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

December, 2020

SNKI SECRETARIAT
OF THE NATIONAL COUNCIL FOR FINANCIAL INCLUSION

MSC
MicroSave Consulting

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 maybe 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 of Contents

Abbreviations

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

Executive Summary

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

E-money players

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

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

P2P lenders

Customers initiate onboarding themselves by self registering on provider applications and the verification process is outsourced to third party vendors

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.

Banks

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

The cost for onboarding a G2P beneficiary ranges between **IDR 24,000-64,000 (USD 1.6- 4.4)** and may take **up to two months.** The cost involved in opening BSA through an agent ranges between **IDR 13,800-35,000 (USD 0.94-2.4)** and may take **up to two weeks.**

*The onboarding process and costs calculated in this report include acquisition, verification, activation, storage, and socialization.
Exchange rate: USD 1 = IDR 14,707

Executive summary (2/2)

Challenges observed in the current customer onboarding processes followed by service providers

E-money players

P2P platforms

- 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.
- This leaves room for manipulation, duplication, and poor quality of data/images.
- To address these issues, FinTechs had to adopt additional processes and exception handling techniques that increase operational costs.

Banks

- Banks mandated for G2P disbursements incur significant costs in printing and distributing KKS cards.
- In the absence of real-time verification of customer identity, BSA account opening through banking agents is a largely manual and time consuming.

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

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

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

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

https://www.bi.go.id/en/publikasi/sistem-pembayaran/riset/Pages/Blueprint-Sistem-Pembayaran-Indonesia-2025.aspx

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

E-money players	P2P lending platform	Banks
Customers Process and cost for signing up customers for a registered e-money account	**Borrowers** Process and cost for onboarding individual borrowers on the platform	**Customers** Process and cost for opening a basic savings account, including under G2P programs, such as PKH
Small merchants Process and cost for onboarding a QRIS merchant	**Lenders** Process and cost for onboarding individual retail lenders on the platform	**Agents** Process and cost for onboarding BSA customers through Laku Pandai agents and bank branches

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

Details captured

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

MSC

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

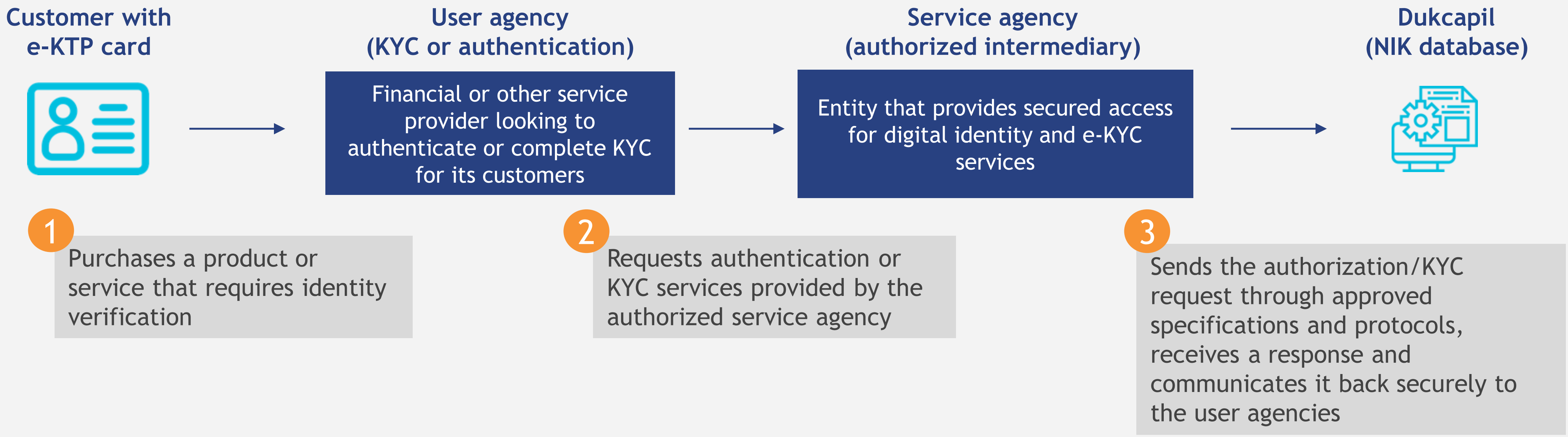
- The results from the report can act as a reference for the willingness to pay of the stakeholders for digital identity and e-KYC services.
- A tiered cost structure can be developed to enable different levels of access
- Countries around the world have adopted different strategies to price digital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



Customer with e-KTP card

User agency (KYC or authentication)

Financial or other service provider looking to authenticate or complete KYC for its customers

