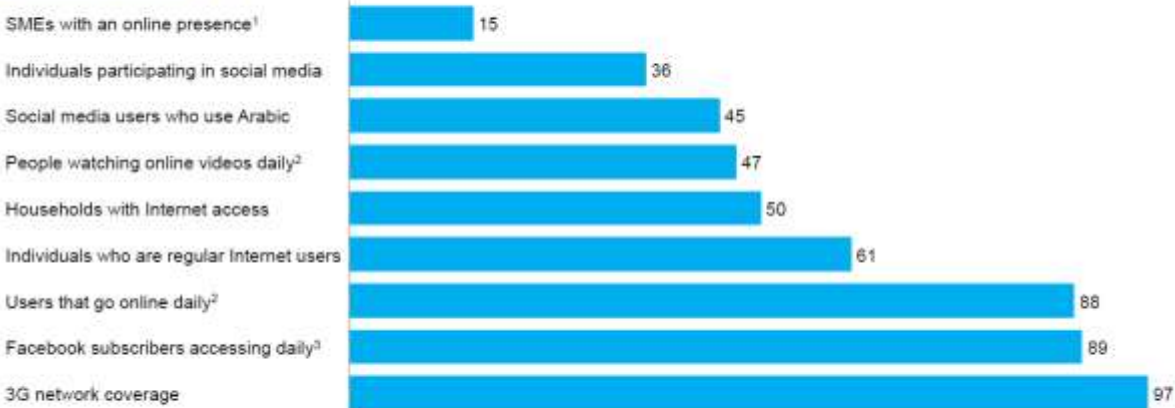
For Moroccan citizens living abroad and wishing to avail banking services remotely, Bank Al Maghrib requires that banks establish appropriate measures of verification and identification of customer’s identity that shall be as effective as that for face to face customers. Banks may be obliged to verify the identity if non face to face customers using complementary measures such as requesting additional documents in order to corroborate the customer identity and requiring that the first transaction consists of credit wire transfer originating from a bank account held by the client at a bank within a jurisdiction that is compliant with FATF standards. Also applying

enhanced due diligence on the customer and the account as long as customer has not established a face to face contact with bank.

Palestine Monetary Authority Launched the Bank Accounts System recently that will help financial institutions including fintech companies enhancing the levels of financial inclusion and environment of transparency, disclosure to reduce operational risks and facilitate and simplify account opening procedures, including achieving the principles of know your customer (KYC) when opening accounts and constantly updating customer’s data to help banks take sound banking decision.

Though Middle Eastern businesses lag behind in digitisation, consumers are leading the charge

Middle East average, %



¹ Saudi Arabia only.

² Google Consumer Barometer 2015 for the United Arab Emirates and Saudi Arabia only.

³ Middle East, North Africa, and Levant, based on Arab Social Media Report 2015, launched at Arab Social Media Influencers Summit 2015.

SOURCE: Networked Readiness Index 2015, World Economic Forum; 2016 Digital Yearbook; We Are Social; Digital Adoption Index, World Bank; The Connected Consumer Survey 2015; Google; McKinsey analysis.

Figure 11 Digitisation - Consumers are leading the charge - Middle east

Digitisation strategies across the region

Several Middle Eastern countries have developed strategies to drive digitisation:

Bahrain's digital strategy focuses on eight pillars: increased society participation and engagement; increased partnerships and private sector ICT readiness; improved national e-literacy and government IT skills; heightened protection of information and user rights; higher performing, collaborative, integrated, and efficient government; comprehensive and effectively managed quality service offering; enhanced e-government channels and user experience with increased service uptake; and greater innovation and entrepreneurship.

Egypt's ICT 2020 Strategy focuses on three main pillars: the transformation of Egypt into a digital society, the development of the ICT industry, and the establishment of Egypt as a global digital hub.

Jordan's digital strategy focuses government initiatives focusing on applications related to electronic services, definition and development of appropriate technological infrastructure, definition and development of the structure of adequate legislative and regulatory environment, effective process re-engineering to achieve high efficiency, transformation and development in the field of education, training and knowledge transfer and change management and restructuring of government institutions.

Saudi Arabia has listed various digital initiatives in its National Transformation Program 2020 such as "improve the efficiency and effectiveness of the healthcare sector using information technology and digital transformation" and "establish emerging technology companies with added value to contribute to the increase of local content". However, these initiatives are isolated in a sector view and could be accelerated with an overarching holistic approach for the whole nation.

