



DIGITAL KYC – DIGITAL'S NEXT FRONTIER

Infosys® | Finacle



The Rise of Digital KYC

Know your customer (KYC) is the process of a business identifying and verifying the identity of its clients. In banking, the process includes customer identification, sanctions screening, customer risk profiling (such as AML risks), and other customer due diligence and investigation. Traditionally financial institutions have been collecting application forms along with the physical supporting documents like Proof of Identity and Certificate of Incorporation. Many of the KYC activities happen within a single ecosystem – the bank itself.

However, KYC cannot be considered as a one-time process. It is a recurring process of both collection and maintenance across many banks and regulators. Because KYC and identity authentication is involved in so many financial services processes - from opening a bank account to making a payment to making an insurance claim – a digital KYC will have a revolutionary impact on banking and financial services industry.

Digital initiatives in banking is not a new concept – in fact it has been the buzzword for several years now. Banking institutions have been and will continue to focus on how to better deliver their products and service their customers via digital channels. But the KYC process is still dependent on traditional methods, requiring physical presence – of the customers and bank personnel, involving significant paperwork and time – leading to customer friction and high costs of acquisition.

This process of onboarding is most often necessitated by the Central Banks/ Regulatory Authorities, leaving banks little choice in the matter. As it is a highly regulated and heavily penalized area of

banking, a change in the process would require regulatory buy-in. Additionally, infrastructure to enable digital KYC and technology support would be required for banks to enable digital onboarding. In a sense, digitizing the KYC process is the last mile in digitizing banking operations in a customer journey.

Digitization is key to a more meaningful and successful KYC compliance. It will ensure centralization of KYC, which may result in negating bottlenecks during Internal and external audits, client onboarding, transaction processing and much more.

What's Happening?

In the recent past, we are seeing increasing focus on digital KYC. We see three main factors that are inducing this change. The first is due to the fact that several governments are looking at digital identities, which banks can leverage for KYC – among other things. Secondly, banks are beginning to understand that the first interaction with their prospects needs fine tuning as their customers are now used to signing up for other services within minutes. Finally, a flurry of companies (start-ups and established players) are providing ecosystem built using the latest technology to banks, leading to banks treating the KYC process as the next digital frontier to be charted.

Government as a Catalyst

Several countries have instituted or are in the process of instituting digital identities. Governments are focusing on building an architecture that lends itself for multiple uses, is API driven and is exceedingly secure. While not all the digital identities

are currently being used for KYC purposes, there is potential to leverage these IDs for KYC. This push for digital identities is being felt from various fronts – including the ID4D (Identification for Development) program by the World Bank. Governments and regulatory bodies across the world are now re-writing the rule books on how KYC needs to be handled – making it more digital friendly. Also, technology standards are being defined for digital identity – for example, NIST has published a set of Digital Identity Guidelines.

A prominent example is Aadhaar ID in India. Aadhaar initiative is to create unique identification for all of India's residents. In addition to providing an ID, Aadhaar enables banks to onboard their customers much more easily in an online fashion through e-KYC – online onboarding enabled via APIs. E-KYC is a process of sending customer data to UIDAI (Aadhaar issuing authority) and confirming the credentials of said customer, thus reducing the onboarding time significantly. Also, it enables financial inclusion as many of the Aadhaar card holders who do not have any other govt. issued ID can now enter the banking system. In addition to the Aadhaar based KYC, India has also instituted the C-KYC process where banks pool their KYC data in a central repository which can then be used for onboarding by any other bank in the country.

Monetary Authority of Singapore has announced a National KYC registry called "MyInfo" – where residents can update their information on a platform which can then be re-used for KYC purposes. The MAS has conducted a pilot with 4 banks on the same.

In Estonia, every citizen, resident has an e-identity, which can be used to open an account or access their bank accounts. This is being looked at as the gold standard for e-IDs across the world. In addition to banking services the e-id acts as a national health insurance card, can be used for voting, to check medical records, submit tax claims, and to use e-prescriptions.

In addition, there are several other countries, like Thailand, Pakistan, Algeria, to name just a few, that are looking at leveraging their existing e-IDs or creating a digital ID infrastructure – which can assist in digital KYC.

Initiatives from Banks

The onboarding process is the first interaction that the customers have with their banks. Engaging the customers starts with smooth, easy and fast onboarding. Today, banks are realizing that this would be the frontline of the war with fintechs and other competitors. Banks are now increasingly focusing on making their onboarding process frictionless and consumer –friendly to compete with the nimble fintechs and digital natives.