Service agency (authorized intermediary)

Entity that provides secured access for digital identity and e-KYC services

Dukcapil (NIK database)

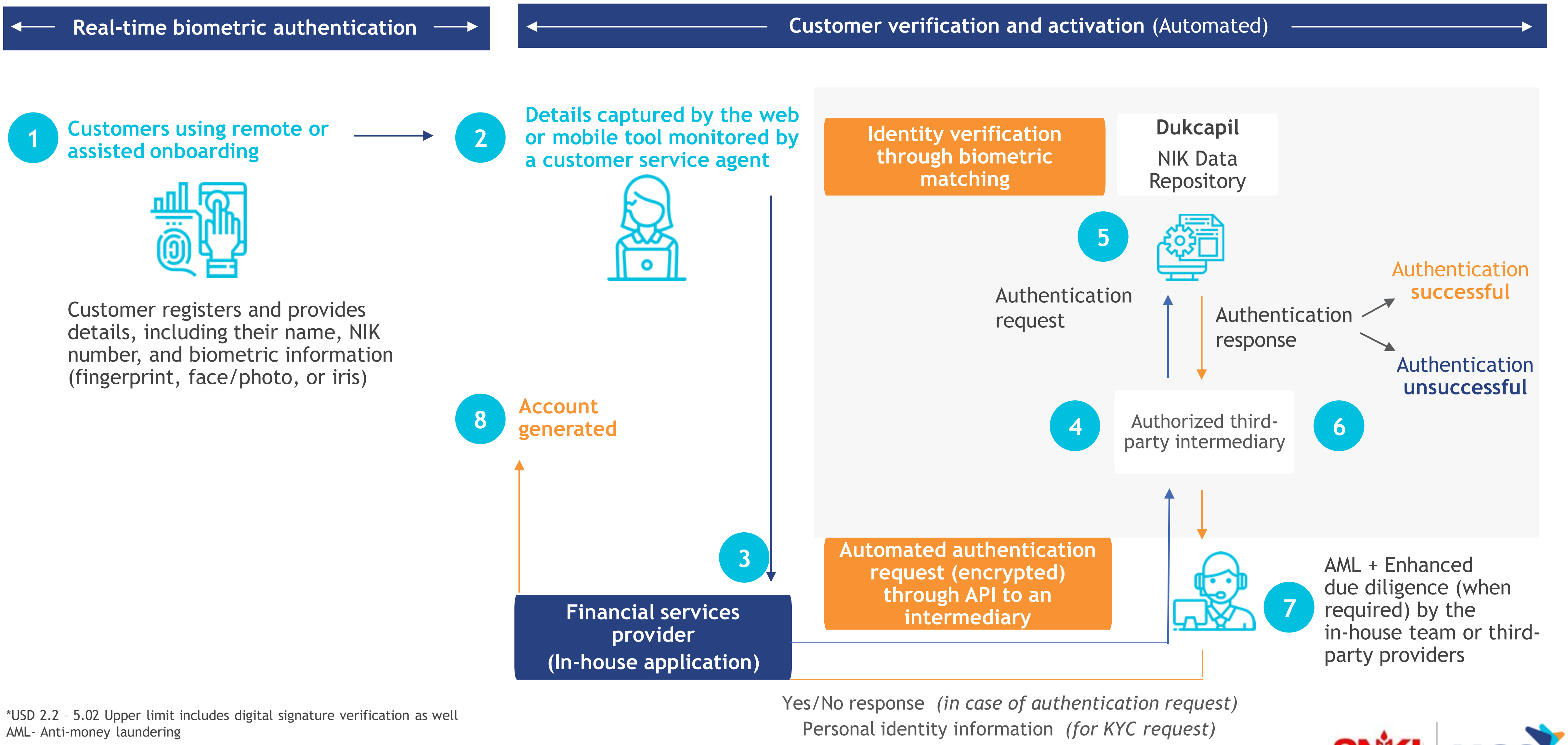
1 Purchases a product or service that requires identity verification

2 Requests authentication or KYC services provided by the authorized service agency

3 Sends the authorization/KYC request through approved specifications and protocols, receives a response and communicates it back securely to the user agencies

- 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



Real-time biometric authentication

Customer verification and activation (Automated)

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

3 Financial services provider (In-house application)

Automated authentication request (encrypted) through API to an intermediary

4 Authorized third-party intermediary

Authentication request

Authentication response

5 Identity verification through biometric matching

Dukcapil NIK Data Repository

6 Authentication successful

Authentication unsuccessful

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

8 Account generated

Yes/No response *(in case of authentication request)*

Personal identity information *(for KYC request)*

*USD 2.2 – 5.02 Upper limit includes digital signature verification as well

AML- Anti-money laundering

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.

