

MSC Policy brief #24

# KYC practices in Indonesia and the opportunity for implementing e-KYC to accelerate financial inclusion

Agnes Salyanty, Arshi Aadil,  
Rahmatika Febrianti,  
Raunak Kapoor, and  
Sneha Sampath



## Introduction and background

In response to the COVID-19 pandemic, the Government of India provided emergency digital cash transfers to more than 300 million people within a month by utilizing the payment system backed by *Aadhaar*, the foundational digital ID in the country. This included a total transfer of USD 3.8 billion (INR 280 billion) to farmers, senior citizens, and women who were identified quickly as they were beneficiaries of social protection programs. The digital payment infrastructure built around Aadhaar provides an interoperable, cost-effective, quick, and secure payment solution using the digital ID to verify beneficiaries and authenticate transactions and withdrawals.

Countries have built robust architecture around foundational identity systems that enable different stakeholders to access the identity database and develop services. For financial sector players alone, access to a digital-ID-backed authentication and verification service allows seamless customer identity verification, onboarding, and authentication of transactions.

Public infrastructure for electronic Know Your Customer (e-KYC) has been critical to financial inclusion initiatives in many developing countries. E-KYC provides multiple benefits over traditional paper-based KYC. It enables efficiency gains in terms of time, cost, and resource requirements involved in the verification of the identity of an individual or entity. This ensures a near real-time onboarding of a customer for any financial product or service. Since an efficient KYC process is one of the most important and costly aspects of any customer due diligence, making it easy and cost-effective is the priority of financial services providers. In addition, inefficiencies in the customer onboarding process can have a significant impact on the trust of a potential customer in the financial service provider and consequently on the adoption and uptake of its products and services.

**Provided below are some examples from across the globe that highlight how the transition from traditional KYC to e-KYC reduces the time and cost involved in onboarding customers.**



### India

The adoption of e-KYC in India decreased the cost of customer verification from USD 15 to USD 0.50 and the time spent from five days to a few seconds. More than 8.04 billion e-KYC transactions have been conducted in India so far. Providers like banks and mobile network operators are projected to save USD 1.3 billion in KYC-related administrative costs by 2021.



### United Kingdom

Reports estimate that a digital identity infrastructure could help the country save USD 13.2 billion. This would include direct savings of up to USD 2 billion through improvement in the current inefficient KYC processes and up to USD 11.3 billion in savings on identity fraud.



### Estonia

Smart-ID in Estonia enables the secure online delivery of 99% of public services. This digital identity system enables Estonians to complete KYC checks much faster, vote online, pay taxes digitally, and buy cryptocurrencies, among others. The government estimates that its e-Estonia systems contribute around 2% of the GDP per year in savings.

More than 98% of the adult population of Indonesia already has a Kartu Tanda Penduduk (e-KTP), the Indonesian identity card. The Ministry of Home Affairs maintains a secure database with the digital identities of citizens, which includes their biometrics. By the end of 2020, around 2,819 government and private institutions, including 1,177 banks, had access to demographic data of citizens from this database. These stakeholders range from banks to FinTechs and hospitals to educational institutions. These institutions are granted access through an MoU signed with Dukcapil for the “right to access.” This gives a stakeholder the right to view the demographic details of the citizens under the terms of the MoU. Dukcapil has also granted licenses to two private entities, together known as the Platform Bersama or “our platform,” to act as intermediaries for providing B2B solutions to the industry. While these positive developments have eased some of the challenges around KYC, access to the biometric database of citizens remains restricted. Certain selected use-cases related to law enforcement agencies are the exception to this, such as access to the data for the police department and the immigration office.

In the past few years, Dewan Nasional Keuangan Inklusif (DNKI), in collaboration with various partners including government departments and private institutions like banks and consulting firms, has been championing efforts to inform policies for the implementation of robust national identity infrastructure. This will facilitate the inclusive delivery of financial services and help Indonesia achieve its vision of providing access to bank accounts to 90% of its adult population by 2024.

