Existing KYC practices in Indonesia and opportunities for implementing e-KYC to accelerate financial inclusion

December, 2020

Disclaimer: This report is based on interviews with a selected number of service providers. Efforts have been made to present the most representative KYC process for different categories of service providers in the market. However, there may be slight variations in actual processes adopted by an individual service provider. The processes mentioned in this report should therefore not be taken to be accurate for every individual service provider.
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>01 Executive summary</td>
<td>4</td>
</tr>
<tr>
<td>02 Background and scope of the study</td>
<td>7</td>
</tr>
<tr>
<td>03 Recommendations for implementing digital identity and e-KYC services in Indonesia</td>
<td>12</td>
</tr>
<tr>
<td>04 Regulatory landscape for KYC in Indonesia</td>
<td>18</td>
</tr>
<tr>
<td>05 Details of existing KYC practices of financial service providers in Indonesia</td>
<td>21</td>
</tr>
<tr>
<td>06 Challenges in the existing KYC processes</td>
<td>37</td>
</tr>
<tr>
<td>07 Costing of the existing KYC processes</td>
<td>40</td>
</tr>
<tr>
<td>08 Strategic considerations for implementing e-KYC</td>
<td>48</td>
</tr>
<tr>
<td>09 Annexes</td>
<td>50</td>
</tr>
</tbody>
</table>
## Abbreviations

<table>
<thead>
<tr>
<th>Sl. no</th>
<th>Abbreviations</th>
<th>Full form</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>AML</td>
<td>Anti-money laundering</td>
</tr>
<tr>
<td>2</td>
<td>API</td>
<td>Application programming interface</td>
</tr>
<tr>
<td>3</td>
<td>BSA</td>
<td>Basic savings account</td>
</tr>
<tr>
<td>4</td>
<td>CDD</td>
<td>Customer due diligence</td>
</tr>
<tr>
<td>5</td>
<td>CFT</td>
<td>Combating the financing of terrorism</td>
</tr>
<tr>
<td>6</td>
<td>DNKI</td>
<td>Secretariat of the National Council for Inclusive Finance</td>
</tr>
<tr>
<td>7</td>
<td>Dukcapil</td>
<td>Directorate of Population and Civil Registration (Dukcapil) of the Ministry of Home Affairs</td>
</tr>
<tr>
<td>8</td>
<td>EDC</td>
<td>Electronic data capture</td>
</tr>
<tr>
<td>9</td>
<td>EDD</td>
<td>Enhanced due diligence</td>
</tr>
<tr>
<td>10</td>
<td>FSP</td>
<td>Financial service provider</td>
</tr>
<tr>
<td>11</td>
<td>G2P</td>
<td>Government to person</td>
</tr>
<tr>
<td>12</td>
<td>IDR</td>
<td>Indonesian Rupiah</td>
</tr>
<tr>
<td>13</td>
<td>IDR</td>
<td>Indonesian rupiah</td>
</tr>
<tr>
<td>14</td>
<td>KKS</td>
<td>Kartu Keluarga Sejahtera, Family welfare card</td>
</tr>
<tr>
<td>15</td>
<td>MoHA</td>
<td>Ministry of Home Affairs</td>
</tr>
<tr>
<td>16</td>
<td>NIK</td>
<td>Nomor Induk Kependudukan (personal identity number)</td>
</tr>
<tr>
<td>17</td>
<td>OTP</td>
<td>One time password</td>
</tr>
<tr>
<td>18</td>
<td>P2P</td>
<td>Person to person</td>
</tr>
<tr>
<td>19</td>
<td>PTEN</td>
<td>Penyelesaian Transaksi Elektronik Nasional (The National Electronic Transaction Settlement)</td>
</tr>
<tr>
<td>20</td>
<td>QRIS</td>
<td>Quick Response Indonesia Standard</td>
</tr>
<tr>
<td>21</td>
<td>SNKI</td>
<td>National Financial Inclusion Strategy</td>
</tr>
</tbody>
</table>
Executive summary (1/2)

Study rationale

• International experience has shown that a public infrastructure for enabling electronic KYC (e-KYC) is critical in accelerating financial inclusion. E-KYC provides multiple benefits over traditional paper-based KYC. It enables efficiency gains in terms of time, cost and resource requirements involved in verifying the identity of an individual/entity and thereby ensuring a near real-time on boarding of customers.

• Government of Indonesia (GoI) has set itself a vision of providing bank account access to 90% of the adult population by 2024.

• In the last few years, Dewan Nasional Keuangan Inklusif (DNKI), in collaboration with relevant partners, has been championing the efforts around informing policies for implementation of a robust digital identity infrastructure in Indonesia for inclusive delivery of financial services.

• This study provides insights into the existing KYC practices of financial service providers (banks, e-money players and P2P lenders) including challenges and costs involved in KYC process. The study also provides policy recommendation to accelerate e-KYC implementation in Indonesia.

Findings from the study

<table>
<thead>
<tr>
<th>E-money players</th>
<th>P2P lenders</th>
<th>Banks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Customers onboard themselves by self registering themselves on the provider application. Small merchants onboarding is outsourced to third party vendors who are responsible for conducting KYC</td>
<td>Customers initiate onboarding themselves by self registering on provider applications and the verification process is outsourced to third party vendors</td>
<td>BSA customers are on boarded through either a centralized account opening process (G2P) or through agents/branches. Many banks have web access to Dukcapil database for identity verification</td>
</tr>
</tbody>
</table>

The cost for the customer onboarding process can be up to IDR 16,000-115,000 (USD 1.1-7.8) for customers and merchants. The process can take up to **one to two days** to complete for a customer on the platform and between **three to ten days** for merchants.

The cost for the onboarding lenders and borrowers can be up to IDR 26,000-76,000 (USD 1.8-5.2). The process can take **just a day for lenders** but **up to three days** to complete for borrowers on the platform.

The cost for opening BSA through an agent ranges between IDR 13,800-35,000 (USD 0.94-2.4) and may take up to **two weeks**.
### Challenges observed in the current customer onboarding processes followed by service providers

<table>
<thead>
<tr>
<th>E-money players</th>
<th>P2P platforms</th>
<th>Banks</th>
</tr>
</thead>
<tbody>
<tr>
<td>• The major challenge for FinTechs is their dependence on direct data input by customers and the lack of a single source of truth to instantly verify the identity of an applicant or prospective customer.</td>
<td>• This leaves room for manipulation, duplication, and poor quality of data/images.</td>
<td>• Banks mandated for G2P disbursements incur significant costs in printing and distributing KKS cards.</td>
</tr>
<tr>
<td>• This leaves room for manipulation, duplication, and poor quality of data/images.</td>
<td>• To address these issues, FinTechs had to adopt additional processes and exception handling techniques that increase operational costs.</td>
<td>• In the absence of real-time verification of customer identity, BSA account opening through banking agents is a largely manual and time consuming.</td>
</tr>
</tbody>
</table>

### Key policy recommendations

In order to accelerate financial inclusion and support requirements of a booming digital economy, a low-cost digital infrastructure to verify identity of an individual is a necessity. An ideal process for KYC verification should be real time, offer multi modal authentication options and should adhere to all compliances and data protection laws and practices. In order to accelerate digital financial inclusion, GoI should:

1. Invest resources to augment infrastructure of its national ID database in order to facilitate digital identity and e-KYC transactions at scale
2. Define rules of engagement for private sector players to create a more robust rule based ecosystem for digital identity
3. Provide affordable pricing for digital identity services that encourages adoption and usage of such services by a wide range of digital financial service providers
4. 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
Background and scope of the study
International experience has shown that a public infrastructure for enabling electronic KYC (e-KYC) is critical in accelerating financial inclusion

- Indonesia has good progress on financial inclusion over the last few years. SNKI-FII data found that account ownership stood at 55.7% in 2018.

- Government of Indonesia (GoI) has set itself a vision of providing bank account access to 90% of the adult population by 2024.

- Given a difficult geographical landscape, implementation of e-KYC would be critical for Indonesia to achieve its financial inclusion goals

**Enabling factors for electronic KYC and digital identity services**

- >95% of the eligible population has e-KTP cards
- Initial pilots highlight feasibility of digital identity and e-KYC solution for financial inclusion
- A booming digital economy and fintech sector

**e-KYC provides multiple benefits over traditional paper-based KYC**

- Offers efficiency gains in terms of the time and cost
- Ensures negligible human interference
- Mitigates the risk of document forgery
- Eliminates paper-based documentation
- Allows consent-based service
This study examines the existing practices of KYC in Indonesia including challenges in identification and verification of customers. The study also scopes opportunities for leveraging the national ID database for implementation of e-KYC in Indonesia

**Study focus**

- **Current practice** of KYC for various service providers
- **Current cost** of KYC processes for the service providers

Through this detailed analysis, the study provides actionable insights to both policymakers as well as service providers to promote the adoption of e-KYC in Indonesia. Specifically, the objective of the study is to provide the following insights:

**For policymakers**

- Comprehensive understanding (challenges, cost and time) of the existing KYC and customer onboarding practices adopted by banks and FinTechs
- Insights for benchmarking the pricing of authentication and e-KYC solutions in Indonesia
- Analysis of potential economic savings for the government on implementing digital identity and e-KYC services

**For service providers**

- Insights on inherent risks and inefficiencies in the existing KYC and customer onboarding processes
- Insights on existing industry practices on KYC including innovations and exception handling
- Insights on the feasibility of implementing an e-KYC solution at an institutional level

The scope of this study extends to the KYC processes followed for a range of financial service products offered by banks, e-money providers, and P2P players.