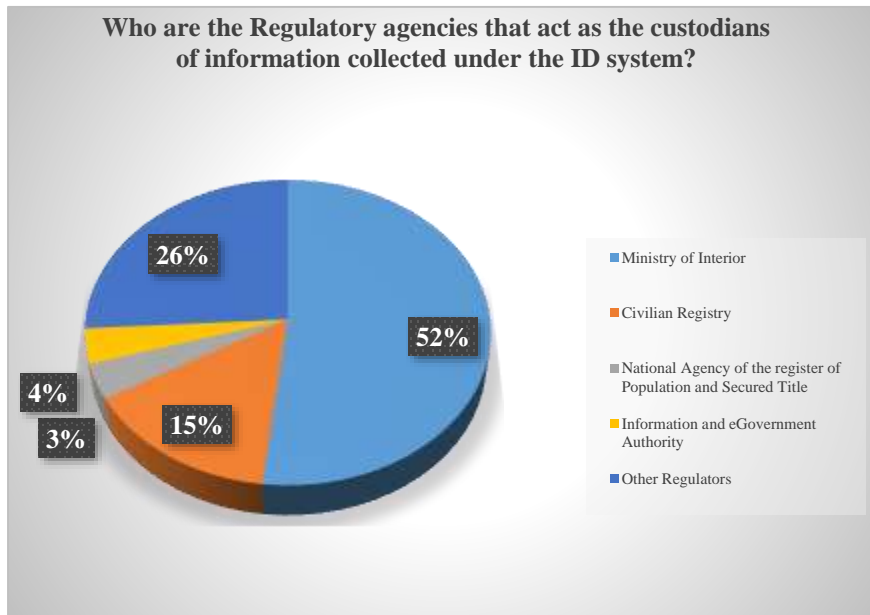
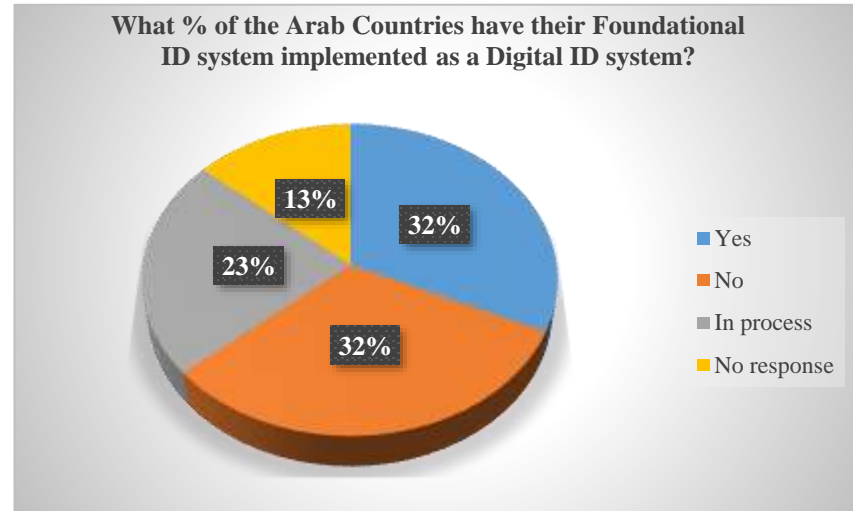
Oman has the Digital Oman Strategy (eOman), which focuses on six main pillars: society and human capital development; enhanced e-government and e-services; ICT industry development; governance, standards and regulations; national infrastructure development; and promotion and awareness.

Tunisia has a National Strategic Plan "Digital Tunisia 2020" and its main aims are to ensure social inclusion and reduce the digital divide, strengthen digital literacy, evolving towards an agile and efficient e-governance and contribute to the reduction of unemployment and job creation in the digital and offshoring sectors by supporting entrepreneurship and stimulating innovation with their "Smart Tunisia" program.

The United Arab Emirates' digital government initiatives are Smart Dubai and Abu Dhabi. Smart Dubai facilitates collaboration among private sector and government partners; it was established to empower, deliver, and promote an efficient, seamless, safe, and impactful city experience for residents and visitors. To achieve its strategic pillars, Smart Dubai aims to introduce strategic initiatives and develop partnerships to contribute to its Smart Economy, Smart Living, Smart Governance, Smart Environment, Smart People, and Smart Mobility dimensions. Similarly, the Abu Dhabi e-government programmes and digital transformation initiatives discuss key digital transformation plans and projects—which include enhancing "the formation of a smart government based on significant and effective services for users, ranging from individuals to the private and government sectors"

Figure 12 Middle East Digitisation strategies - a few examples

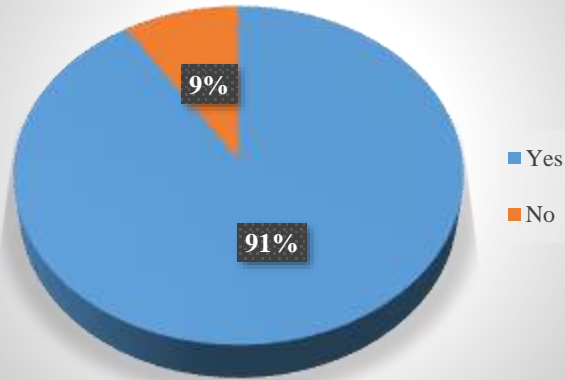
Survey Response Analysis:



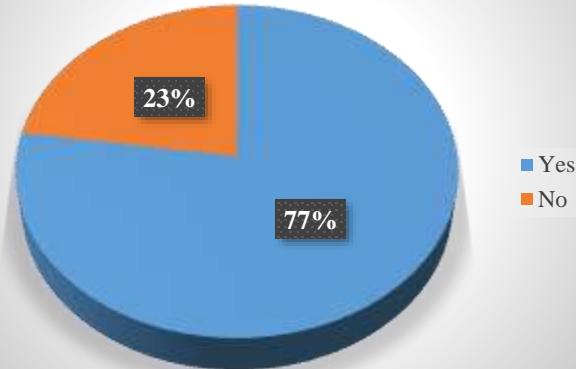
Civilian Registry- Jordan's Civil status and passport department, and Kuwait's Public authority for Civil Information perform the same duties as Sudan's Civilian Registry.

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)

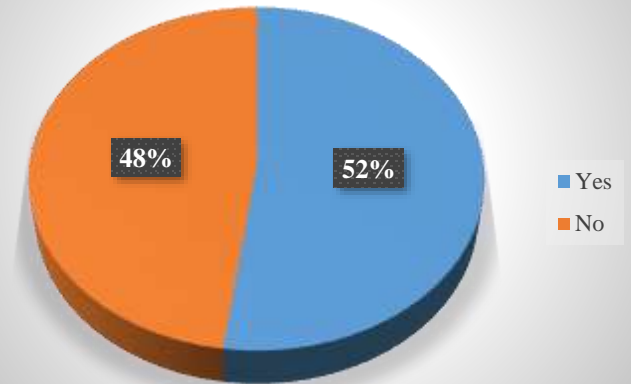
Do the Arab Countries have any regulation governing the use of National ID data?



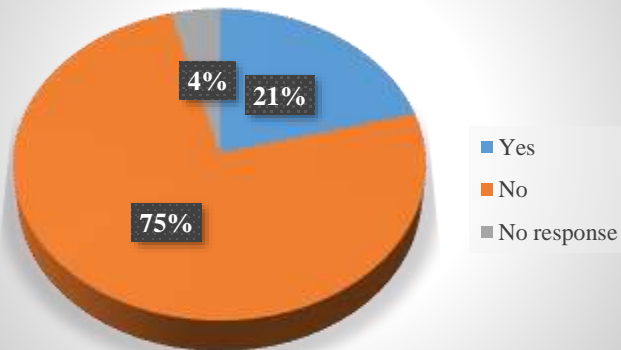
Are there any regulations in place or being drafted in relation to e-signature?



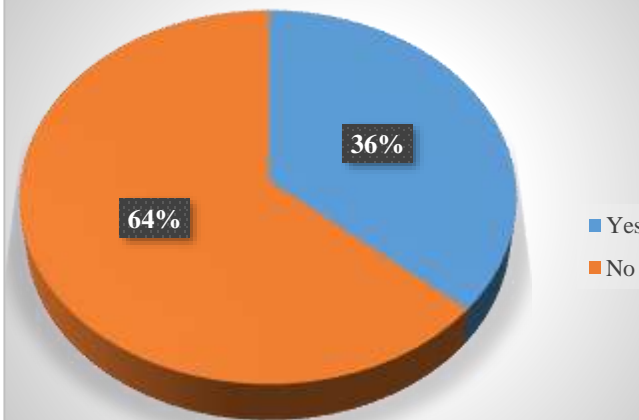
Do Financial Institutions have access to the database in case they need to open accounts?



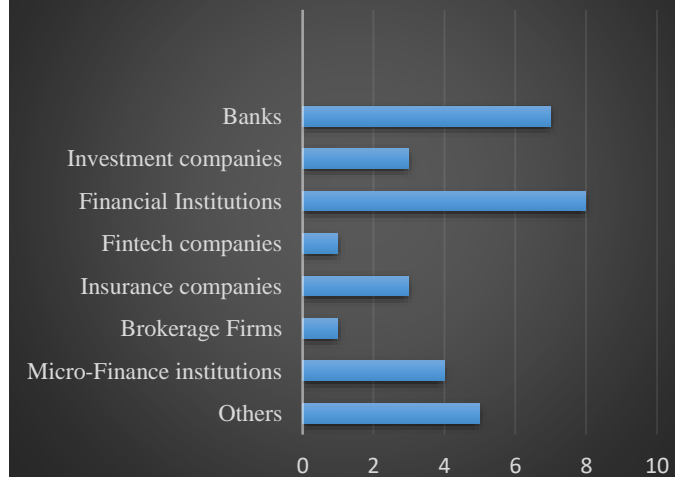
Do the Arab Countries' National Database also capture financial transactions data?