An enabling infrastructure and policy framework on e-KYC would help the country achieve its vision of financial inclusion. This policy brief is based on a study conducted by MicroSave Consulting (MSC) in collaboration with DNKI to assess the existing KYC processes **banks and**

**FinTechs** have adopted in Indonesia. The study provides insights into the challenges, costs, and time taken by service providers to conduct the KYC process. It further provides actionable policy recommendations to promote a public infrastructure for e-KYC to accelerate digital inclusion. The detailed report is available [here](#).

## Regulatory landscape for KYC for banks and FinTechs

Several laws and governing bodies regulate the KYC process for the financial services industry in Indonesia. Depending on the type of product and service and the level of risk involved, the requirements and levels of assurance vary when it comes to the verification process for customers. Law No. 8 (2010) on the Prevention of Crime and Money Laundering requires financial service providers to implement a KYC process and report to the Indonesian Financial Transaction Reports and Analysis Centre (PPATK) regarding any suspicious transaction

The Anti-Money Laundering/Combating the Financing of Terrorism (AML-CTF) regulations of Otoritas Jasa Keuangan<sup>1</sup> for banks and peer-to-peer (P2P) lenders and Bank Indonesia<sup>2</sup> for e-money players define the overall framework within which the service providers can design their KYC processes. They lay down the rules for customer due diligence for different types of accounts and risk profiles, which include options for using electronic verification of customer identity. In addition, government regulation as stated in Permandagri No. 102 provides an overarching framework for access to and use of national citizenship data. The table below provides a snapshot of the existing regulatory framework for KYC and its implications for different categories of service providers.

1 OJK: Financial Services Authority of Indonesia is a government agency in Indonesia that regulates and supervises the financial services sector.

2 BI: Central bank of the Republic of Indonesia

Service providers (financial instrument)	Regulations on AML-CTF in the financial sector	Laws on citizenship database and access	Presidential Regulation on Social Assistance	Draft law on Personal Data Protection
Bank (Basic savings account)	<u>POJK No. 23 /POJK.01/2019</u> <sup>3</sup> defines the rules for the implementation of AML CFT in the financial service sector. It comprises rules on tiered customer due diligence (simplified CDD <sup>4</sup> , basic CDD, and enhanced DD), as well as both face-to-face and non-face-to-face verification. The later verification can be done by using at least two-factor authentication (what you are/have/know). (Article 17)	<u>The Population Administration Law No. 24 Year 2013</u> states that the biometric data held in the NIK <sup>5</sup> (SIAK) database needs protection. However, it does not provide details on the treatment of “protected data.” (Article 54)  <u>Permendagri No.102 Year 2019</u> states that:  1. Legal entities can only access the Dukcapil database and receive a yes or no response after matching for verification. The types of database include NIK, family card number, biometrics (fingerprint, iris, photo), and a combination of the population data elements. (Article 29)  2. MoHA offers three methods to access data: Using a card reader, through a web service, and through a web portal. (Article 21)  3. Access to the Dukcapil database is limited to the MoHA staff and users (including business entities) who have the mandate under an MoU. Users need to establish an SOP on the technical implementation of data access (Article 13)  4. Violation of the access right may result in revoked access for the user or deactivation of the card reader, disconnection of the network, and termination of the MoU. (Article 45)  <u>PP 40 Year 2019</u> states that MoHA has the right to obtain reciprocal data from the granted users. (Article 10)		<u>The draft law</u> bestows several rights to financial service users regarding personal data with some exceptions.  The users have the following rights:  1. Right to delete and destroy personal data as well withdraw consent to the processing of data;  2. Right to choose or not to choose the processing personal data through a pseudonymous mechanism for specific purposes;  3. Right to delay or limit the processing of data;  4. Right to use and transmit data.
G2P <sup>6</sup> – Himbara Banks (Delivery of social assistance)	<u>POJK 23/2019</u> relaxes the identification and verification requirement for government-related institutions. On the other hand, low-risk customer profiles, such as G2P beneficiaries can open accounts by utilizing simplified CDD. (explanation of <u>POJK No. 12 /POJK.01/2017</u> , page 3)		<u>Perpres 63 Year 2017</u> states that:  1. Bank partners shall conduct G2P account registration and opening based on the DTKS database. This account must be used to receive benefits under other social assistance programs. (Article 6)  2. To ensure interoperability and interconnectivity, the payment services should be owned, managed, or both, by state-owned commercial banks. (Article 11)  3. All costs associated with the implementation of the non-cash social assistance distribution are covered by the government budget. (Article 18)	
e-money players	<u>PBI No.19/10/PBI/2017</u> on the implementation of AML CFT for the non-bank payment service provider allows for both face-to-face and non-face-to-face verification. It provides details on the procedure for non-bank payment providers to conduct a simplified CDD. (Article 29) Service providers may utilize biometric or electronic data only if they can ensure the validity and reliability of the data. (Article 20)			
P2P lenders	<u>POJK 77/POJK.01/2016</u> comprises rules for P2P players to implement AML-CFT policy as mandated in <u>POJK No. 23 /POJK.01/2019</u> . (Article 42)			