However, given the fact that the study pivots around digital financial inclusion opportunities, the scope is limited to mass market product offerings of financial service providers.

<table>
<thead>
<tr>
<th>E-money players</th>
<th>P2P lending platform</th>
<th>Banks</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Customers</strong></td>
<td><strong>Borrowers</strong></td>
<td><strong>Customers</strong></td>
</tr>
<tr>
<td>Process and cost for signing up customers for a registered e-money account</td>
<td>Process and cost for onboarding individual borrowers on the platform</td>
<td>Process and cost for opening a basic savings account, including under G2P programs, such as PKH</td>
</tr>
<tr>
<td><strong>Small merchants</strong></td>
<td><strong>Lenders</strong></td>
<td><strong>Agents</strong></td>
</tr>
<tr>
<td>Process and cost for onboarding a QRIS merchant</td>
<td>Process and cost for onboarding individual retail lenders on the platform</td>
<td>Process and cost for onboarding BSA customers through Laku Pandai agents and bank branches</td>
</tr>
</tbody>
</table>
The main aspects captured were the activities, costs, and time taken to complete each of the key stages of customer onboarding process by financial service providers.

### Customer onboarding process stages

**Acquisition**
- Finding potential customers, handling of customer queries, filling of the form, and the collection or uploading of KYC documents

**Verification**
- Digitization of data or the registration form, verification of KYC data and documents, checking of the customer’s background, and business verifications

**Activation**
- Activation of account as well as the verification and linking of bank accounts

**Storage**
- Storage of customer data

### Direct cost (IDR)
- Staff cost
- Administrative cost
- Third-party cost

### Time taken
- To complete the process
- Lag between each activity

### Staff and teams involved
- Productivity in terms of the applications processed in a day
- Internal teams involved

### Challenges
- Issues in verification and identification of new customers

After completion of a thorough assessment of the existing practices, we arrived at policy recommendations for implementing e-KYC and digital identity services in Indonesia.
Recommendations for implementing digital identity and e-KYC services in Indonesia
A robust technical architecture that provides digital identity and e-KYC services at scale is critical for supporting the needs of a booming digital economy.

For the efficient adoption of e-KYC in Indonesia, all identity verification requests should be routed through the NIK database. The system should provide access to multiple biometric authentication methods to support the different needs of the stakeholders.

Invest resources to develop a robust public infrastructure for e-KYC and digital identity:
- Invest resources in order to augment the infrastructure of its national ID database in order to facilitate digital identity and e-KYC transactions at scale.
- This would require investment in cost-effective, device agnostic authentication infrastructure to enable biometric matching, enhanced network and cybersecurity systems and reliable application programming interfaces (APIs).

Define rules of engagement for the private sector:
- In order to meet the requirements of a wide range of actors in the Indonesian digital economic landscape, it would be critical that digital identity and e-KYC services are not subject to discretionary powers of one or two government agencies but instead made available to a wide range of players by defining a standardized set of rules for engagement that fosters a robust rules based ecosystem.

Affordable pricing of solutions to encourage adoption:
- The results from the report can act as a reference for the willingness to pay of the stakeholders for digital identity and e-KYC services.
- A tiered cost structure can be developed to enable different levels of access.
- Countries around the world have adopted different strategies to price digital identity services.

Encourage ecosystem partners and data protection:
- Build and encourage an ecosystem of institutions for enrollment and authentication, among others, to ensure usage of services.
- 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 supporting architecture should allow easy access and affordable verification services to a variety of stakeholders

The proposed architecture should encourage development of a rule based ecosystem which allows both service as well user agencies to build innovative digital identity solutions that meet the requirements of a dynamic digital economy

- A technology-agnostic design will allow players to adopt a process best suited to their requirements. Service agencies can further develop their business/operating models based on business requirements of user agencies.

- Not all biometric technologies fit every use-case, which makes it important to recognize the right biometrics for the right scenario based on different performance and suitability parameters.
Proposed process flow of an ideal KYC verification process

1. Customers using remote or assisted onboarding
   - Customer registers and provides details, including their name, NIK number, and biometric information (fingerprint, face/photo, or iris)

2. Details captured by the web or mobile tool monitored by a customer service agent
   - Financial services provider (In-house application)
   - Automated authentication request through API to an intermediary
   - Authentication successful/unsuccessful
   - Yes/No response (in case of authentication request)
   - Personal identity information (for KYC request)

3. Account generated

4. Authorized third-party intermediary

5. Identity verification through biometric matching

6. Dukcapil NIK Data Repository

7. AML + Enhanced due diligence (when required) by the in-house team or third-party providers

8. Yes/No response (in case of authentication request)

*USD 2.2 – 5.02 Upper limit includes digital signature verification as well
AML - Anti-money laundering

---

All rights reserved. This document is proprietary and confidential.
An affordable and tiered costing structure could be considered to encourage adoption and uptake of digital identity services

The costing structure can consider the type of authentication and any data exchange to offer economical options to all stakeholders according to their needs.

<table>
<thead>
<tr>
<th>1</th>
<th>Simple Yes/No reply whether a match is found in the NIK database</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>Confirmation of a match as well as viewing of demographic data and credentials for verification</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Tentative cost (per request) for service providers (user agencies)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Simple Yes/No reply</td>
</tr>
<tr>
<td>Confirmation of a match as well as viewing of demographic data and credentials for verification</td>
</tr>
</tbody>
</table>

This is calculated based on the willingness to pay of stakeholders, actual charges and real cost will differ based on government decisions during rollout.

The service agency can further build its business model to offer services like digital signature, digital lockers, among others.

Based on above estimates, if e-KYC were to be implemented in Indonesia, the financial sector could see huge economic savings due to efficiency gains and cost effective verification of customer identity.

The implementation of e-KYC could save the FinTech sector USD 3.9-4.4 billion (IDR 57-63 trillion) and the banking sector close to USD 160-237 million (IDR 2,357-3,436 billion) in the next 10 years.

This is calculated based on the savings from the verification process as well as the savings from reduced administrative processes during onboarding. Additional savings in e-authentication processes can also be realized.

USD/IRD exchange rate: 14,500 (Avg over the period June-Nov’20)
Countries have adopted different strategies to price digital identity and e-KYC services

Although the investments in building a digital identity architecture is significant, countries around the world have adopted different strategies to sustain the maintenance of the digital identity infrastructure.

<table>
<thead>
<tr>
<th>Country</th>
<th>Population (in million)</th>
<th>Model of pricing</th>
<th>Pricing of verification and identity services</th>
</tr>
</thead>
</table>
| India       | 1339                    | Free for public sector and nominal charges for private sector | • Public sector: Free  
• Private sector: USD 0.007 for Aadhaar authentication with a yes/no response - USD 0.3 for e-KYC transactions |
| Malaysia    | 31                      | Nominal charges for both public and private sector        | • USD 0.13 to verify a demographic record  
• USD 0.25 to verify a demographic and biometric record |
| Pakistan    | 193                     | Nominal charges for both public and private sector        | • Public sector: USD 0.09 per query  
• Private sector: USD 0.29 per query |
| Thailand    | 69                      | Free for both public and private sector                   | • Free verification of a demographic record and the national ID card (it is considered as a citizen service) |

Source: ID4D, World Bank
Regulatory landscape for KYC in Indonesia
Several laws and governing bodies directly or indirectly regulate the KYC process for financial services industry in Indonesia

Regulations on AML-CTF in the financial sector

- **Banks:** POJK No. 23 /POJK.01/2019 defines the regulations on AML and CFT in the financial service sector. It outlines procedures for:
  - Tiered customer due diligence (simplified CDD, basic CDD and enhanced DD),
  - Face-to-face and non-face-to-face verification. The later requires at least 2 factor authentications (art.17)
- **POJK 23/2019** relaxes the identification and verification requirement for low risk customer profiles such as BSA customers. BSA can be opened by adopting a simplified CDD process (explanation of POJK No. 12 /POJK.01/2017, page 3)
- **E-money players:** PBI No.19/10/PBI/2017 outlines the regulations on AML and CFT for the non-bank payment service providers. It allows for: both face-to-face and non-face-to-face verification. It provides detail on the procedure of non-bank payment providers doing a simplified CDD (art 29). Service providers may utilize biometric or electronic data only if they can ensure the validity and reliability of the data (art.20)
- **P2P players** POJK 77/POJK.01/2016 defines regulations for P2P players to implement AML-CFT policy as mandated in POJK No. 23 /POJK.01/2019 (art.42)

Laws on citizenship database and access

- **The Population Administration Law No. 24 Year 2013** states that the biometric data held in the NIK (SIAK) database needs to be protected. However, it does not provide details on the treatment of “protected data.” (art.54)
- **Permendagri No. 102 year 2019** states that:
  1. Legal entities can only access Dukcapil database by using a Yes/No verification matching.
  2. MoHA provides 3 alternative methods for data access: using card reader, through a web service, and a web portal access (art.21)
  3. Access to the Dukcapil database is limited to MoHA staff and users (including business entities). The user agencies are required to enter into an MoU with Dukcapil.
  4. Violation of the access right may result in: web user access or card reader deactivation, network disconnection, and termination of MoU (art.45)
Regulations for customer due diligence processes for BSA, P2P lending, and e-money accounts are regularly updated

