

Digital ID and eKYC: a catalyst for financial inclusion

A trusted digital identity framework has a powerful role in facilitating crisis response and recovery, opening the gates for financial inclusion to underserved populations.

PAYMENT

IDENTITY

POSTED ON 06.30.20

The digital identity ecosystem is increasingly complex, with a wide range of identity models and actors covering diverse responsibilities, interests, and priorities. In general, individuals (citizens or clients) are the primary end-users in a system, while government bodies and private firms are the primary providers of digital identity, authentication and services. Other key stakeholders include public actors responsible for regulation, as well as public and private actors responsible for standard setting and trust building.



While governments will obviously play a large role in digital identity systems, it is essential that there be collaboration with private sector organizations to define best practices, identify the best technologies and implement the best policies for these infrastructures.

Kate Eagle, Director of Ecosystem Engagement, Digital Business Unit at IDEMIA

A comprehensive approach of the entire digital revolution spectrum is critical for inclusive and effective policy design. There are huge synergies between ID, mobile communication and financial inclusion. It is important to understand the strengths of each of these pillars and to exploit their common capacities when constructing digital program frameworks.

Digital ID: a common goal for governments and private sector organizations

Today, it is estimated that more than 1.1 billion people worldwide lack a legally recognized form of identity.

Any digital identity system should be as inclusive as possible and reach all groups disproportionately impacted by

financial exclusion – including women, rural populations, and forcibly displaced persons. An undertaking of such proportions cannot be addressed by any organization alone.

During a recent webinar hosted by AFI Group*, Mr. Norbert Mumba, Deputy Executive Director at the Alliance for Financial Inclusion pointed out that **“This goal can only be achieved through collaborative partnerships to create seamless digital financial services ecosystems.”**

Private organizations can also play a big role in developing a widely accepted digital ID framework in absence of a national digital ID. For example ‘Federated e-IDs’ in Sweden, Norway, Finland and Denmark have solved the issue of identity verification by giving their citizens an online identity which is recognized by service providers and authorities.

When it comes to helping the most vulnerable, financial service providers need to focus on providing multiple ‘financial health’-focused services, such as micro credit services for women or insurance and credit for farmers. This can be supported by a strategy of rapidly rolling out a minimalist, but “full” digital identity. This targeted use case approach can be best implemented within the umbrella of a digital ID onboarding solution, which covers branch, remote, and self-managed onboarding options and is based on biometrics.

The role of regulation in a digital identity framework

The rules for opening new bank accounts often come with a number of requirements that vulnerable users find hard to meet – such as providing different forms of identification, proof of address, source of income – and providers find too costly to handle – such as handling paper-based forms, or conducting a personal interview.

Policy makers and regulatory bodies must take actions to support the uptake of the digitalization of financial services, especially in crises. The regulation should not only support remote onboarding and verification processes, but also make way to private parties to take a larger role in the system.

“Non face-to-face business are not necessarily high-risk,” said Ms. Shana Krishnan, Policy Analyst at the FATF during the AFI webinar. **“They can actually be standard-risk or lower-risk if they are using a trusted digital ID.”**

From remote document authentication to passive liveness detection, new technologies enable service providers and governmental institutions to seamlessly and rapidly perform the necessary user authentications and then unlock access to essential services and government aid.

Krishnan added, **“We want to make sure that the AML/CFT requirements are not a barrier to financial inclusion, nor financial services, aid, or economic recovery.”**

Designing an inclusive digital identity framework

When choosing an appropriate model for digital identity infrastructure and services, stakeholders should consider the existing identity landscape, the capacity of government systems, and the ability of the private sector to provide the required level of security and privacy protection.

For it to be successful, a digital identity framework should be:

- **Adaptable**, to local workflows and regulations
- **Omni-channel**, to ensure convenience and a true cross-channel experience
- **Interoperable**, for maximum scalability and availability, no matter the country or region and avoid vendor locking bias
- **Modular**, for easy adaptability to business needs and use cases
- **Compliant**, with Anti-Money Laundering (AML) and Counter Financing of Terrorism (CFT) regulations, as well as other local regulations

→ **Highly secure**, ensuring the highest levels of data privacy for both companies and consumers

For banks and many other financial institutions who are operating on legacy systems, this will require a large overhaul of their existing infrastructure – but that should not be a deterrent from this reform.

As Yuri Bozhor, at the Central Bank of Russia stated during the AFI webinar, digitization offers countless benefits, especially to companies “**who provide these services, and show more modern alternatives to the usual, traditional way of providing essential services.**”

Ensuring best practices

Recent events have proved the essential need for digital identity systems in facilitating global preparedness for future crises. “**This will require addressing concerns such as privacy, security, consumer trust and consent – the accessibility for vulnerable groups,**” Sally Abdelkader, GSPWG Vice Chair at the Central Bank of Egypt, stated in her closing remarks of the AFI webinar.

The frameworks that we – governments, regulators, and contributing organizations – define now have the power to set the tone for global digital and financial inclusion for decades to come. To ensure this success, we must keep in mind three best practices:

- 1 ➤ Facilitate interconnectedness between trust frameworks and identity services nationally and internationally
- 2 ➤ Design for scale – to grow and accommodate the needs of accredited participants and relying parties
- 3 ➤ Promote flexibility and innovation in technology and business models

There is a host of technologies based on Machine Learning and Artificial Intelligence to address these challenges. At IDEMIA, we make it our mission to help governments and private organizations understand how **these technologies** can contribute to a better future with the common objective to achieve financial and digital inclusion for billions of people worldwide.

***AFI Group** is the world’s leading organization on financial inclusion policy and regulation. A member-owned network, AFI promote and develop evidence-based policy solutions that improve the lives of the poor through the power of financial inclusion. More information: <https://www.afi-global.org/>