Note: The laws and regulations that are applicable to all service providers are highlighted in grey.

<sup>3</sup> POJK No.23/2019 is an amendment to the regulation of the financial service authority No. 12/POJK.01/2017.

<sup>4</sup> Customer due diligence

<sup>5</sup> Nomor Induk Kependudukan – National identity number

<sup>6</sup> Government-to-person: Includes transfers in cash and kind under social assistance programs

## Existing KYC practices in Indonesia

In Indonesia, service providers adopt different models to conduct KYC for their customers. These practices are summarized in the table below.

	KYC process operational model	Service providers	Summary	Estimated time required to complete the account opening or registration process
01	Conventional branch-based model	Commercial banks	Walk into the service provider outlet, face-to-face interaction with service provider staff, physical checking of documentation	1–2 days
02	Agent-assisted model	Commercial banks with agent networks	Walk to an agent of the service provider, documentation at agent point, documents transported to a branch of the service provider, document checked by the service provider staff	3–14 days
03	G2P model	Himbara banks	Relevant government ministry shares the beneficiary list with the banks for account opening. The banks connect to the Dukcapil database (web access) to verify the identity of the beneficiaries. The accounts are opened in a centralized manner while the passbook, PIN, or card is distributed in the field through face-to-face interaction between the bank staff and beneficiaries	Typical service-level agreement is 60 days from the time of receiving the data to handing over the KKS cards to the beneficiaries
04	Mobile service provider staff model	Commercial banks	Service provider staff opens the bank account (mobile) using a biometric device attached to a tablet. The device can read data from the chip on the e-KTP card and match customer fingerprints with biometrics stored on the card	Sign up is instant but account activation may take 1-3 days
05	Remote KYC using the service provider mobile app	FinTechs (e-money issuers, P2P lenders)	Account opened remotely on a mobile app by uploading a selfie with a photo of the e-KTP	1-3 days

## Challenges involved in the KYC process

While most service providers have made efforts to digitize the KYC process, the lack of public infrastructure for identity verification has forced many providers to adopt sub-optimal processes to verify the identity of their customers. The major challenges for service providers are as follows:

### 1. Limited data for verification:

Service providers are dependent on the data that customers submit directly, such as basic details, a photograph of their KTP cards, and selfies. Currently, verification is done only against the NIK number that the customer provides. While some service providers, which have signed an MoU with Dukcapil, have web access (demographic) to the national ID database, the process itself involves a lot of manual eye-balling for verification. This is time-consuming and prone to human errors. Some providers have tried to automate a part of this process while others have simply outsourced the verification to a third party. Service providers do not have digital access to the databases of other permissible IDs like a passport and driver's license.

### 2. Risk of manipulation and errors:

MSC's in-depth interviews with service providers reveal that approximately 30-60% of the total customer applications are rejected because of blurry selfies of customers or images of their KTP cards. This is largely due to the poor quality of the camera or faulty capturing of photos by customers. Therefore, it becomes necessary for the staff to double-check the images of a customer's KTP card manually to ensure that it has not been tampered with. This increases both the time and cost of KYC verification.