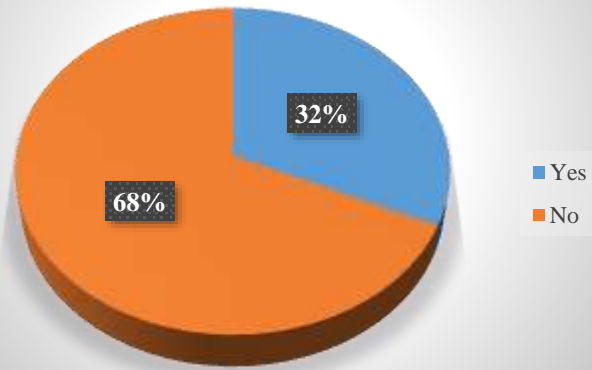
Is the National Database linked to credit bureaus?



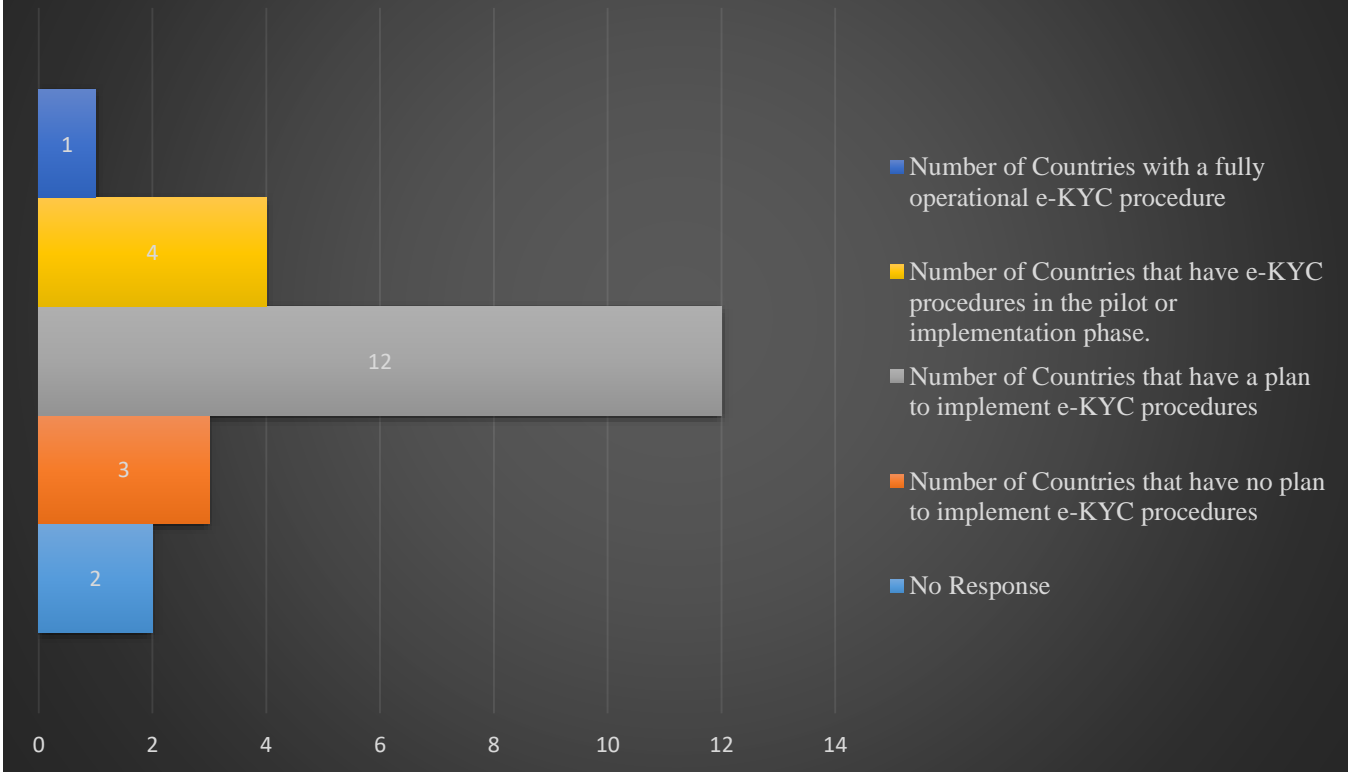
The types of financial institutions that have access to the database