### Customer acquisition
A customer needs to submit the following documents:
- Valid ID (e-KTP, passport, KITAS, etc.)
- Fill in data points
- Signature or fingerprint

References:
- PBI 14/27/PBI/2012 article 15
- POJK 12/POJK.03/2018 article 11

### Customer verification
1. Customer identity can be verified face-to-face or by utilizing an eligible electronic device with at least two-factor authentication from what you have (valid ID), what you are (biometric database), and what you know (PIN/ password/OTP)
2. Financial Service Providers (FSPs) must assess the customer’s risk profile based on their profile, country, product usage, transaction line, and where the level of tiered CDD* requires minimum data:

<table>
<thead>
<tr>
<th>Simplified CDD</th>
<th>Name, ID, Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>Basic CDD</td>
<td>DBO/POD, ID, phone number, addresses (home and office), occupation, gender, marital</td>
</tr>
<tr>
<td>Enhanced CDD</td>
<td>Source of fund, transaction purpose, business relationship</td>
</tr>
</tbody>
</table>

3. A third party to represent FSP in conducting CDD should gain approval from OJK and related FSPs shall be responsible for the result of the CDD.

References:
- On Banks: PBI 14/27/PBI/2012 article 23, POJK 19/POJK.03/2014 article 31 and 33, POJK 12/3/2018
- On FinTechs: 19/10/PBI/2017 article 29, 30, 40, 20/6/PBI/2018 article 37, POJK 23/POJK.01/2019 article 17, 28, 30)

### Activation
1. Unverified BSA customers can only do savings (POJK 19/POJK.03/2014 article 31)

### Data storage
1. Customer data is stored, in accordance with explicit consent of the customer, in forms (original paper based form), copy, electronic form, microfilm, or as regulated by OJK (POJK 23/POJK.01/2019 article 56)
2. Customer data must be kept for at least five years (PBI 19/10/PBI/2017 article 51, PBI 14/27/PBI/2012 article 41)
3. The Data Center and Backup (DRC) must be located within the Indonesia geographic area (ICT Ministry Regulation 20/2016 article 17, POJK 38/POJK.03/2016 article 21)

* Tiered CDD includes: Simplified CDD (i.e. for G2P Basic Saving Account), basic DD, and Enhanced DD
** BSSN, BPPT, PrivyID, Perum Peruri, VIDA, Digisign
Details of existing KYC processes followed by financial service providers in Indonesia
Snapshot of different models for KYC in Indonesia. Business requirements, level of access to citizenship data and internal capacities have implications on KYC process chosen by a particular service provider

<table>
<thead>
<tr>
<th>S. No.</th>
<th>KYC operational model</th>
<th>Service providers</th>
<th>Summary</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Conventional branch-based model</td>
<td>Commercial banks</td>
<td>Customer walks into the service provider outlet, face-to-face interaction with service provider staff, physical checking of documentation</td>
</tr>
<tr>
<td>2</td>
<td>Agent-assisted model</td>
<td>Commercial banks with Laku Pandai agent networks</td>
<td>Customer walk into the service provider agent, documentation at agent point (including copy of e-KTP), documents transported to the service provider branch, document check by the service provider staff and KTP details verified from web access to Dukcapil database</td>
</tr>
<tr>
<td>3</td>
<td>G2P model</td>
<td>Himbara banks</td>
<td>Relevant government ministry shares the beneficiaries data with the banks for account opening. The banks connect to Dukcapil database (web service) to verify identity of the beneficiaries. The accounts are opened in a centralized manner while passbook/PIN/card is distributed in the field through by bank staff and</td>
</tr>
<tr>
<td>4</td>
<td>Mobile service provider staff using e-KTP readers</td>
<td>Commercial banks</td>
<td>Account opened by the service provider staff or contracted third parties who deploy mobile agents to acquire customers. The mobile agents carry a biometric card reader device attached to a smart device. The device captures customers biometrics and matches it with the data stored on e-KTP chip. If the match is successful, relevant demographic details are retrieved digitally from the e-KTP chip</td>
</tr>
<tr>
<td>5</td>
<td>Remote KYC using the service provider mobile app</td>
<td>FinTechs (e-money, P2P players)</td>
<td>Account opened remotely by self registration on service provider mobile application. Customer are asked to enter their personal identity data along with a selfie with a photo of the their e-KTP card. Few service providers have web access to Dukcapil and can match the data</td>
</tr>
</tbody>
</table>
Many institutions and private players have signed MoU agreements with Dukcapil for access to the NIK database, however, such access is currently restricted to demographic data only.

Most recently, 13 financial institutions, including e-wallet and P2P players, were granted access to citizenship data through an MoU signed with Dukcapil on 11th June, 2020. Thousands of other institutions also have an MoU with Dukcapil. These include 1,177 banks, 462 higher education institutions, 124 capital market players, and 45 hospitals. Government ministries such as MoSA also have access to Dukcapil database and use it extensively for delivery of G2P programs.

Apart from individual institutions, intermediaries that provide verification services have the following different levels of access:

<table>
<thead>
<tr>
<th>PrivyID</th>
<th>Verijelas</th>
<th>ASLI RI</th>
<th>Nodeflux</th>
</tr>
</thead>
<tbody>
<tr>
<td>MoU signed with Dukcapil</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Types of access granted</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>NIK database</td>
<td>NIK database, e-KTP photo data</td>
<td>NIK database (some news also mentioning about biometric access as well)</td>
<td>NIK database and e-KTP photo to support police' face search system</td>
</tr>
</tbody>
</table>

To gain the "right to access," industry players must pass all terms and procedures set by MoHA. They must also fulfill some legal requirements* and obtain recommendation from an authority, such as OJK.

*Legal requirements, such as submitting a formal request to Dukcapil, attaching business documents, and obtaining a recommendation from the authority.
## Details of existing onboarding processes for customers and agents

<table>
<thead>
<tr>
<th></th>
<th>Banks</th>
<th>E-money players</th>
<th>P2P lenders</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Customers</strong></td>
<td>Process and cost for opening a basic savings account, including under G2P programs, such as PKH</td>
<td>Customer Process and cost for signing up customers for a registered e-money account</td>
<td>Borrower Process and cost for onboarding individual borrowers on the platform</td>
</tr>
<tr>
<td><strong>Agents</strong></td>
<td>Process and cost for onboarding BSA customers through Laku Pandai agents and bank branches</td>
<td>Small merchants Process and cost for onboarding QRIS merchants</td>
<td>Lenders Process and cost for onboarding individual retail lenders on the platform</td>
</tr>
</tbody>
</table>
For Himbara banks that implement the G2P mandate, the beneficiary onboarding process is centralized and resource-heavy. As per their Service Level Agreement (SLA), the banks are required to complete the process within 60 days.

Teams involved
Ministry/Government entity

Government Project team
Cash and Trade Operation team or the Jakarta-based central HQ operations
Cash and Trade Operation team (savings book) and the Electronic Channel Operation team (cards)/HQ in Jakarta

Branch staff and taskforce

Receive beneficiary data from the Ministry of Social Affairs (MoSA)

Dukcapil has allotted a quota of 1,000,000 for the bank per day. Currently, no fee is paid to Dukcapil.

Verification by host-to-host matching with Dukcapil and checking of duplicate data at the bank. Mapping of beneficiaries done at the regional or branch office

Yes

Input data to the Account System for bulk account opening process

Account number generated

Card and savings book printing and deployment

Amount of cards and savings books reach branch office

Gather beneficiaries in groups and conduct socialization

Beneficiaries receive cards and savings books

T+14

T+28

T+31 to max. T+35

T+45 to T+50

max. T+60

T+30 to T+60

10-15 employees are involved in socialization, camps that last 3-5 days, and approximately 300-500 beneficiaries attend per day depending on location

~10% of applications are returned to MoSA due to incomplete data (missing NIK) or duplicate data.

MoSA will complete the beneficiary data or replace the data with accurate info

A maximum of 200,000 beneficiaries can be processed through Bulk Account Opening per day

Ministry/Government entity

Acquisition Verification Activation Socialization

Details in the annex slide
The onboarding process of BSA customers through Laku Pandai agents can take up to two weeks. Given the inefficiencies in the process, majority of agents in Indonesia do not offer account opening services.

### Teams involved

**Agents**

**Customers fill the application form via Laku Pandai agents, including copies of his/her e-KTP card**

**Sales Representative (SR)**

The sales representative picks up the forms, usually in batches

**Branch office (CSO and CSR)**

Cabang Pengelola Agent (agent-managing branch office) receives the form

**Sales Representative (SR)**

A simple CDD process is performed by the branch staff. The branch staff verifies the document as well as the identity details through a web access facility to Dukcapil database

**Agents**

The branch opens the basic savings account and issues a welcome letter

**Agents**

The sales representative brings the welcome letter to agents

**Customers visit agents to collect their welcome letter**

This is the process followed by mobile-based BSA accounts, for some banks who have conventional BSA accounts, the customer is required to collect the passbook and/ the ATM card from the branch.