### 3. Increased operational costs due to manual processes and dependence on third parties for data verification and exception handling:

KYC verifications through third parties significantly increase the verification costs for service providers. Moreover, manual and additional verification processes to deal with exceptions, such as video calls or physical checks further increase staff costs and the time taken in the process.

### 4. Ability to compete:

Many institutions still do not have an MoU with Dukcapil to access citizenship data. They have to rely on either third parties or conduct resource-intensive manual processes. For institutions that do have access, the levels of access are not always uniform. For example, some institutions may have access to photos while others may only have access to demographic data. This lack of standardization in terms of the level of access restricts many industry players from competing on fair and equal terms.



The table below provides a snapshot of key challenges that different categories of service providers face during the KYC process for opening or registration of accounts.

	KYC process operational model	Service providers	Challenges
01	Conventional branch-based model	Commercial banks	High operational costs due to manual verification processes
02	Agent-assisted model	Commercial banks with agent networks	<ul style="list-style-type: none"> <li>High cost of agent acquisition, especially in areas without physical branches</li> <li>Time-consuming process</li> </ul>
03	Centralized account opening in G2P initiatives	Commercial banks	<ul style="list-style-type: none"> <li>Incomplete or missing data</li> <li>Limited quota for verification</li> <li>Daily limit restrictions on bulk account opening</li> <li>High operational costs due to resource-intensive manual processes like socialization of beneficiaries and disbursement of kits</li> <li>Time-consuming process</li> </ul>
04	Mobile service provider staff model	Commercial banks	<ul style="list-style-type: none"> <li>Cost of devices like mobiles, laptops, etc.</li> <li>High staff costs</li> </ul>
05	Remote KYC using the service provider mobile app	FinTechs (e-money issuers, P2P lenders)	<ul style="list-style-type: none"> <li>Blurry pictures (Selfie and e-KTP)</li> <li>Absence of a single source of truth to verify customer identity</li> <li>Dependence on third parties for data verification and exception handling</li> <li>Risk of manipulation of the e-KTP card</li> </ul>



## Current costs involved in the KYC process

The cost of conducting KYC varies significantly across service providers and depends largely on regulatory requirements that service providers are subject to, as well as the service provider's level of automation of the KYC process. However, in the absence of a low-cost public infrastructure for digital verification of the identity of the customer, most service providers spend significant resources in conducting the entire due diligence process for a new customer. The table below highlights the costs involved in various stages of customer onboarding by different service providers.

Service provider	Stages of onboarding			Total IDR k (USD)	Comments
	Acquisition	Verification of identity	Activation of account and storage of data		
<b>e-Money</b>					
<b>Customer</b>	0	1.6-16	0	1.6-16k (0.11 - 1.1 USD)	The high cost of verification is largely due to third-party verification
<b>Merchant</b>	0-80	3-32	1.5-3	4.5-115k (0.3-7.9 USD)	The costs of acquisition vary depending on the type of onboarding—self-initiated or through third-party agents with on-ground acquisition teams. The range indicates the difference in verification costs involved in-house automated verification and outsourced verification.
<b>P2P</b>					
<b>Lender</b>	0	59-76	0	59-76k (4-5.2 USD)	Verification costs also include enhanced due diligence and digital signature verification completed through outsourced third parties.
<b>Borrower</b>	0	8-21	0-4.5	8-26k (0.5 - 1.7 USD)	Verification costs include outsourced third party verification who complete the process manually.
<b>Banks</b>					
<b>G2P beneficiary</b>	0	0.4	23.6-63	24-63.4k (1.6 - 4.3 USD)	Activation includes the socialization process, which involves face-to-face verification and the distribution of the bank passbook, card, and PIN.
<b>Basic savings account</b>	7.2	6.2	0.5-21.8	13.8-35k (0.9 - 2.4 USD)	Verification is completed face-to-face. The activation costs include the cost of printing cards, which varies depending on the type of card.
<b>Agent</b>	1.6	6.1	166-211	170-215k (11.7 - 14.8 USD)	Activation costs include costs for the training and marketing material given to agents.