Tentative cost (per request) for service providers (user agencies)

1. Simple Yes/No reply whether a match is found in the NIK database → **IDR 400-800 (USD 0.03-0.05)**
2. Confirmation of a match as well as viewing of demographic data and credentials for verification → **IDR 4,000-7,000 (USD 0.28-0.47)**

This is an estimation of the cost based on the willingness to pay of stakeholders, actual charges and real cost will differ based on government decisions during roll out.

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.

Country	Population (in million)	Model of pricing	Pricing of verification and identity services
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

Regulators

Areas of authorization

OTORITAS JASA KEUANGAN

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)

KEMKOMINFO

Draft Law on Personal Data Protection

The Draft law bestows several rights to financial service users for their personal data with some exceptions.

The users have right:

1. to delete, destroy, withdraw consent to process,

2. to choose or not to choose processing personal data through a pseudonymous mechanism for specific purposes,

3. to delay or limit processing of Data

4. to use and transmit data

SNKI MSC

Regulations for customer due diligence processes for BSA, P2P lending, and e-money accounts are regularly updated

Basic savings account

P2P

E-money

Customer acquisition

A customer needs to submit the following documents:

- Valid ID (e-KTP, passport, KITAS, etc.)
- Fill in data points
- Signature or fingerprint

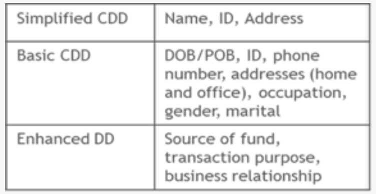
References:

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

Basic savings account

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:



Simplified CDD	Name, ID, Address
Basic CDD	DOB/POB, ID, phone number, addresses (home and office), occupation, gender, marital
Enhanced DD	Source of fund, transaction purpose, business relationship

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)

Basic savings account

1. All P2P electronic transactions must use an e-certificate from the licensed providers** (Law number 19 of 2016, Article 1 on electronic transactions)
2. All QR-based merchant payment must use QRIS (PADG 21/2019 article 6, 19/8/PBI/2017 article 28)

P2P/E-money

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

S. No.	KYC operational model	Service providers	Summary
1	Conventional branch-based model	Commercial banks	Customer walks into the service provider outlet, face-to-face interaction with service provider staff, physical checking of documentation
2	Agent-assisted model	Commercial banks with Laku Pandai agent networks	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
3	G2P model	Himbara banks	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
4	Mobile service provider staff using e-KTP readers	Commercial banks	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
5	Remote KYC using the service provider mobile app	FinTechs (e-money, P2P players)	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

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:

	PrivyID	Verijelas	ASLI RI	Nodeflux
MoU signed with Dukcapil	29th March, 2019	13th December, 2019	1st January, 2020	1st January, 2020
Types of access granted	NIK database	NIK database, e-KTP photo data	NIK database (some news also mentioning about biometric access as well)	NIK database and e-KTP photo to support police' face search system