Details in the annex slide
Acquisition of Laku Pandai agents is done through multiple channels. Verification of agent identity is done by checking agent identity data through web access to Dukcapil database.

<table>
<thead>
<tr>
<th>Teams involved</th>
<th>Sales representative at the branch office</th>
<th>Branch Manager or Area Head</th>
<th>Head office</th>
<th>Area office</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>T</strong></td>
<td><strong>T</strong></td>
<td><strong>T+1 to T+5</strong></td>
<td><strong>T+5</strong></td>
<td></td>
</tr>
<tr>
<td>Agents are acquired in one of the following three ways:</td>
<td>Sales Representative at the branch office inputs data in the Agent Management system</td>
<td>Verification of agent identity data is affirmed through an eyeballing process by the head office or branch office through the Dukcapil web portal access</td>
<td>Upload of approved agent details on agent management system for EDC deployment</td>
<td>Onboarding and training, especially on EDC device operations</td>
</tr>
<tr>
<td>1. Agent may initiate self register at branch</td>
<td>Additionally, bank staff may conduct an site visit to check the viability of the place and business</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2. In-house agent acquisition team</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3. Third-party acquirers in some remote regions through related stakeholders, such as MoSA or Bulog</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Acquisition | Verification | Activation | Socialization
## Details of existing onboarding processes for customers and merchants

<table>
<thead>
<tr>
<th>Banks</th>
<th>E-money players</th>
<th>P2P lenders</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Customers</strong></td>
<td><strong>Customer</strong></td>
<td><strong>Borrower</strong></td>
</tr>
<tr>
<td>Process and cost for opening a basic savings account, including under G2P programs, such as PKH and BPNT</td>
<td>Process and cost for signing up customers for a registered e-money account</td>
<td>Process and cost for onboarding individual borrowers on the platform</td>
</tr>
<tr>
<td><strong>Agents</strong></td>
<td><strong>Small merchants</strong></td>
<td><strong>Lenders</strong></td>
</tr>
<tr>
<td>Process and cost for onboarding BSA customers through Laku Pandai agents and bank branches</td>
<td>Process and cost for onboarding QRIS merchants</td>
<td>Process and cost for onboarding individual retail lenders on the platform</td>
</tr>
</tbody>
</table>
The existing customer onboarding process for FinTechs involves a considerable amount of manual intervention, which results in errors and increased costs as well as the need for exception handling.

**Front-end customer acquisition**

Customers self-register through the web or mobile app.

Fill in the name and NIK number, Take a selfie and provide a separate ID picture.

Enter other required customer details in FSS.

**Customer verification and activation (Manual or automated process)**

Web/mobile tool/customer service

Automated matching systems/OCR on the ID details.

Outsourced agency/in-house staff*

Authentication successful

Request sent to third-party agents via web services

Activation of account

Financial services provider (In-house application)

Authentication unsuccessful

Manual eyeballing against Dukcapil through web access. In the case of EDD, other databases like the UN-sanctioned list of terrorist, PEP, KPU, among others, are used for AML compliances

视频 calls/process restart

Exception handling procedures

*Outsourced/third party agencies typically employ operators who are given computers, etc and access to the web portal of Dukcapil and other databases to complete the verification process as per the service provider requirements.

FSS: Financial software and systems
The existing processes of e-money players are semi-digital, with manual processes for verification

<table>
<thead>
<tr>
<th>Step 1. Sign up</th>
<th>Self-initiated process</th>
<th>Step 4. Identity verification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Customers sign up via the service provider mobile application</td>
<td>Two checks are performed, a photo match and a demographic data check. Some players have developed automated matching systems for the initial checking of data entered by the customer with e-KTP details. Some players use the OCR technology and conduct liveness checks. Most players use the eyeballing method for verification. Some players employ in-house staff while others use outsourced agents. The data entered by the customer is cross-checked with the details on the e-KTP card.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 2. Fill up the registration form</th>
<th>Manual and automated data verification</th>
<th>Step 5. Automated in-house EDD and AML</th>
</tr>
</thead>
<tbody>
<tr>
<td>Customers fill basic details into the form on the app</td>
<td>Customers need to upload pictures of e-KTP and a selfie of themselves holding the e-KTP card</td>
<td>Customer details are checked against various databases and the in-house team verifies any hits. Some players have dynamic AML processes and conduct enhanced due diligence checks using AI.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 3. Upload the required documents</th>
<th>Step 6. Activation by the system</th>
</tr>
</thead>
<tbody>
<tr>
<td>Customers must upload pictures of e-KTP and a selfie of themselves holding the e-KTP card</td>
<td>Once the verification is complete and recorded on the system, the activation is done in the backend.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 7. Customers receive a notification on successful activation</th>
<th>Step 8. Data storage on the server and cloud</th>
</tr>
</thead>
<tbody>
<tr>
<td>The customers get a notification through SMS.</td>
<td>Some players use third-party services while some use their own. The data is stored for five years after the business interaction ends.</td>
</tr>
</tbody>
</table>

OCR: Optical character recognition

T+1 to 2 days
To open a merchant account, the business owner first needs to complete their KYC followed by the business verification process.

**Step 1. Sign up**
Most players hire third parties for acquisition and the fee is paid based on successful conversions.

**Step 2. Onboarding of the merchants**
Onboarding is either done through the app by the merchant or by the merchant acquisition team that sends the details for manual entry at the backend.

**Step 3. Upload the required documents**
Merchants share KYC data as well as business profiles and details.

**Step 4. Identity verification**
Players use either automated matching systems or the eyeballing method for identity verification of the owner. Eyeballing is mostly outsourced.

Automated in-house EDD and AML checks against various databases are also completed.

**Step 5. Business verification**
Business verification is completed by eyeballing of photos, location, and online screenshots of the shop as well as through checking by third-party agents. Some players verify the business by sending local teams to physically verify the business.

**Step 6. QRIS registration**
QRIS registration is completed and the details are sent to PTEN through email. The response is received and linked to the merchant account in the backend. Some players verify the provided bank account details through their switching partners.

**Step 7. Starter kit distribution**
Starter kits are sent to merchants through courier partners.

**Step 8. Data storage on the server and cloud**
The data is stored in-house or on vendor cloud servers.

The data is stored for five years after the business interaction ends.

**Third-party acquirers**

**Manual and automated data verification**

**QRIS registration and automatic activation**

**Customer data is stored as per regulation**
The KYC process can be broadly divided into stages handled by different teams, e-money players use different options but verification it is largely outsourced.

<table>
<thead>
<tr>
<th>Customers</th>
<th>Merchants</th>
</tr>
</thead>
<tbody>
<tr>
<td>Teams involved (Team size)</td>
<td>Teams involved (Team size)</td>
</tr>
<tr>
<td>Self-initiated process</td>
<td>In-house customer service (100) and outsourced</td>
</tr>
<tr>
<td>Option 1: Outsourced service provider</td>
<td>Option 1: In-house teams: Business user (5), Commerce (5), Operations (10)</td>
</tr>
<tr>
<td>30% rejected due to blurry or mismatched pictures</td>
<td>2.5% rejected due to e-KTP issue or duplicate merchant name</td>
</tr>
<tr>
<td>Option 2: In-house automated system for Dukcapil matching</td>
<td>Option 2: Outsourced field team</td>
</tr>
<tr>
<td>Option 3: In-house AML analysts (5) and outsourced KYC agents (100)</td>
<td></td>
</tr>
<tr>
<td>Automated</td>
<td>In-house Operations team, service provider (Switcher and PTEN)</td>
</tr>
</tbody>
</table>

*Fraud: Abusing cashback offers
*Rejections do not include merchants rejected due to discrepancies found during onsite visits
## Details of existing onboarding processes for borrowers and lenders

<table>
<thead>
<tr>
<th>Banks</th>
<th>E-money players</th>
<th>P2P lenders</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Customers</strong>&lt;br&gt;Process and cost for opening a basic savings account, including under G2P programs, such as PKH and BPNT</td>
<td><strong>Customer</strong>&lt;br&gt;Process and cost for signing up customers for a registered e-money account</td>
<td><strong>Borrower</strong>&lt;br&gt;Process and cost for onboarding individual borrowers on the platform</td>
</tr>
<tr>
<td><strong>Agents</strong>&lt;br&gt;Process and cost for onboarding BSA customers through Laku Pandai agents and bank branches</td>
<td><strong>Small merchants</strong>&lt;br&gt;Process and cost for onboarding QRIS merchants</td>
<td><strong>Lenders</strong>&lt;br&gt;Process and cost for onboarding individual retail lenders on the platform</td>
</tr>
</tbody>
</table>
Borrowers on P2P platforms are acquired through multiple channel and require a valid NIK number to begin on boarding process

**Step 1. Sign up**
Borrowers may sign up through the service provider mobile application, website, or e-commerce platform

**Step 2. Fill up the registration form**
The fields of the form include not only the personal details but also the purpose of the loan.

**Step 3. Upload the required documents**
All players require e-KTP and some also require NPWP (Tax number)

**Step 4. Verification of data**
- Only a few players use a 100% automated process while others use a combination of the manual and automated methods.
- A few players have developed their own verification machine. Others use third-party service and a report is maintained on a live Google Sheet.
- Some players employ in-house staff and others use third-party agents.