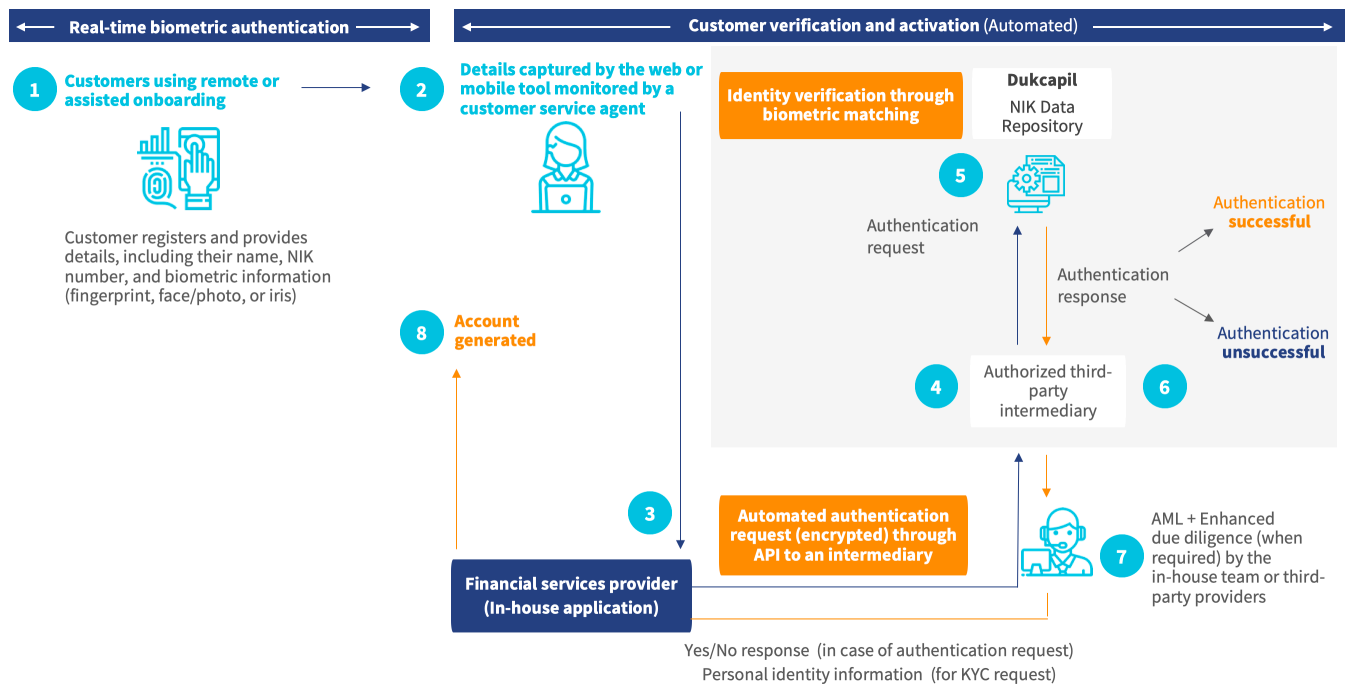


# The implementation of electronic KYC in Indonesia and its potential impact on cost savings for the industry

A low-cost digital infrastructure to verify the identity of an individual is essential to accelerate financial inclusion and meet the requirements of a booming digital economy. An ideal process for KYC verification should have the following key features:

- Real-time secure access to the Nomor Induk Kependudukan (NIK) or the national identity number database for the verification of individual identity;
- Multi-modal biometric authentication options, such as fingerprint, iris, face recognition, among others, to suit the requirements of different types of service providers;
- A tiered technology infrastructure that allows for an intermediary (authorized service agencies) to act as a bridge between user agencies and Dukcapil. This will ensure the scalability of digital identity services and help Dukcapil focus its supervision efforts on a few authorized entities rather than the entire ecosystem of users;
- A data processing protocol that adheres to all compliances around data protection as stated under the relevant law.

The figure below illustrates the proposed KYC process.