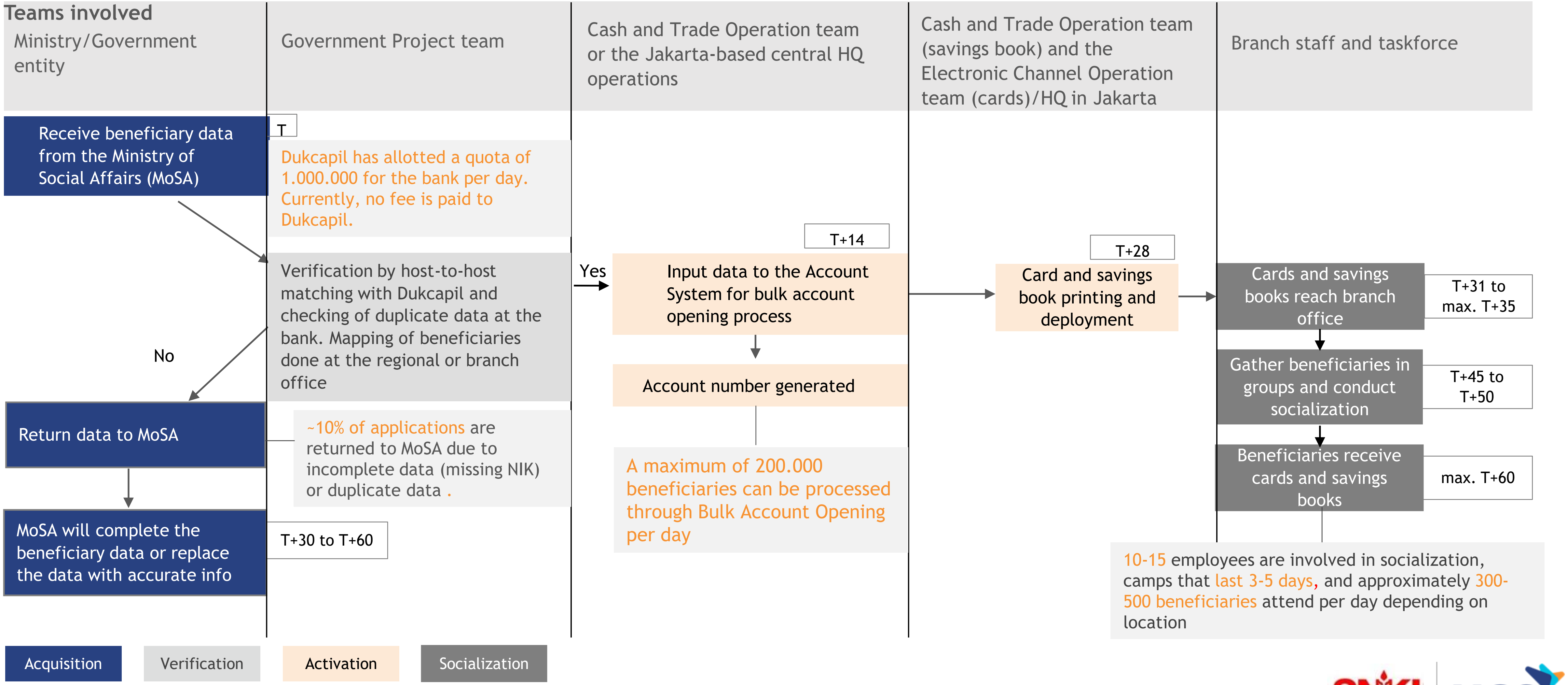
To gain the "right to access," industry players must pass all terms and procedures set by MoHA. They must also fulfill some legal requirements* and obtain recommendation from an authority, such as OJK.

*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

Banks	E-money players	P2P lenders
Customers Process and cost for opening a basic savings account, including under G2P programs, such as PKH	**Customer** Process and cost for signing up customers for a registered e-money account	**Borrower** Process and cost for onboarding individual borrowers on the platform
Agents Process and cost for onboarding BSA customers through Laku Pandai agents and bank branches	**Small merchants** Process and cost for onboarding QRIS merchants	**Lenders** Process and cost for onboarding individual retail lenders on the platform

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)

T

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

No

Return data to MoSA

~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

T+30 to T+60

Yes

T+14

Input data to the Account System for bulk account opening process

Account number generated

A maximum of 200.000 beneficiaries can be processed through Bulk Account Opening per day