**Step 5. Verification of the digital signature**
Some conduct digital signature verification while some do not. Third-party vendors connected to the system through APIs conduct digital signature verifications.

**Step 6. Activation by the system**
Once the verification is complete and recorded on the system, the activation is done in the backend.

**Step 7. Borrowers get a notification on successful activation**
Service providers notify lenders through an email and/or service provider mobile application

**Step 8. Data storage on the server and cloud**
Some players use third-party services while some use their own.

The credit rating of the borrowers is also conducted simultaneously with this process and the score remains dynamic throughout the borrower’s business association.
P2P players use both automated and manual KYC processes during which lenders must provide a valid e-KTP and bank account details.

**Acquisition**
Self-initiated process

**Step 1.** Sign up
Some lenders sign up via app, some others via website

**Step 2.** Fill up the registration form
The field details of the form are as per OJK regulation.

**Step 3.** Upload the required documents
Different players might require different documents, but e-KTP and bank account details are typically common.

**Verification**
Manual and automated data verification

**Step 4.** Eyeballing process
Some players employ *in-house staff* while others use *outsourced agents* who report through live Google Sheets.

**Step 5.** Verify against third-party resources
1. All players use third-party services to check the validity of the e-KTP.
2. Some use a third-party database to check the background of the lenders and validate their bank accounts.
3. Players also complete digital signature verification through third parties

**Activation**
Automatically done by the system

**Step 6.** Activation by the system
Once the verification is complete and recorded on the system, the activation is done in the backend.

**Step 7.** Lenders get a notification on successful activation
Service providers notify lenders through an email and/or service provider mobile application

**Storage**
Customer data is stored as per regulation

**Step 8.** Data storage on the server and cloud
Some players use third-party services while some use their own.
The KYC process is handled by in-house teams or outsourced to service providers and the productivity varies depending on the type of P2P lender

<table>
<thead>
<tr>
<th>Lenders</th>
<th>Borrowers</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Acquisition</strong></td>
<td></td>
</tr>
<tr>
<td>Institutional lending player 1</td>
<td>Retail lending player 1</td>
</tr>
<tr>
<td>Teams involved (Team size)</td>
<td>Teams involved (Team size)</td>
</tr>
<tr>
<td>Self-initiated process</td>
<td>Self-initiated process</td>
</tr>
<tr>
<td>Outsourced to service provider (SP) and in-house customer service (2)</td>
<td>Outsourced to SP for digital signature and credit bureau</td>
</tr>
<tr>
<td>Outsourced SP and in-house credit risk team (15)</td>
<td>Outsourced to SP and in-house AI application</td>
</tr>
<tr>
<td>Teams involved (Team size)</td>
<td>Teams involved (Team size)</td>
</tr>
<tr>
<td>avg applications per day</td>
<td>avg applications per day</td>
</tr>
<tr>
<td>20-30</td>
<td>27</td>
</tr>
<tr>
<td>300</td>
<td>300</td>
</tr>
<tr>
<td>20% rejected due to low credit score</td>
<td>20-25% rejected due to low credit score</td>
</tr>
<tr>
<td><strong>Verification</strong></td>
<td></td>
</tr>
<tr>
<td>Teams involved (Team size)</td>
<td>Teams involved (Team size)</td>
</tr>
<tr>
<td>Self-initiated process</td>
<td>Self-initiated process</td>
</tr>
<tr>
<td>Outsourced to service provider</td>
<td>Outsourced to SP for digital signature and the Operations team for exception handling</td>
</tr>
<tr>
<td>Teams involved (Team size)</td>
<td>Teams involved (Team size)</td>
</tr>
<tr>
<td>avg applications per day</td>
<td>avg applications per day</td>
</tr>
<tr>
<td>20% rejected due to low credit score</td>
<td>20-25% rejected due to low credit score</td>
</tr>
<tr>
<td><strong>Activation</strong></td>
<td></td>
</tr>
<tr>
<td>Teams involved (Team size)</td>
<td>Teams involved (Team size)</td>
</tr>
<tr>
<td>Self-initiated process</td>
<td>Self-initiated process</td>
</tr>
<tr>
<td>Teams involved (Team size)</td>
<td>Teams involved (Team size)</td>
</tr>
<tr>
<td>avg applications per day</td>
<td>avg applications per day</td>
</tr>
<tr>
<td>60% rejected due to low credit score</td>
<td>60% rejected due to low credit score</td>
</tr>
<tr>
<td>22-30% cases for exception handling due to delayed response</td>
<td>22-30% cases for exception handling due to delayed response</td>
</tr>
<tr>
<td><strong>In-house quality assurance (1)</strong></td>
<td><strong>In-house quality assurance (1)</strong></td>
</tr>
<tr>
<td><strong>Customer service (2)</strong></td>
<td><strong>Customer service (2)</strong></td>
</tr>
<tr>
<td><strong>Marketing (80)</strong></td>
<td><strong>Marketing (80)</strong></td>
</tr>
<tr>
<td><strong>Outsourced SP</strong></td>
<td><strong>Outsourced SP</strong></td>
</tr>
<tr>
<td><strong>56% rejected due to blurry or invalid KTP</strong></td>
<td><strong>56% rejected due to blurry or invalid KTP</strong></td>
</tr>
</tbody>
</table>
Challenges in the existing KYC processes
The dependence on just one source of identification data for verification creates major challenges for the service providers.

No single source of truth to verify customer identity data (limited access and not real time)

Risk of manipulation and errors in data entered by the customer

High rates of errors and false positives

Dependence on third parties, exception handling, and manual processes

Increase in the operational cost

---

**Key issues in individual KYC (customers, lenders, and borrowers)**

<table>
<thead>
<tr>
<th>Limited data for verification</th>
<th>Errors require manual interventions</th>
<th>Activities that increase cost</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dependence on customer input and photographed KTP card for identity data</td>
<td>30-60% rejections* because of blurry images due to the poor quality of camera or photo</td>
<td>Increase in staff costs and time to deal with exceptions by conducting video calls or physical checks</td>
</tr>
<tr>
<td>Other permissible IDs like passport and driver’s license do not have a source for authentication</td>
<td>Necessary to double-check manually to ensure the KTP has not been tampered with</td>
<td>Third-party KYC verifications range from IDR 21,500 - 33,000 (USD 1.5-2.3) per query</td>
</tr>
</tbody>
</table>

---

**Key issues in merchant (business entity) KYC**

<table>
<thead>
<tr>
<th>Multiple NMID and QRIS</th>
<th>Bank account verification</th>
<th>Business verification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Different QRIS and NMID issued for the same merchant by PTEN. PTEN uses the same name of the merchant as the differentiator. If there is a slight difference in the name, a different QR code will be issued.</td>
<td>Most players do not verify bank account details. Some use the services of a switching agent to verify and match the name.</td>
<td>Currently, no standards are set for business verification. The data points checked across players are different.</td>
</tr>
</tbody>
</table>

---

*Source: Stakeholder interviews*
Banks involved in the G2P mandate face a different set of challenges when onboarding beneficiaries as well as managing agents that serve beneficiaries

Several challenges arise in the process of onboarding and socializing G2P beneficiaries. These processes increase the cost for the bank since a large number of staff is required.

**Errors in beneficiary data:** The bank may receive incomplete or duplicate data (beneficiary already having a bank account) from the Ministry leading to delays and increase in costs.

**Limited quota for verification:** The allocated quota for Dukcapil verification includes the quota for other bank products as well. When the large G2P mandates have to be processed, the quota requirements lead to delays in account opening and one batch of G2P mandate may take days to complete. It also affects identity verification processes for other products and services.

**Cost of staff involved in socialization incurred by the bank:** Due to additional responsibilities for the staff involved in the socialization process, the bank needs to recruit and train more staff in some remote areas and thus incurs additional staff costs.

In addition to this, the bank also has to bear the cost of agent acquisition, especially in areas where they do not have branches and must pay high rates to third-party acquirers.
Costing of the existing KYC processes

Disclaimer: Costs have been rounded off to the nearest 1,000’s and efforts have been made to provide a range where applicable. However, it may not reflect the exact cost for all service providers in the market.
Banks

1. Social assistance program delivery (G2P)
2. Agent (Laku Pandai) assisted customer onboarding
3. Agent onboarding
The highest amount is spent on the socialization of beneficiaries and disbursement of kits during beneficiary onboarding.

Costs incurred per G2P beneficiary throughout the process.

Cost of acquisition is zero, however for 10-15% of cases where there is data mismatch, exception handling techniques will cost the bank.

Cost of verification includes only staff cost (through bulk account opening) as currently there is no fee for accessing the NIK database.

IDR 400

Cost of verification includes only staff cost (through bulk account opening) as currently there is no fee for accessing the NIK database.

IDR 9,600 - 30,100

IDR 14,400 - 33,400

Annual maintenance cost of the account is estimated to be between IDR 30-50k.