The interest in the space is evident with banks like Deutsche Bank undertaking projects to create an online identity platform which can be used across industries. Several banks are also looking at harnessing Blockchain and distributed ledger technology to solve the digital identity problem. WEF published the Blueprint for Digital Identity, where banks are positioned as the ideal candidates to play a pivotal role in filling the gap for digital identity – as they are custodians to extensive verified customer data, which cover multiple types of customers (individuals, legal entities, assets) and in certain cases span multiple regions and geographies.



In addition, some banks are approaching the digital KYC process as a revenue opportunity. Banks traditionally have a treasure trove of customer information, which can be monetized (with consent). For example, Capital One is experimenting with a Digital Identity API, available to other businesses through which its customers can use Capital One credentials to sign up for third party apps. Regulatory initiatives such as Open banking, PSD 2 etc. that mandate banks to share customer data, relegating banks to basic providers of infrastructure, are also encouraging banks to find ways and avenues to monetize the data available to them.

Banks are also taking a consortium approach to implement a shared KYC. In 2017, Royal Bank of Canada, Bank of Montreal, Scotiabank, CIBC, TD Bank and National Bank of Canada, proposed to create a “nationwide” digital identity ecosystem that “will make transacting and sharing personal data online easier and safer”.

Eco System Support

Besides regulators and banks, ecosystem players such as telecoms, e-commerce firms, and Fintechs - have started to realize that digitization can help institutions in providing an easy and hassle-free process towards KYC maintenance, as well as in fulfilling the regulatory requirements.

There has been a flurry of activity in digital identity management. One World Identity has listed 187 companies with presence in this space. Their value propositions span the entire spectrum from attribute

verification (prove or verify identity attributes) to authentication to monitoring. These companies provide a platform for banks to use in order to plug the gap of digital identity. They use technology to the maximum advantage – distributed ledgers, cloud, APIs and encryption.

What's Enabling Digital KYC?

From the technological perspective, digital KYC was born as a result of the emergence and the convergence of contemporary technologies. These technologies came from advances in APIs, security, analytics, AI and cloud storage. There are three key technologies that contribute to the anatomy and the characteristics of digital KYC.

Digital identity. Digital and biometric identity is well and truly established as one of the most critical components of digital KYC. Many new digital identity technologies and regulations have emerged in the last few years. For instance, a new ICAO working group on digital travel credentials has been created, led by Australia. Other examples include digital driver's license in USA, e-residency program in Estonia (as mentioned early) and eIDAS in Europe. Moreover, numerous new national eID programs (including card and/or mobile-based schemes) have been launched across Algeria, Italy, Thailand, Netherlands, Bulgaria, Norway, Liberia, Poland and many others. Many of these programs now include biometrics, the majority in the form of fingerprints.

API Banking and Open Platform. APIs are sets of protocols that define how one application interacts with another, usually to facilitate an information exchange. APIs expedite the realization of an interconnected and interdependent ecosystem that promotes (intra and cross-sector) partnerships, stimulates co-operation and increases information/resource sharing between organizations, including banks, regulators, telecoms, e-commerce firms and Fintechs in case of digital KYC.

Cloud. Cloud computing provides economies of scale, enhances operational efficiencies, and delivers potential cost savings given that thousands of customer records are needed to be stored in a secure place and to be maintained regularly. A secure cloud infrastructure is an enabler for digital KYC innovations, working well together with open API.

Technology is always working as a catalyst for change. With the support of digital identity and API banking - along with the development of other technology innovations such as blockchain and IoT - these emerging technologies are and will continue to refine a real-time, secure, accurate and interconnected digital KYC process.

The future of Digital KYC

#1 Digital Identity in the center of Digital KYC

We believe that the future of digital KYC is very closely linked to the evolution and future of Digital Identity. Digital Identity of the future will be an amalgamation of physical identity (like biometrics), digital footprint and device footprint. Digital identity will be owned and controlled by individuals allowing each individual will to decide what information to share at what point and with whom.

It is not farfetched to imagine a future where the KYC process is entirely driven by devices with zero human interaction. For example, a customer could authenticate himself and instruct his virtual assistant to open an account with a bank. The virtual

assistant opens the banking application, fills in details, accesses his digital identity (which is on the cloud) and share the same with the bank. Once the bank identifies and validates it via his Digital Identity, his account is opened.