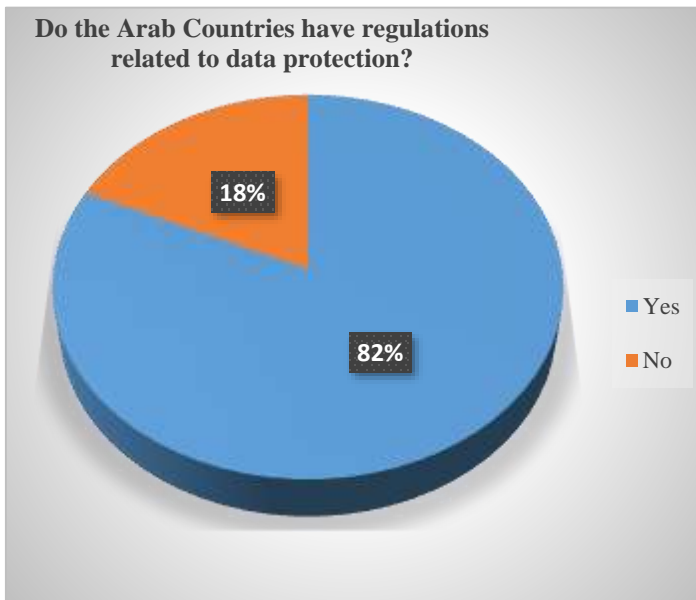
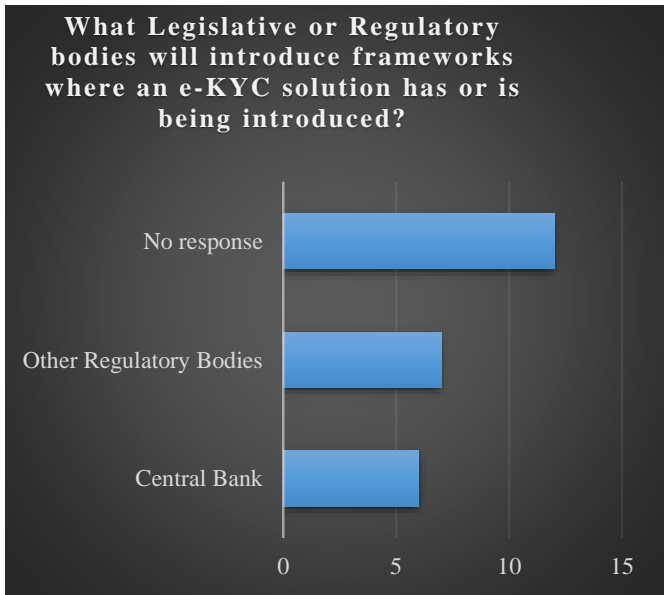


Do the Arab Countries have any recognized private sector initiatives for creating a Digital ID system in their respective countries?



The Arab Countries' position on the implementation of e-KYC procedures



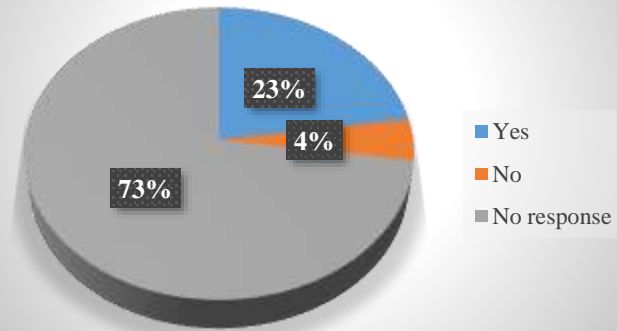


9% of the Countries have indicated the use of blockchain technology and 14% of the Countries have also suggested that a repository will be created for a database. However, 77% of the Countries have not responded.

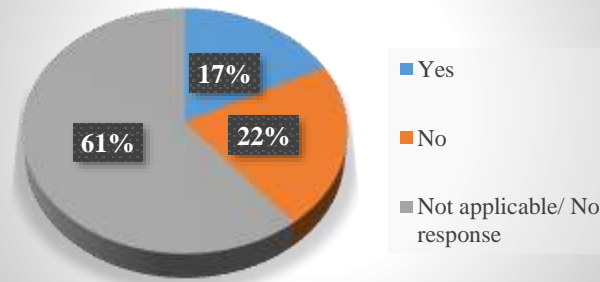


Use of Underlying technologies

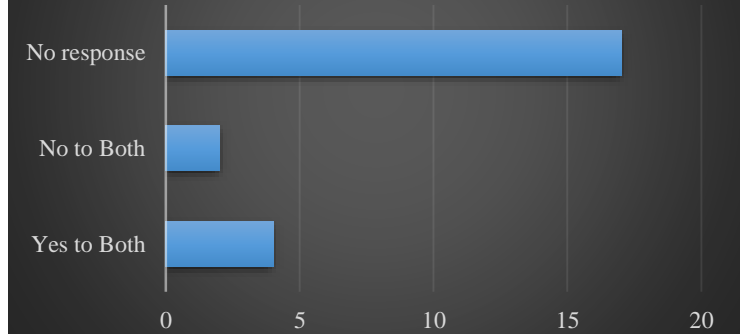
Would the store/vault be a central digital vault available for all banks to leverage and consume with customer consent?