T+28

Card and savings book printing and deployment

Cards and savings books reach branch office

T+31 to max. T+35

Gather beneficiaries in groups and conduct socialization

T+45 to T+50

Beneficiaries receive cards and savings books

max. 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

Acquisition

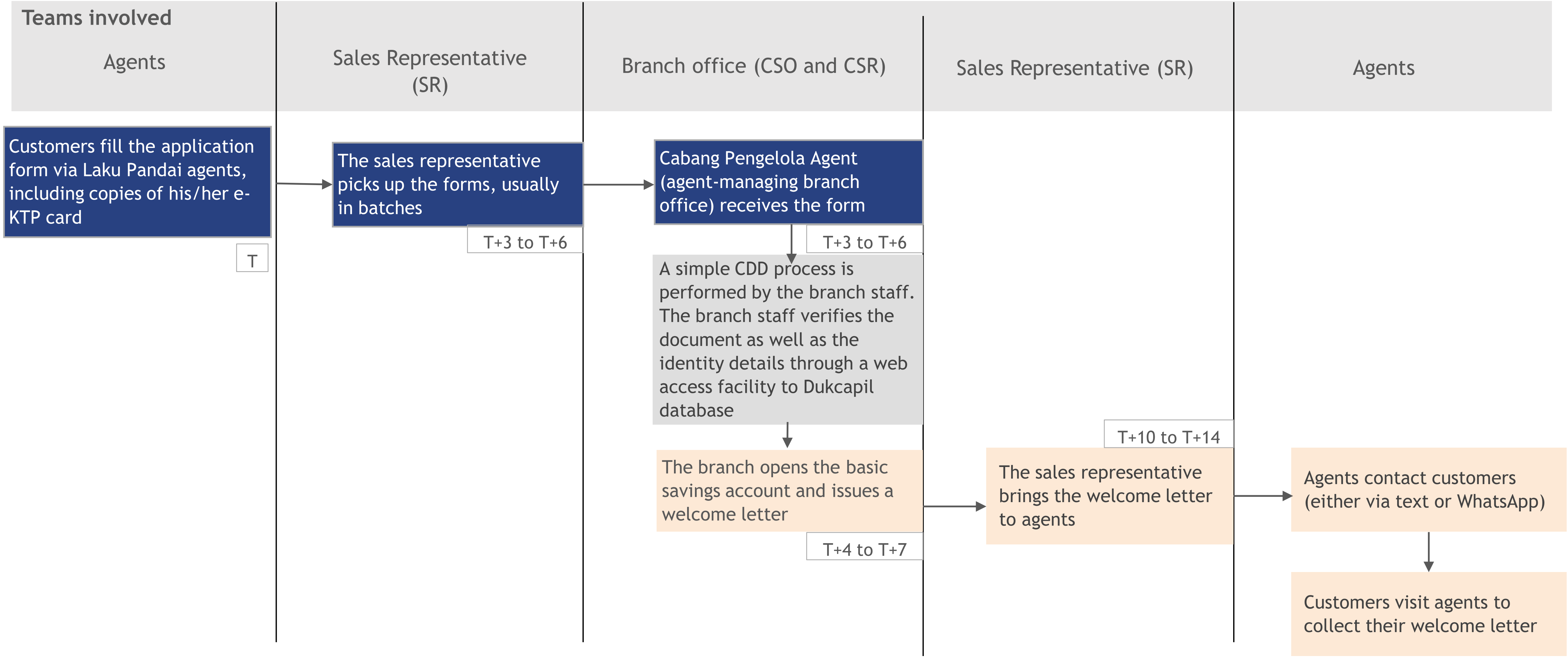
Verification

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

T

Sales Representative (SR)

The sales representative picks up the forms, usually in batches

T+3 to T+6

Branch office (CSO and CSR)

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

T+3 to T+6

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

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

T+4 to T+7

Sales Representative (SR)

T+10 to T+14

The sales representative brings the welcome letter to agents

Agents

Agents contact customers (either via text or WhatsApp)

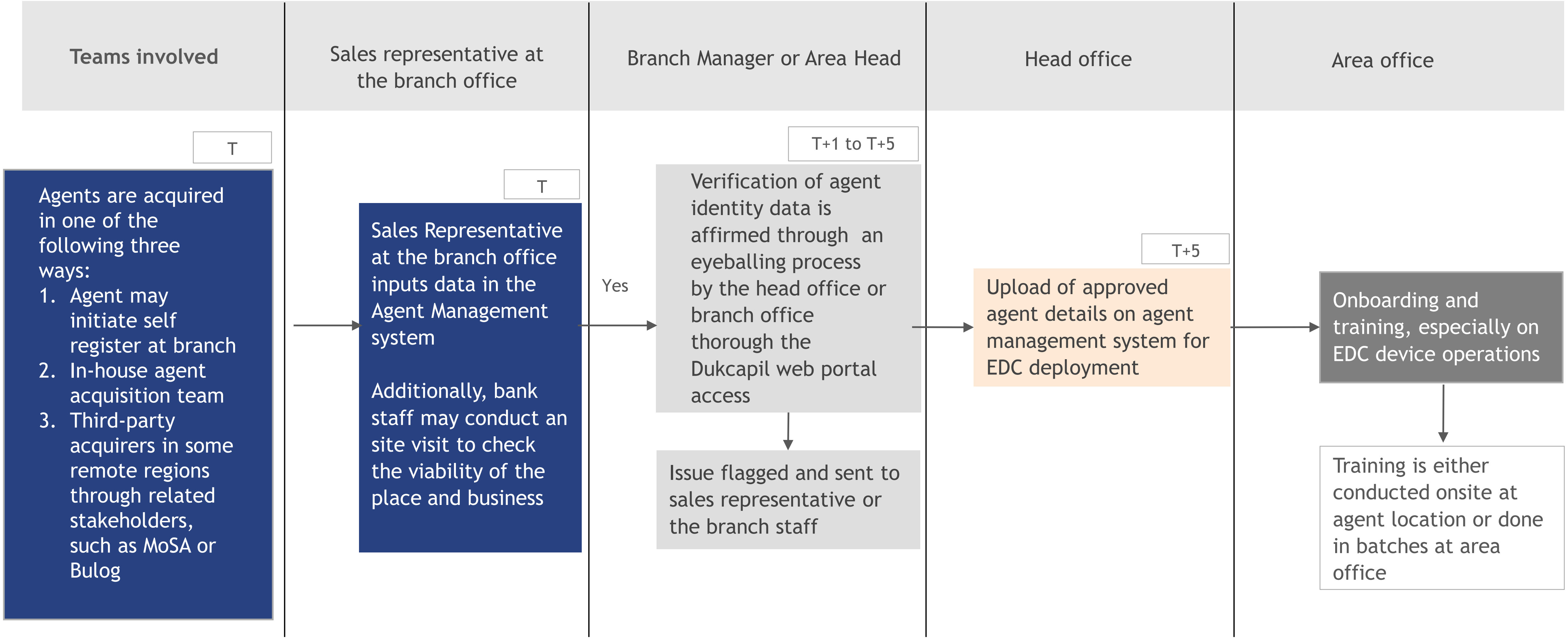
Customers visit agents to collect their welcome letter