### Acquisition

<table>
<thead>
<tr>
<th>Particulars</th>
<th>Amount</th>
</tr>
</thead>
<tbody>
<tr>
<td>Beneficiary data shared by the government stakeholder (MoSA)</td>
<td>IDR 400</td>
</tr>
</tbody>
</table>

### Verification

<table>
<thead>
<tr>
<th>Particulars</th>
<th>Amount</th>
</tr>
</thead>
<tbody>
<tr>
<td>Verification cost</td>
<td>N/A</td>
</tr>
<tr>
<td>Staff costs</td>
<td>400</td>
</tr>
<tr>
<td>Printing costs*</td>
<td>2,750-21,300</td>
</tr>
<tr>
<td>Courier costs</td>
<td>800</td>
</tr>
<tr>
<td>Total</td>
<td>IDR 400</td>
</tr>
</tbody>
</table>

### Activation

<table>
<thead>
<tr>
<th>Particulars</th>
<th>Amount</th>
</tr>
</thead>
<tbody>
<tr>
<td>Staff costs</td>
<td>6,000-8,000</td>
</tr>
<tr>
<td>Printing costs*</td>
<td>2,750-21,300</td>
</tr>
<tr>
<td>Marketing and communication</td>
<td>2,000-21,000</td>
</tr>
<tr>
<td>Total</td>
<td>IDR 9,600-30,100</td>
</tr>
</tbody>
</table>

### Socialization

<table>
<thead>
<tr>
<th>Particulars</th>
<th>Amount</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total</td>
<td>IDR 14,400-33,400</td>
</tr>
</tbody>
</table>

### Note:

- Staff costs calculated as per time taken to complete process and average salary depending on team locations.
- Costs based on interviews with two Himbara banks.
- *Card costs vary depending on if there is a chip or magnetic strip.

<table>
<thead>
<tr>
<th>Particulars</th>
<th>Amount</th>
</tr>
</thead>
<tbody>
<tr>
<td>Beneficiary data shared by the government stakeholder (MoSA)</td>
<td>IDR 400</td>
</tr>
</tbody>
</table>

Note: Staff costs calculated as per time taken to complete process and average salary depending on team locations.

Costs based on interviews with two Himbara banks.

*Card costs vary depending on if there is a chip or magnetic strip.

Annual maintenance cost of the account is estimated to be between IDR 30-50k.
The highest amount is spent on the verification of basic savings account holders

Costs incurred per BSA customer throughout the process

- Application form: IDR 500
- Staff costs (face-to-face verification): IDR 6,200
- Welcome letter: IDR 500
- Printing costs for cards*: IDR 2,750
- Agent commission: IDR 4,000-5,000
- Total: IDR 7,200

- Staff costs: IDR 1,650
- Printing costs for cards*: IDR 2,750
- Total: IDR 6,200

- Annual maintenance cost is estimated to be between IDR 30-50k

Note: Staff costs are calculated as per the time taken to complete the process and the average salary depending on the team locations.

*Card costs varies depending on type of card and is optional.
The cost of agent acquisition varies across different channels of acquisition

<table>
<thead>
<tr>
<th>Cost Item</th>
<th>Amount</th>
</tr>
</thead>
<tbody>
<tr>
<td>Staff costs</td>
<td>IDR 1,650</td>
</tr>
<tr>
<td>Courier charges for deploying EDC machines</td>
<td>IDR 16,000</td>
</tr>
<tr>
<td>Additional cost of EDC if bank purchases the device else, rent amount as part of agent management</td>
<td>IDR 170,000 - 195,000</td>
</tr>
<tr>
<td>Training cost</td>
<td>IDR 100,000 - 125,000</td>
</tr>
<tr>
<td>EDC machines*</td>
<td>IDR 3,000,000</td>
</tr>
<tr>
<td>Marketing material</td>
<td>IDR 50,000 - 70,000</td>
</tr>
<tr>
<td>Agent support</td>
<td>TBD</td>
</tr>
<tr>
<td>Total</td>
<td>IDR 1,650</td>
</tr>
</tbody>
</table>

Note: Staff costs calculated as per time taken to complete process and average salary depending on team locations
FinTechs

1. Customer and merchant onboarding for e-money players
2. Lender and borrower onboarding for P2P players
While verification contributes significantly to the overall costs for onboarding e-money customers, merchant acquisition can be a substantial cost if third-party acquirers are used.

**E-money customer**

- **Acquisition**: IDR 1,600-16,000
- **Verification**: IDR 0
- **Activation and storage**: IDR 0

**Cost drivers:**
- **Self-initiated processes on the apps**
- **Third-party agent costs**
- **Automatic system activation and in-house storage**

**E-money merchant**

- **Acquisition**: IDR 4,500-115,000
- **Verification**: IDR 0-80k
- **Activation and storage**: 1.5-3k

**Cost drivers:**
- **High costs due to third-party agencies with on-the-ground field teams while other merchants self-initiate onboarding through the app**
- **Range due to in-house automated verifications compared to outsourced providers**
- **Activation includes bank account check through switchers**

Costing estimates do not include digital marketing costs.
Verification is the highest contributor to the operational costs of onboarding a customer to a P2P platform.

**P2P lenders**

<table>
<thead>
<tr>
<th>Cost drivers:</th>
<th>IDR</th>
</tr>
</thead>
<tbody>
<tr>
<td>Self-initiated process on the app</td>
<td>0</td>
</tr>
<tr>
<td>Third-party agent costs including enhanced due diligence and digital signature verification</td>
<td>59-76k</td>
</tr>
<tr>
<td>Automatic system activation and in-house storage</td>
<td>0</td>
</tr>
</tbody>
</table>

**P2P borrowers**

<table>
<thead>
<tr>
<th>Cost drivers:</th>
<th>IDR</th>
</tr>
</thead>
<tbody>
<tr>
<td>Self-initiated process on the app</td>
<td>0</td>
</tr>
<tr>
<td>Third-party agent costs</td>
<td>8-21k</td>
</tr>
<tr>
<td>Automatic system activation and in-house storage</td>
<td>0-4.5k</td>
</tr>
</tbody>
</table>

Costing estimates do not include digital marketing costs.
Strategic considerations for implementing e-KYC
Key strategic considerations to implement digital identity and e-KYC services in Indonesia

1. **Policy**
   Should e-KYC and digital identity services using the Dukcapil infrastructure be a public good or will the private sector play a role in providing such services?

2. **Infrastructure**
   Is the Dukcapil infrastructure ready to conduct authentication and e-KYC? What infrastructure-level changes or modifications and capacity enhancements will Dukcapil need to make?

3. **Regulation**
   Would digital onboarding require any sort of legal or regulatory changes from OJK, BI, Dukcapil, or any other relevant government institution?

4. **Implementation**
   Are banks and FinTechs internally ready with systems to do e-KYC? What system modifications will they need to do digital onboarding (application, devices, connection to Dukcapil)?
Annexes
Annex 1:
Experience of other countries in implementing of digital identity and e-KYC service

- India
- Estonia
- Pakistan
- Singapore
The Unique Identification Authority of India (UIDAI) has made e-KYC and authentication services available in India by utilizing the Aadhaar ID program. It provides a unique biometric identifier to more than 1.2 billion people.

- eKYC service shares demographic data and the photograph of the user with the service provider when the user provides consent. This enables the onboarding of users for services, such as opening bank accounts, getting a SIM card, etc.
- UIDAI has open APIs to allow service providers in the public and private sector to authenticate users.
- The use of Aadhaar-enabled e-KYC for registration led to an increase in financial accounts from 48 million in 2017 to 138 million in 2018.

Account opening | Customer due diligence | Transaction authentication
---|---|---
- eKYC data is shared with the reporting entity in real time. Furthermore, the KYC data is released directly to service providers only upon the consent of the customer.
- The financial entities using eKYC and Aadhaar authentication can save up to USD 3 per KYC.
- Paytm, a payments application in India, used Aadhaar to register more than 6 million offline merchants. The onboarding process took less than three minutes on average.
- An OTP with a limited time validity is sent to the mobile number, e-mail address, or both of the Aadhaar number holder registered with the Authority. The Aadhaar number holder provides this OTP along with his Aadhaar number during authentication, which is then matched with the OTP generated by the Authority.
- Fingerprint-based or iris-based authentication or other biometric modalities are based on biometric information stored in the CIDR.

The customer onboarding process for financial services:
1. The user with an Aadhaar number presents the Aadhaar number or Virtual ID number and a biometric or OTP to the service provider (AUA).
2. The encrypted biometric from the UIDAI certified biometric device is packaged by the AUA as per the API specification and sent to ASA.
3. ASA transmits this packet over a leased line and invokes the authentication API of the Aadhaar system.
4. The API checks the incoming data against the CIDR and returns a YES/NO response based on the result of the match.
5. This response is conveyed by ASA to AUA and onwards to the user. AUA provides the service when the response is YES.

Costs for e-KYC: INR 20 (~USD 0.28) per request
Cost for authentication service: INR 0.5 per request (~USD 0.01)

Jio, an Indian telecom provider, onboarded around 160 million new customers in less than 18 months using e-KYC, enabled by India’s national digital ID system.

CIDR- Central Identities Data Repository
https://rbidocs.rbi.org.in/rdocs/notification/PDFs/NOTI190B865EC9E06464105A4A93180119A7455B.PDF
The Financial and Banking sector in Estonia embraced the use of digital IDs. Customers can open bank accounts, access services, conduct transactions, and affix their digital signatures using just their digital ID. Today, over 99% of all banking transactions in the country are carried out online.