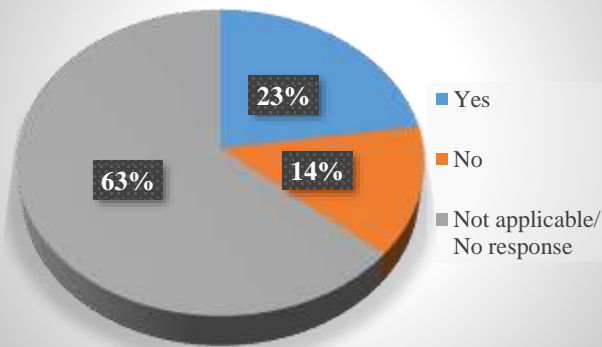
Can the customer upload/amend documents in this vault?



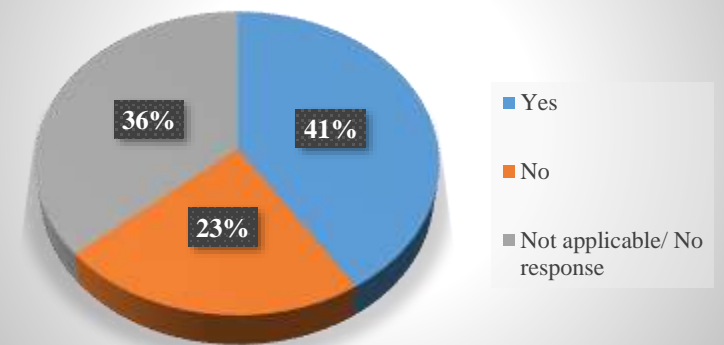
Are the Countries that have or are introducing e-KYC considering the usage of Digital Signatures in ID authentication and Document Signing?



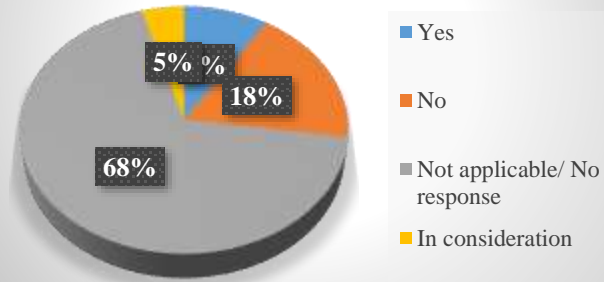
Are such contributions captured at the time of Identity creation/update in the country?



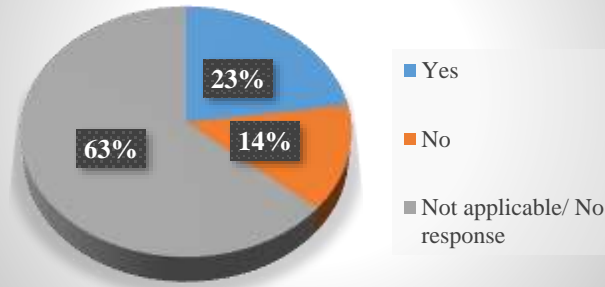
Are the Arab Countries actively amending the law to allow the use of digitally signed documents/artefacts to have legal status?



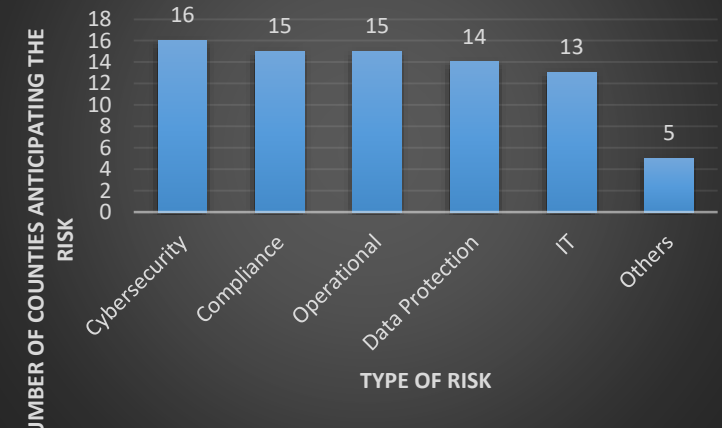
Have the Countries that have or are introducing e-KYC considered the use of banks as an additional vehicle for authentication and onboarding customers to the central digital identity repository?



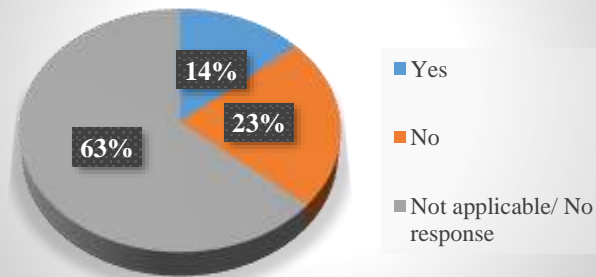
Do the Countries that have or are introducing e-KYC have any special considerations with respect to GDPR?