Our analysis shows that the implementation of e-KYC could **save the FinTech sector approximately USD 3.9-4.2 billion (IDR 57-61 trillion) and the banking sector close to USD 160-212 million (IDR 2,357-3,123 billion) in the next 10 years**. These figures are calculated based on the savings from the verification process, assuming that the cost per verification would fall

in the range of IDR 4,000–7,000 (USD 0.28–0.47), in line with the industry's willingness to pay for verification. The calculations also assume around 50% savings through a reduction in the administrative processes<sup>7</sup> during onboarding. Besides the onboarding use-case for customers, it is also possible to realize additional savings in e-authentication processes in G2P delivery.

<sup>7</sup> <https://www.finextra.com/blogposting/18559/6-reasons-to-connect-to-e-kyc-utilities>

## Recommendations for policymakers

Over the last few years, digitization in the delivery of financial services has witnessed massive growth. Incumbents, such as large commercial banks, insurance companies and capital market players, and the rapidly growing FinTech sector, have equally embraced these efforts. The efforts of the government to accelerate digital financial inclusion has also forced service providers to innovate with their solutions. While efforts are underway to develop the next generation of infrastructure for micro-payments, it is equally important that the Government of Indonesia takes concerted measures to build a robust infrastructure for digital identity verification, which is key to the adoption of most digital services.

Given below is a list of policy recommendations to accelerate the adoption of e-KYC in Indonesia.

### 1. Invest resources to develop a robust e-KYC infrastructure as a public good

Indonesia has a fairly robust national ID database with nearly universal coverage. However, the country needs to invest resources to enhance the infrastructure and thus the capabilities of its national ID database to facilitate digital identity and e-KYC transactions at scale. This would require investment in cost-effective and device-agnostic authentication infrastructure to enable biometric matching. Such an infrastructure should ensure enhanced network or cybersecurity systems and reliable application programming interfaces (APIs) for Proof of Identity (PoI) or Proof of Address (PoA) services to facilitate third-party access. These enhancements require significant investments and may need specific budgetary allocations. The proposed investments have a long-term horizon and countries that have made such investments, such as India, Nigeria, Pakistan, and Singapore, have witnessed significant cost savings in both public and private sector domains.

### 2. Define the rules of engagement for the private sector

As stated earlier, many agencies currently access limited verification services from the Dukcapil. These include both user agencies as well as licensed intermediaries. However, to meet the requirements of a wide range of actors in the Indonesian digital economic landscape, digital identity and e-KYC services must not be subject to the discretionary powers of one or two government agencies. The government should make these services available to private players. The definition of a standardized set of rules of engagement that foster a robust rules-based ecosystem can help achieve this goal. The private sector and any entity, either in the capacity of a user agent or as an intermediary, that meets those requirements should be free to utilize the verification services available on the national ID infrastructure of the country. This will also encourage fair competition among various actors in the digital economy.

The Government of Indonesia should publish a standardized list of requirements for different levels of verification services, such as authentication and e-KYC, among others. This will enable industry players to choose from the setlist based on their requirements and help them prepare their internal systems accordingly. The government should also utilize open APIs to enable developers and service providers to connect securely and seamlessly to the national ID database. This will encourage stakeholders to develop innovative solutions around verification services for personal applications, offer such solutions to other players in the industry, or both. Lastly, the government may need to define standards and certify hardware devices as well as the software required to enable verification that may include biometric devices, such as fingerprint scanners, iris scanners, face recognition software, biometric match standards, encryption protocols, etc.

### 3. Pricing of solutions to encourage adoption





Despite significant investments in the development of a digital identity architecture, countries around the world have adopted different strategies to price digital identity services. Some countries consider it a public good and provide free access to such services. Whereas, other countries adhere to a hybrid approach where access is free for public institutions while the private sector is charged nominal amounts for such services. The levied charges provide a consistent source of revenue to maintain and upgrade the infrastructure. The table below highlights the pricing protocols in some countries that have implemented a digital identity infrastructure. (Source: [ID4D, World Bank](#))

Policymakers in Indonesia can take a call on the pricing strategy they want to adopt. The results from the report can also act as a reference for the willingness of the stakeholders to pay for

these services. The government can develop a tiered cost structure to enable different levels of access. Based on the findings of the study and an analysis of the willingness to pay by various stakeholders, the tentative costs per request are as follows:

- **Authentication service:** A simple yes or no response to whether a match is found in the NIK database: IDR 400-800 (USD 0.03-0.05) per query
- **E-KYC:** Confirmation of a match as well as access to view the demographic data and credentials for verification: IDR 4,000-7,000 (USD 0.28–0.47)

This is an estimation of the cost. The actual charges and the real cost will differ based on government decisions during the rollout. The government should consider this facility as a “public good” and levy charges or fees accordingly.