<table>
<thead>
<tr>
<th>Account opening</th>
<th>Customer due diligence</th>
<th>Transaction authentication</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Opening a bank account online is possible using e-ID or e-Residency card, a video interview recording, and facial recognition technology.</td>
<td>• The eID provides full legal status for any interaction in Estonia that requires identity confirmation, such as e-commerce, electronic banking, and signing contracts.</td>
<td>• To identify the cardholder, the terminals deployed in practice read the publicly readable personal data file that resides on the chip of the Estonian ID card.</td>
</tr>
<tr>
<td>• Estonia ID card is a cryptographically secure digital identity card powered by a blockchain-like infrastructure on the backend. It allows an Estonian to access public services, financial services, and medical and emergency services. People can also pay taxes online, e-vote, provide digital signatures, etc.</td>
<td>• Estonian residents willingly allow government entities and service providers to use their digital identity information in exchange for trusted and high-quality services.</td>
<td>• To read the records, the terminal has to send several Application Protocol Data Unit (APDU) commands to the smart card and read the responses.</td>
</tr>
<tr>
<td>• To identify the cardholder, the personal ID code is the best option as it does not change during the cardholder’s lifetime.</td>
<td>• Through a key tool named “X-Road,” all decentralized components of the system are linked together and can operate in harmony, regardless of what platform is used. These components include various databases and registers in both the public and private sector.</td>
<td>• Any institution can use the public key infrastructure.</td>
</tr>
</tbody>
</table>

E-KYC in Pakistan utilizes the biometric ID system managed by the National Database & Registration Authority (NADRA). It provides authentication and verification services to several public and private agencies.

<table>
<thead>
<tr>
<th>Account opening</th>
<th>Customer due diligence</th>
<th>Transaction authentication</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Customers with a verified SIM dial a USSD string with their CNIC number. A backend system sends the Computerized National Identity Card (CNIC) number to NADRA to fetch customer data and populates all the data directly from NADRA servers into the operator’s database. Once this is completed, an account is opened.</td>
<td>• NADRA data is used to verify the identity of individuals for both bank account opening and mandatory mobile SIM card registration.</td>
<td>• NADRA has facilitated different stakeholders like banks, mobile operators, and other companies through biometric verification.</td>
</tr>
<tr>
<td>• The national ID cards allowed opening of bank accounts and reliable enforcement of transaction limits, which enabled the growth of branchless banking agents</td>
<td>• NADRA provides an online verification system where, for a fee, FSPs can verify the identity of a customer.</td>
<td>• This facility includes the following:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Secure verification service for third-party service providers</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Integration with telcos, banks, e-Sahulat, security companies, etc.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Real-time fingerprint verification</td>
</tr>
</tbody>
</table>

https://www.nadra.gov.pk/services/financial-service-solutions/

Account opening process using NADRA’s CNIC

NADRA has developed its own financial service solutions designed to provide the following services:

- Utility bill payment or collection
- Billing gateway
- Mobile banking
- Secure remittance platforms
- Electronic point of sales solutions
Singapore Personal Access or SingPass is an authentication system for citizens to transact online with the government. MyInfo, the government-backed digital vault, consolidates the personal data of residents and shares it with the government and private agencies on user request.

### Account opening

- Logging in using their SingPass, customers consent to the bank using their MyInfo profile to set up a new account.
- An online account application form is then pre-filled with the customer’s details so they do not need to key in details or submit any additional documentation to banking agents.

### Customer due diligence

- Private firms are required to register their systems with “MyInfo.”
- With the digitized KYC process, customers get authenticated real-time using electronic means, and the approval for successful account applications is granted instantly.

### Transaction authentication

- SingPass uses 2-Factor Authentication (2FA) as the customers are required to log in with their SingPass number.
- It takes less than five minutes to open an account through the bank’s website. Customers do not need to visit a bank branch or provide documents.

---

Digital account opening process using SingPass:

1. Open your account instantly
   - Easy application using MyInfo as your information is pre-filled. Supporting documents are not required.

2. Log in with SingPass for 2FA
   - Give consent to auto-retrieve data from MyInfo

3. Review pre-filled fields

4. Upload digital signature

5. A/C number displayed on screen

---

SingPass Mobile can be used as an alternative two-factor authentication (2FA) method to log in to government digital services. With SingPass Mobile, users can log in more easily using fingerprints or a 6-digit passcode.

- It is a easy and secure gateway to hundreds of government digital services and some from private sectors.
- It can be used to check the balance of CPF (pension fund), file tax returns, view personal information, and receive notification from government agencies.

---

https://www.youtube.com/watch?v=0pYtU2kG368/
https://www.singpass.gov.sg/myinfo/intro
Annex 2:
Additional details and timelines for the customer onboarding process

• BSA account opening for social assistance program delivery
• BSA account opening at an agent outlet
• E-money customer and merchant onboarding
• Borrowers and lenders onboarding on P2P platforms
Based on the agreement with MoSA, the overall process should be completed within two months.

**Acquisition**
- Day 0
- Min 0
- Verification
- Activation takes 3-4 days

**Verification**
- Day 9
- 1 Min
- Verification
- System initiated process for bulk account opening

**Activation**
- Day 14
- 5 Min
- Socialization of beneficiaries
- Approximately 200,000 accounts can be processed under BAO (Bulk Account Opening) in a day

**Printing**
- Day 28
- N/A
- Socialization of beneficiaries
- Approximately 30,000 cards and books printed in a day

**Deployment of kits**
- Day 35
- N/A
- Socialization of beneficiaries
- Kits received by beneficiaries
- Camps held for 3-4 days, with approximately 800 (Java) and 300 (Kalimantan) beneficiaries a day

**Socialization of beneficiaries**
- Day 50
- 3-5 Mins
- Socialization takes between 3-5 mins per beneficiary

**Deployment of kits**
- Day 60
- N/A

---

*The number of accounts cleansed per day varies with the bank. A maximum of 400,000 accounts are processed each day.*
Account activation usually takes up to two weeks as account opening forms are sent in batches from the agents to the associated branch.

Customer fills the application form and provides a copy of the KTP to agents.

The process is done after closing hour to prevent disruption.

The welcome letters are printed directly after activation, or until EoD.

Staff time required to complete the process:
- Acquisition: Agents turn in the application by either going directly to the branch office or waiting for the Sales Representative (SR), which takes longer.
  - Agents are usually located 1-3 hours away from the branch office.
- Verification: Agents perform a simple KYC beforehand. The branch staff call the customers and reconfirm the data. They then input the data into the system and compare it to Dukcapil data.
  - If rejected, the agents are informed. They offer customers the option to either drop the application or open a regular account.
- Activation: Staff at the branch is in charge of account activation.
- Deployment of kits: Since SRs are required to visit agents once a week, a week-long time lag is possible.

Days to complete the process:
- Day 0: Acquisition - 0 min
- Day 6: Verification - 30 min
- Day 14: Activation - 10 min
- N/A: Deployment of kits

Kits received by customers: N/A
Activation and setting up of accounts for merchants consumes the longest time on E-money platforms

E-money players

**Customers**

- **Day 0**: Acquisition 0 min
- **Day 1**: Verification 6-13 min, Activation and storage 23-43 min
- **Day 2**: Verification, activation, and storage 1 min

**Merchants**

- **Day 0**: Acquisition 0 min
- **Day 1-2**: Verification 22-42 min, Activation and storage 22-60 min
- **Day 2-5**: Verification, activation, and storage
- **Day 3-10**: Activation and storage 2,880 min

**Acquisition**

- Day 0
- Day 0

**Verification**

- Day 1
- Day 1-2
- Day 2-5

**Activation and storage**

- Day 2
- Day 2-5
- Day 3-10

**QRIS registration and generation or issuance of NMID for merchant**

**KYC as well as enhanced due diligence procedures completed**

**Online registration and onboarding by agents**

**KYC of merchant completed first, followed by business verification done by different agents**
Whereas the entire process is fairly quick for P2P players and is usually completed within a day.

**P2P players**

**Borrowers**
- **Day 0**: Acquisition
- **Day 1**: Verification, Credit rating of borrowers completed, simultaneously increasing the timeline
- **Day 1-2**: Activation and storage
- **Day 1-3**: Activation and storage

**Lenders**
- **Day 0**: Acquisition, verification, activation, and storage
- **Day 1**: Activation and storage

Online registration on the application or website.