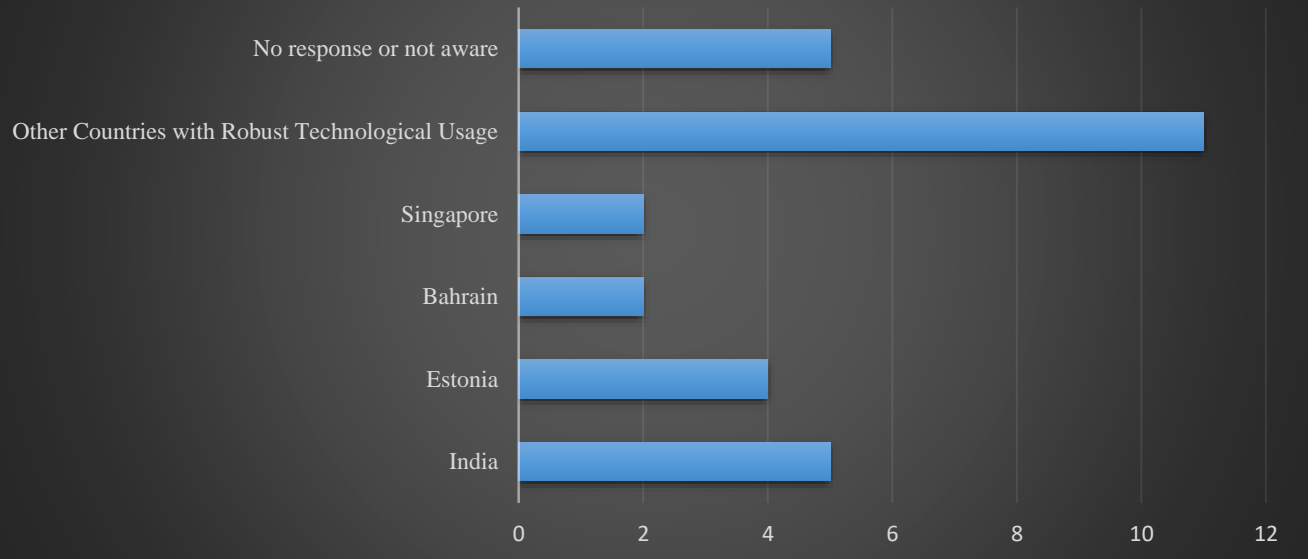
What kinds of risks do Arab Countries anticipate from the implementation of E-KYC?



Is there any misuse of the e-KYC implementation such as fraud, manipulation?



Which Countries' Digital ID and e-KYC system should be covered as a case study?



10. CONCLUDING REMARKS

The importance of Digital identification has been established as a means to propel economies and create deep and lasting value to the quality of life of the citizens and also to the efficient and cost effective functioning of the Governments. There are myriad digital identification mechanics and associated infrastructure and governance mechanisms which were saying being played out among the Arab countries.

We also see almost all Arab countries embarking upon digital identification for their citizens as part of their vision and digitisation roadmap.

The goal of increasing digitisation comes with both significant challenges and huge opportunities. These goals are not unsurmountable and there are many enabling foundational technologies and vendors who can provide solutions in this space. Best practice examples across the world abound which can be adapted for specific application in the Arab countries.

Customer digital on-boarding into the financial system is just one use case of the application of digital identification and provides means of increased uptake of the population into the banking system including the under-privileged sections of society. This enables multiple value added services which can be enjoyed by the citizens in all arenas of public interaction in their daily lives –B2B, B2C, P2P, G2P, G2B – and also fosters development of a true global world order.



To maximize the myriad economic and social gains at the digital frontier, countries must also develop the requisite technologies and associated human capital

Digital Mckinsey



The technical architecture towards achieving true customer digital on-boarding with robust eKYC and compliance, anti-money laundering and anti-terrorist financing deterrents and controls is quite mature and several case studies are available to be adapted. The complementary technology of electronic signatures is also explained and its role in the interaction of the citizens with the respective financial institutions has been elaborated and this technology is also quite mature and ready for adoption.

The role of the Public-private sector partnerships cannot be underestimated coupled with the role of academia in developing the citizenry and human capital ready for the digital future.

The survey feedback from the Central banks of the Arab countries reveal that the vision of the Arab countries to also focus and lead in the domain of e-governance for betterment of the lives of their citizens and residents and also shows that several countries have already embarked on rolling out foundational technologies to meet their stated of goals of digitization and enabling a true digital economy.

Opportunities for enabling a digital revolution.