Acquisition | Verification | Activation

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



Teams involved

Sales representative at the branch office

Branch Manager or Area Head

Head office

Area office

T

Agents are acquired in one of the following three ways:

1. Agent may initiate self register at branch
2. In-house agent acquisition team
3. Third-party acquirers in some remote regions through related stakeholders, such as MoSA or Bulog

T

Sales Representative at the branch office inputs data in the Agent Management system

Additionally, bank staff may conduct an site visit to check the viability of the place and business

Yes

T+1 to T+5

Verification of agent identity data is affirmed through an eyeballing process by the head office or branch office thorough the Dukcapil web portal access

Issue flagged and sent to sales representative or the branch staff

T+5

Upload of approved agent details on agent management system for EDC deployment

Onboarding and training, especially on EDC device operations

Training is either conducted onsite at agent location or done in batches at area office

Acquisition

Verification

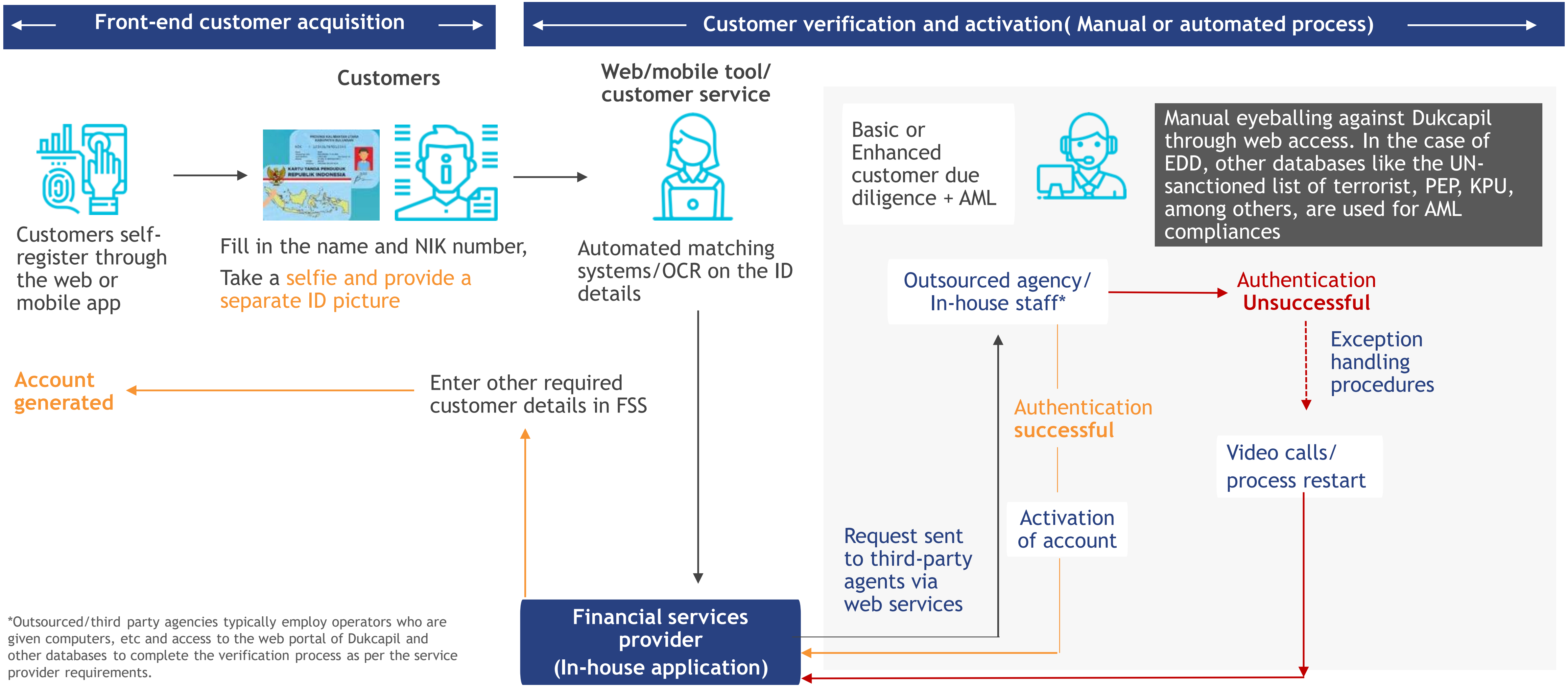
Activation

Socialization

Details of existing onboarding processes for customers and merchants

Banks	E-money players	P2P lenders
Customers Process and cost for opening a basic savings account, including under G2P programs, such as PKH and BPNT	**Customer** Process and cost for signing up customers for a registered e-money account	**Borrower** Process and cost for onboarding individual borrowers on the platform
Agents Process and cost for onboarding BSA customers through Laku Pandai agents and bank branches	**Small merchants** Process and cost for onboarding QRIS merchants	**Lenders** Process and cost for onboarding individual retail lenders on the platform

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

Customer verification and activation(Manual or automated process)

Customers

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

Web/mobile tool/ customer service

Automated matching systems/OCR on the ID details

Financial services provider (In-house application)

Request sent to third-party agents via web services

Basic or Enhanced customer due diligence + AML

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

Outsourced agency/ In-house staff*

Authentication successful

Activation of account

Authentication Unsuccessful

Exception handling procedures

Video calls/ process restart

Enter other required customer details in FSS

Account generated

*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