Country	Population (in million)	Model of pricing	Pricing of verification and identity services
<b>India</b> 	1,339	Free for the public sector and nominal charges for the private sector	<ul style="list-style-type: none"> <li>• Public sector: Free</li> <li>• Private sector: USD 0.007 for Aadhaar authentication with a yes or no response, and USD 0.3 for e-KYC transactions</li> </ul>
<b>Malaysia</b> 	31	Nominal charges for both the public and private sectors	<ul style="list-style-type: none"> <li>• USD 0.13 to verify a demographic record</li> <li>• USD 0.25 to verify a demographic and biometric record</li> </ul>
<b>Pakistan</b> 	193	Nominal charges for both the public and private sectors	<ul style="list-style-type: none"> <li>• Public sector: USD 0.09 per query</li> <li>• Private sector: USD 0.29 per query</li> </ul>
<b>Thailand</b> 	69	Free for both the public and private sectors	<ul style="list-style-type: none"> <li>• Free verification: Number of a demographic record and the national ID card</li> </ul>

#### 4. Ensure the protection of customer data as per the defined policy framework

Indonesia needs to speed up the establishment of the personal data protection law to ensure that proposed verification services strictly adhere to the mandated data protection protocols of the country. The data protection requirements would serve as a guiding principle to standardize all requirements for private and public sector engagements on digital identity services. This would mitigate risks related to the abuse of personal data and, hence, increase the confidence of policymakers and consumers in these services. The implementation of data protection protocols could also enable open banking services, as users will have the right to share or protect personal data while accessing a range of digital financial services at their disposal. This will encourage competition and provide more choices to the end consumers.



#### 5. Readiness of service providers to implement e-KYC

While the government needs to ensure a robust public infrastructure on digital identity, service providers should also equip themselves to access the proposed verification services and meet the mandated technical requirements. This would require them to invest in both software and hardware capabilities, as well as human resources that have adequate technical skills to monitor and supervise the integration

and maintenance of such systems at the service provider level. Service providers also need to reassess their existing network or cybersecurity systems as well as data protection protocols to meet the required standards and protocols mandated by relevant policymakers.