Slight increase in time due to digital signature verification.
Annex 3:
Timeline of regulatory initiatives to promote digital financial inclusion
Timeline of regulations to promote digital financial inclusion and initiatives to help banks and FinTechs innovate and grow

Regulatory initiatives

- In 2014, OJK released the Branchless Banking regulation
- In 2016:
  - BI announced the National Payment Gateway to improve interoperability for banks and FinTech payment
  - BI launched the FinTech Office to monitor and advise FinTech services and security
  - OJK released a regulation on IT based-lending
- In 2017, Both BI and OJK regulated the application of AML and the prevention of CFT for non-bank FIs
- To respond to the growth of cashless payment and FinTech, in 2018:
  - BI updated e-money regulations, outlining capital guideline requirements and settlement
  - OJK launch the Innovation Centre for Digital FinTech Technology Office to facilitate the non-payment FinTech ecosystem
  - OJK mandated that all FinTech companies must be registered and go through the regulatory sandbox
- In 2019:
  - BI implemented the national QR standard for payment (QRIS)
  - OJK updated AML CFT implementation for P2P
  - The Ministry of Home Affairs released the regulation on citizenship data administration and utilization

Key trends

- Up to 2015
  - RFID and other contactless payment systems are evolving
- 2016
  - Global investment was focused on FinTech
  - Indonesia was the 4th largest mobile market (43% of the population used cell phone)
  - Consequently, social media and e-commerce grew

Market initiatives

- Six banks* initiated the launch of *Laku Pandai* products
- The first FinTech association (AFTECH) was established
- Bank Mandiri launched its FinTech incubator
- GoJek, Lazada, T-cash, and other FIs started to launch a closed-loop QR payment system
- G2P disbursement program was modified from postal office to BSAs
- Banks started to develop partnerships with FinTechs**
- 10 Banks and seven FIs signed an MoU to access the Dukcapil database

*The six banks include Mandiri, BRI, BNI, BTN, BTPN, and BCA.
**Partnership examples: Bank Mandiri-Cashlez/Amartha, Investree-Danamon
Annex 4:
Others

- Key assumptions for estimating economic savings of implementing e-KYC
- Comparison of different technologies for biometric authentication
- International standards for user authentication services
### Key assumptions for estimating economic savings from implementation of e-KYC services

<table>
<thead>
<tr>
<th>Data points used in the model from the study</th>
<th>Value (assumptions)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Average cost of the current process (including customer, merchants, borrowers, and lenders)</td>
<td></td>
</tr>
<tr>
<td>a) E-money</td>
<td>IDR 24,000 (USD 1.62)</td>
</tr>
<tr>
<td>b) P2P</td>
<td>IDR 48,500 (USD 3.28)</td>
</tr>
<tr>
<td>Assumed cost of e-KYC through Dukcapil for one application</td>
<td>IDR 5,000-7000 (USD 0.34-0.47)</td>
</tr>
<tr>
<td>Current administrative costs</td>
<td>IDR 8,000</td>
</tr>
<tr>
<td>Assumed savings in administrative cost</td>
<td>50%</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Data points used in the model</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Current number of customers:</td>
<td></td>
</tr>
<tr>
<td>a) E-money</td>
<td>125 million</td>
</tr>
<tr>
<td>b) P2P</td>
<td>16.4 million</td>
</tr>
<tr>
<td>Growth rate for the e-money sector</td>
<td>15% for 5 years</td>
</tr>
<tr>
<td>Assumed mean revert rate</td>
<td>5%</td>
</tr>
<tr>
<td>Growth rate for the P2P sector</td>
<td>10% for 5 years</td>
</tr>
<tr>
<td>Assumed mean revert rate</td>
<td>2%</td>
</tr>
<tr>
<td>Population growth</td>
<td>1.01%</td>
</tr>
<tr>
<td>Interest-free rate used for present value calculations (across all years)</td>
<td>6.73%</td>
</tr>
</tbody>
</table>
Comparison of different technologies for biometric authentication (1/2)

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Fingerprint authentication</th>
<th>Iris recognition</th>
<th>Facial recognition</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Engagement</strong></td>
<td>Contact-based</td>
<td>Contactless</td>
<td>Contactless</td>
</tr>
<tr>
<td><strong>Accuracy</strong></td>
<td>Moderate</td>
<td>High</td>
<td>Low</td>
</tr>
<tr>
<td><strong>Performance</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1. False acceptance rate (unauthorized people are accepted incorrectly)</td>
<td>High</td>
<td>High</td>
<td>Moderate</td>
</tr>
<tr>
<td>2. False rejection rate (authorized people are rejected incorrectly)</td>
<td>Low (0.01%)</td>
<td>Lowest (0.0001%)</td>
<td>High (0.2%)</td>
</tr>
<tr>
<td><strong>Cost</strong></td>
<td>Relatively Inexpensive</td>
<td>Expensive</td>
<td>Relatively Inexpensive</td>
</tr>
<tr>
<td><strong>Usability</strong></td>
<td>Easy</td>
<td>Moderate</td>
<td>Easy</td>
</tr>
<tr>
<td><strong>Scalability (depending on the tech and type of matching)</strong></td>
<td>High (approximately a billion matches per second)</td>
<td>High (matching rate of approximately 200,000 templates per second)</td>
<td>Low</td>
</tr>
<tr>
<td><strong>Security</strong></td>
<td>Low</td>
<td>High</td>
<td>Moderate</td>
</tr>
<tr>
<td><strong>Technology challenges</strong></td>
<td>Struggles to capture damaged prints</td>
<td>Requires highly specific positioning of the subject</td>
<td>Variable capture conditions</td>
</tr>
<tr>
<td><strong>Resistance to circumvention</strong></td>
<td>Low (Easy to spoof)</td>
<td>High (Very difficult to spoof)</td>
<td>Moderate (Easy to spoof)</td>
</tr>
</tbody>
</table>

Sources: [https://tinyurl.com/y5wtrm3to](https://tinyurl.com/y5wtrm3to); [Comprehensive survey on various biometric systems, Research India publications](https://researchindia.com/biometric-systems); [Technology landscape for digital infrastructure, World Bank](https://worldbank.org/technologylandscape).

*Surgery/ age/ etc. can affect results.*
Comparison of different technologies for biometric authentication (2/2)

<table>
<thead>
<tr>
<th>Fingerprint authentication</th>
<th>Iris recognition</th>
<th>Facial recognition</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Stability</strong>&lt;br&gt;Not universally inclusive: Gives unreadable results for people working in agriculture, manual labor, as well as the elderly and infants</td>
<td><strong>Affordability</strong>&lt;br&gt;Iris-capture hardware and software typically costs more than the one used for fingerprint authentication</td>
<td><strong>Performance</strong>&lt;br&gt;Satisfactory performance only under controlled scenarios. Performance degrades with aging and poor illumination</td>
</tr>
<tr>
<td><strong>Adoption</strong>&lt;br&gt;Contact-based fingerprint capture sensors are unhygienic and this perception could limit the willingness to use</td>
<td><strong>Adoption</strong>&lt;br&gt;Not as user friendly as fingerprint authentication. Some iris-capture devices require highly-specific positioning of the subject</td>
<td><strong>Security</strong>&lt;br&gt;Technology not immune to circumvention, risky in unsupervised environments</td>
</tr>
<tr>
<td><strong>Security</strong>&lt;br&gt;Technology not immune to circumvention</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Sources: [https://tinyurl.com/y5wtm3to](https://tinyurl.com/y5wtm3to); Comprehensive survey on various biometric systems, Research India publications, Technology landscape for digital infrastructure, World Bank

*Surgery/age/etc. can affect results*
International standards for user authentication services

There should be harmonization between regulations on CDD as mandated by regulators for different categories of financial accounts, including regular bank accounts, basic savings accounts, e-money accounts (registered and non-registered), insurance products, and capital market accounts. The CDD regulations should take into account the principle of proportionality while defining levels of assurances for authentication procedures.

The following two are widely accepted standards that could form the base for all regulations around user authentication:

ISO/IEC 29115

The future international standard ISO/IEC 29115 (Entity Authentication Assurance Framework) provides a framework to manage user authentication guarantees. It establishes four levels of assurance (LoAs) for entities, stipulating the criteria and guidelines for each of the defined levels.

Regulatory bodies in Indonesia should collectively define the level of assurance required for different services or products and standardize the requirements for the authentication of customer identity.

The framework for managing entity authentication assurance in a given context:
- Specifies four levels of entity authentication assurance;
- Specifies the criteria and guidelines to achieve each of the four levels of entity authentication assurance;
- Provides guidance for mapping other authentication assurance programs to the four LoAs;
- Provides guidance for exchanging the results of authentication based on the four LoAs;
- Provides guidance concerning controls that should be used to mitigate authentication threats.

NIST SP 800-63

NIST SP 800-63 (Electronic Authentication Guideline) establishes technical guidelines to implement authentication mechanisms for government and electronic commerce. While these recommendations are specifically for the US, they are broadly applicable to any environment that requires the authentication of entities and users.
MSC is recognized as the world’s local expert in economic, social and financial inclusion

International financial, social & economic inclusion consulting firm with 20+ years of experience

180+ staff in 11 offices around the world

Projects in ~65 developing countries

Our impact so far

550+ clients

Assisted development of digital G2P services used by 875 million+ people

Developed 275+ FI products and channels now used by 55 million+ people

>850 publications

Implemented >850 DFS projects

Trained 9,000+ leading FI specialists globally

Some of our partners and clients

- Bill & Melinda Gates Foundation
- MetLife Foundation
- Mastercard Foundation
- IFC (International Finance Corporation)
- UNCDF
- USAID
- World Bank Group
- CGAP
- Omidyar Network
- ADIB
- NPCI
- MIF	
- FirstBank
- DFSE
- Equity Bank
- Family Bank
- Credit Suisse
- Safaricom
- Centenary Bank
- mpesa
- Airtel
- Vodafone
- Access Bank
- Ecobank
- CESAG
- HF

Assisted development of digital G2P services used by 875 million+ people

MSC is recognized as the world’s local expert in economic, social and financial inclusion