Acquisition

T

Self-initiated process

Step 1. Sign up

Customers sign up via the service provider mobile application

Step 2. Fill up the registration form

Customers fill basic details into the form on the app

Step 3. Upload the required documents

Customers need to upload pictures of e-KTP and a selfie of themselves holding the e-KTP card

Verification

Manual and automated data verification

Step 4. Identity verification

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.

Step 5. Automated in-house EDD and AML

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.

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. Customers receive a notification on successful activation

The customers get a notification through SMS.

Storage

T+1 to 2 days

Customer data is stored as per regulation

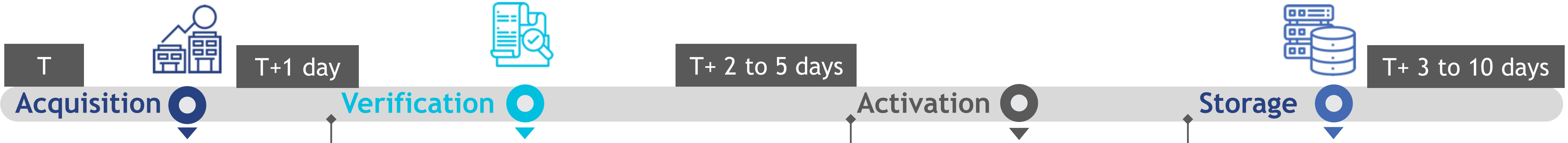
Step 8. Data storage on the server and cloud

Some players use third-party services while some use their own.

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

OCR: Optical character recognition

To open a merchant account, the business owner first needs to complete their KYC followed by the business verification process



Third-party acquirers

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.

Manual and automated data verification

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.

QRIS registration and automatic activation

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.

Customer data is stored as per regulation

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.

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

	Customers			Merchants		
		Teams involved (Team size)	Avg. applications per day		Teams involved (Team size)	Avg. applications per day
Acquisition		Self-initiated process	5,000-25,000	Option 1	In-house customer service (100) and outsourced	1,000-10,000
				Option 2	Outsourced to vendor	500 - 1,000
Verification	Option 1	Outsourced service provider	4,000-5,000	Option 1	In-house teams: Business user (5), Commerce (5), Operations (10)	300
		30% rejected due to blurry or mismatched pictures			2.5% rejected due to e-KTP issue or duplicate merchant name	
	Option 2	In-house automated system for Dukcapil matching		Option 2	Outsourced field team	
		60% rejected due to blurry pictures or mismatched names			30% rejected** due to blurry pictures	
	Option 3	In-house AML analysts (5) and outsourced KYC agents (100)				
		Reasons for rejections are mainly blurry pictures, wet KTP, and suspected fraud*				
Activation		Automated			In-house Operations team, service provider (Switcher and PTEN)	