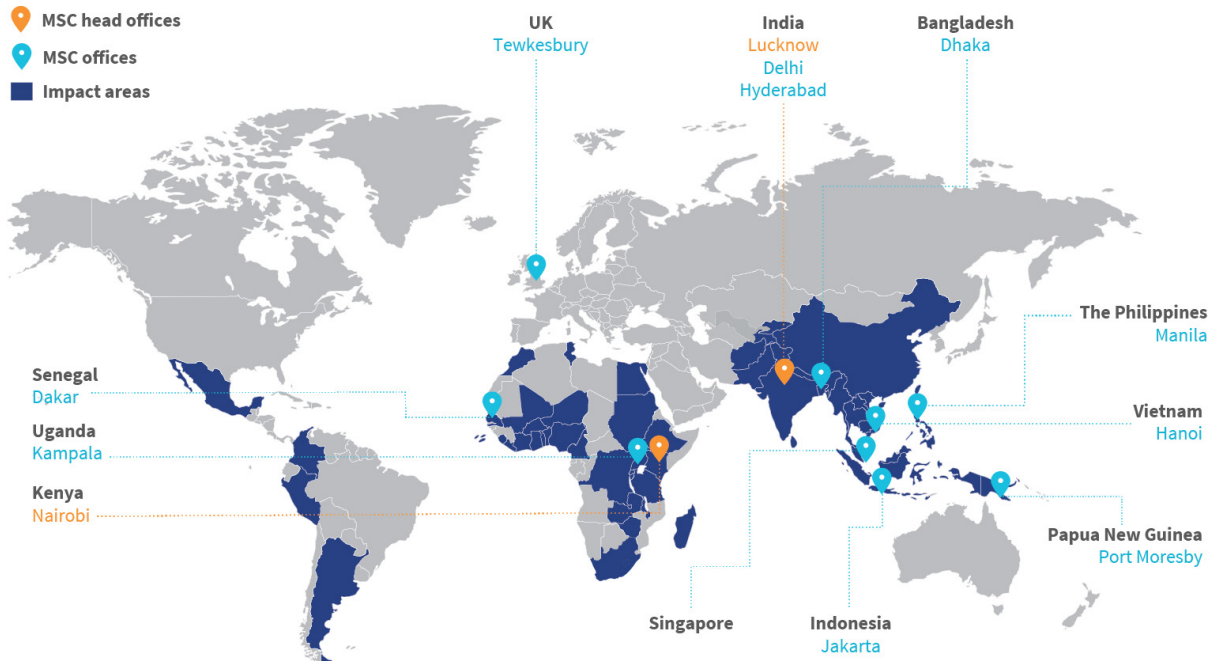
## Conclusion

With over 170 million internet users, Indonesia has one of the largest online population bases. More than 3,000 financial service providers operate in the country and a large majority of these have been making significant efforts to digitize the delivery of financial services to serve the needs of a growing digital economy. Digital identity services have the potential to catalyze digital economy initiatives by making it easier for people to participate, join, and use the digital environment in a frictionless manner. Digital identity solutions can help service providers penetrate deeper and serve unserved and underserved segments cost-effectively.

Like most countries that have successfully implemented their digital identity initiatives, Indonesia also needs to undertake a strategic long-term project that encourages the development of public infrastructure for e-KYC and digital identity by utilizing the national ID database. Such an initiative needs to be viewed as an ecosystem of innovation, and not merely as an activity that is currently being spearheaded by one or two policy-makers. The government should establish an Inter-Ministerial Working Committee (IMWC) led by a cross-cutting policy-making authority to foster wide-ranging consultations to discuss the use-cases of national digital identity and e-KYC. This will allow Indonesia to build a strong foundation for digital financial inclusion and hence catapult its developing economy to a higher level. In addition to savings and efficiency gains in the financial sector, the proposed architecture and services around the NIK database can disrupt several other sectors in Indonesia and can act as an enabler of economic, social, and political activity in the digital age. The wide variety of use-cases and interactions between stakeholders could utilize a robust digital ID platform to create value and contribute to savings.

The opportunities for e-KYC in Indonesia are endless. The large social protection system of the country could utilize this system to authenticate beneficiaries, eliminate ghost and duplicate beneficiaries, and reduce frauds, which would lead to significant cost savings. The Government of India estimates that it has already saved USD 19.25 billion until March, 2019. Other G2P services can also benefit from the time and efficiency gains. e-KYC also offers other economic benefits for individuals and institutions, such as increased use of financial services by decreasing onboarding costs as well as remote onboarding and improved service delivery. It can improve access to employment and efficiencies in the labor market through digital talent matching and contracting platforms enabled and secured by a digital ID for the informal labor force. Another significant benefit is increased agricultural productivity through formalized landownership, which would enable more investments into farming and better agriculture output. A digital ID can help deliver these benefits to build the economy of Indonesia, and ensure greater inclusion, formalization, and digitization.





## Asia head office

28/35, Ground Floor, Princeton Business Park, 16 Ashok Marg,  
Lucknow, Uttar Pradesh, India 226001

Tel : +91-522-228-8783 | Fax : +91-522-406-3773

Email : [manoj@microsave.net](mailto:manoj@microsave.net)

## Africa head office

Shelter Afrique House, Mamlaka Road, P.O. Box 76436,  
Yaya 00508, Nairobi, Kenya

Tel : +25-420-272-4801 | Fax : +25-420-272-0133

Email : [anup@microsave.net](mailto:anup@microsave.net)

[www.microsave.net](http://www.microsave.net)