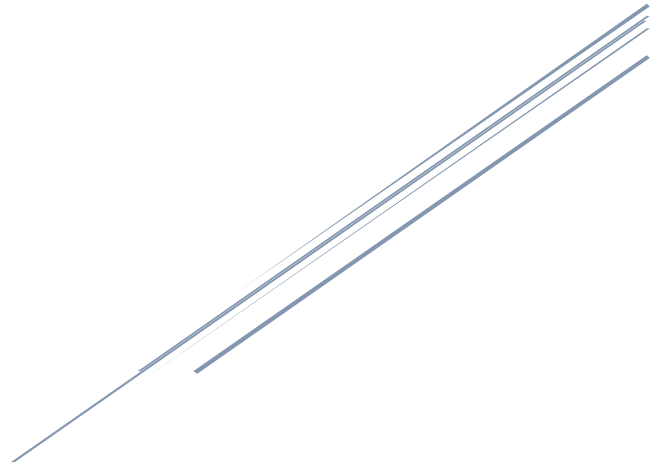
The following graphic provides a strategic view of the opportunities in enabling private and public sector digital revolution.

Government	<ol style="list-style-type: none"> 1. Move from e-government-focused digital initiatives to full digital economy development 2. Empower national digital agencies 3. Create policy frameworks that foster, and do not hamper, digital innovation 4. Seize the opportunity of large public IT spending to create home-grown IT players at scale
Business	<ol style="list-style-type: none"> 5. Take the once-in-a-lifetime opportunity to create critical digital platforms for the region 6. Step up the collaboration among corporations and digital disrupters in the region 7. Embrace agility through digital to address the ever-faster business environment
Funding	<ol style="list-style-type: none"> 8. Scale digital VC funding and increase visibility of investment opportunities
Talent	<ol style="list-style-type: none"> 9. Create digital curricula and seamless learning pathways from primary schools to higher education and into employment 10. Rethink how to attract and retain digital talent and reconsider applicability of nationalisation to digital

Figure 13 Opportunities for enabling a Digital revolution



REFERENCES



11. REFERENCES

1. Institute of International Finance. (2019). *Digital Identity: Key concept*. Retrieved from https://www.iif.com/Portals/0/Files/content/Regulatory/iif_digital_id_07022019.pdf
2. DIGITAL KYC PROOF-OF-CONCEPT WHITE-PAPER 1 Overview of the Digital KYC authentication system 1. INTRODUCTION “Fraud Management. (2019). Retrieved 11 November 2019, from <https://webcache.googleusercontent.com/search?q=cache:jOUIFcJ9a-wJ:https://findasystem.com/download/KPI%2520FINDA%2520FSTI%2520P OC%2520paper%25201%2520-%252019Nov2018.pdf+%&cd=1&hl=en&ct=clnk&gl=om&client=firefox-b-d>
3. Helix Institute of Digital Finance. (2019). Retrieved 11 November 2019, from <http://www.helix-institute.com/blog/progress-and-challenges-kyc-and-digital-id-venkata-n-atluri-and-david-cracknell-4>
4. Jee, J. (2019). How can traditional banks meet the fintech challenge? Retrieved 11 November 2019, from <https://www.telegraph.co.uk/business/business-reporter/customer-onboarding/>
5. Thomson Reuters. (2016). *Digital Innovation in Client Onboarding and KYC: In a digital world, don't get left behind*. Thomson Reuters. Retrieved from <http://Digital Innovation in Client Onboarding and KYC: In a digital world, don't get left behind>
6. *Digital Identification: A Key to Inclusive Growth; A Summary of Findings*. Mckinsey Global Institute, 2019, <https://www.mckinsey.com/~media/McKinsey/Business Functions/McKinsey Digital/Our Insights/Digital identification A key to inclusive growth/MGI-Digital-identification-Report.ashx>.

7. *G20 Digital Identity Onboarding*. World Bank Group, 2018, *G20 Digital Identity Onboarding*.
8. Vander, Ronan, et al. "Digital Onboarding for Financial Services, A Must-Have for Digital Natives." *Inside Magazine - Part 01 - From a Digital Perspective*, 2018.
9. "NIST Glossary." NIST, NIST, <https://csrc.nist.gov/glossary/term/NIST>.
10. *Technology Landscape for Digital Identification*, World Bank Group, 2018, <http://documents.worldbank.org/curated/en/199411519691370495/Technology-Landscape-for-Digital-Identification.pdf>.
11. Sivasankaran, Sujay. *Digital Signatures in Banking (Zafin Series, Part 1)*. Zafin, <https://zafin.com/our-articles/digital-signatures-banking-zafin-series-part-1/>
12. E&Y research, digital onboarding, e-KYC and digital signatures, Oct 2019
13. Tarek ElMasry, et al. "Digital Middle East: Transforming the region into a leading digital economy", Digital Mckinsey, Oct 2016
14. The DocuSign eSignature Legality Guide, Docusign, <https://www.docusign.com/how-it-works/legality/global>