#2 Moving to National and Global Digital KYC

KYC at banks will also evolve to match the evolving digital identity trends. Already today, as stated above, several geos are harnessing the national digital IDs for KYC. Sharing of digital identity across national or even global brings lots of synergy and efficiency, not to mention the benefits of AML. While national KYC is not only about data, but also process. A standardized and seamless KYC process can also make KYC become an API based service capable of being accessed by the digital ecosystem.

#3 Digital KYC as part of Customer's "Digital Life"

Eventually, a secure, efficient and accurate KYC is needed across many industries, not just banking. Banks may have the most rigid requirements in KYC due to the nature of the business. In the year 2018 and future, along with the trends of digitalization, we foresee digital KYC becoming a part of customer's digital life. KYC services offered by the commercial and central bank will become an open service that can be accessed from the ecosystem – so that any third party, such as an e-commerce portal, a telecom, or a Fintech are able to integrate digital KYC into their customer journey seamlessly.



Recommendations to Banks

Rethink Process and Technology – A fundamental change in the process of completing KYC needs to be undertaken. KYC of the future will not be a siloed activity for banking, but rather banks will have to be a part of the larger movement to accept and utilize digital identities for onboarding /payments /transactions. Banks will have to re-imagine the onboarding process, taking into account paperless, mobile and biometric lead KYC processes. APIs, Blockchain, Biometrics and IoT will all play an increasing role in the identification and authentication process.

Scan the Horizon – Today, in several geographies, government initiatives have made it easy for banks to digitize their onboarding process, while in others it has been mandated. Additionally, there are many players in the identity space that provide solutions for digitally verifying KYC of prospects and customers. Another suggestion to banks is to experiment in a sandbox environment which can then be

taken to the regulator for their approval. Banks need to scan the eco-system of the geos they operate in, in order to make the best use of the available resources.

No Time like the Present – Banks have waited too long to digitize their KYC processes, hence leading to lengthy and inefficient onboarding process. While there is increasing regulation around KYC/ AML, there is increasing expectation from customers on this front. Customers are today used to fast, digital onboarding processes that they experience in other aspects of their daily life, demanding the same experience from their bankers as well. The time is ripe for Banks to explore these options – either via an existing eco-system, or take the lead to create an eco-system.

There are many benefits to be realized – greater customer experience, reduced costs, and in fact, if used effectively, a new revenue stream.

Authors



Ethan Wang
Product Manager, Infosys Finacle



Shweta Shivaraja
Product Manager, Infosys Finacle

About Infosys Finacle

Finacle is the industry-leading universal banking solution from EdgeVerve Systems, a wholly owned product subsidiary of Infosys. The solution helps financial institutions develop deeper connections with stakeholders, power continuous innovation, and accelerate growth in the digital world. Today, Finacle is the choice of banks across 94 countries, and serves over 848 million consumers – estimated to be nearly 16.5 percent of the world's adult banked population. Over a billion bank accounts are powered by Finacle globally.

Finacle solutions address core banking, online banking, mobile banking, payments, treasury, origination, liquidity management, Islamic banking, wealth management, and analytics needs of financial institutions worldwide. Assessment of the top 1000 banks in the world reveals that institutions powered by Finacle enjoy 50 % higher returns on assets, 30 % higher returns on capital, and 8.1 % points lesser costs to income than others.



For more information, contact finacle@edgeverve.com

www.finacle.com

©2018 EdgeVerve Systems Limited, a wholly owned subsidiary of Infosys, Bangalore, India. All Rights Reserved. This documentation is the sole property of EdgeVerve Systems Limited ("EdgeVerve"). EdgeVerve believes the information in this document or page is accurate as of its publication date; such information is subject to change without notice. EdgeVerve acknowledges the proprietary rights of other companies to the trademarks, product names and such other intellectual property rights mentioned in this document. This document is not for general distribution and is meant for use solely by the person or entity that it has been specifically issued to and can be used for the sole purpose it is intended to be used for as communicated by EdgeVerve in writing. Except as expressly permitted by EdgeVerve in writing, neither this documentation nor any part of it may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, printing, photocopying, recording or otherwise, without the prior written permission of EdgeVerve and/or any named intellectual property rights holders under this document.