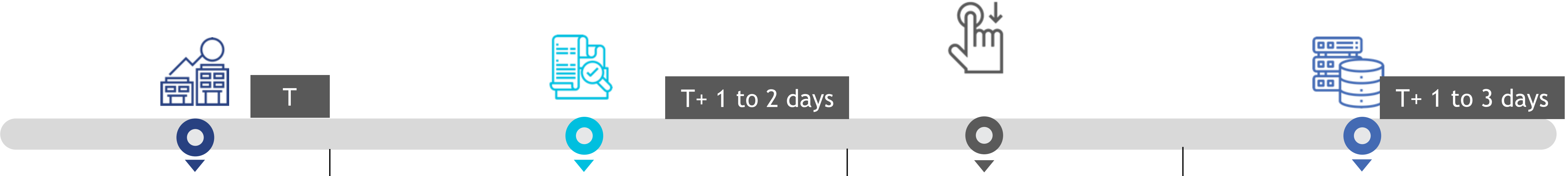
*Fraud: Abusing cashback offers

**Rejections do not include merchants rejected due to discrepancies found during onsite visits

Details of existing onboarding processes for borrowers and lenders

Banks	E-money players	P2P lenders
Customers Process and cost for opening a basic savings account, including under G2P programs, such as PKH and BPNT	**Customer** Process and cost for signing up customers for a registered e-money account	**Borrower** Process and cost for onboarding individual borrowers on the platform
Agents Process and cost for onboarding BSA customers through Laku Pandai agents and bank branches	**Small merchants** Process and cost for onboarding QRIS merchants	**Lenders** Process and cost for onboarding individual retail lenders on the platform

Borrowers on P2P platforms are acquired through multiple channel and require a valid NIK number to begin on boarding process



Acquisition

Self-initiated 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)

Verification

Manual and automated data verification

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.

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. Borrowers get a notification on successful activation

Service providers notify lenders through an email and/or service provider mobile application

Storage

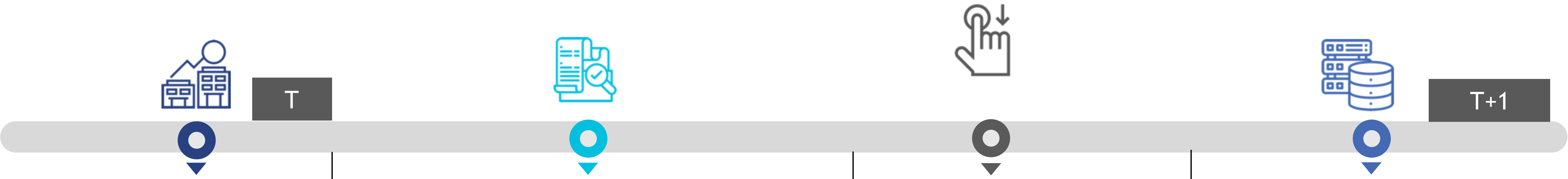
Customer data is stored as per regulation

Step 8. Data storage on the server and cloud

Some players use third-party services while some use their own.

The 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.

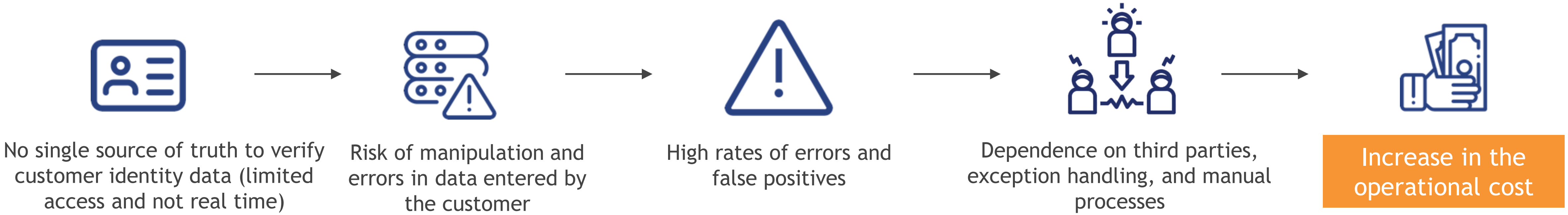
The KYC process is handled by in-house teams or outsourced to service providers and the productivity varies depending on the type of P2P lender

		Institutional lending player 1		Retail lending player 1		Retail lending player 2	
		Teams involved (Team size)	Avg applications per day	Teams involved (Team size)	Avg applications per day	Teams involved (Team size)	Avg applications per day
Acquisition	Lenders	Self-initiated process	20-30			Self-initiated process	500-700
	Borrowers	Self-initiated process	27	Self-initiated process	4,000 - 5,000	Self-initiated process through e-commerce partner	2,400
Verification	Lenders	Outsourced to service provider (SP) and in-house customer service (2)				In-house quality assurance (1), customer service (2), marketing (80), and outsourced SP 56% rejected due to blurry or invalid KTP	
	Borrowers	Outsourced SP and in-house credit risk team (15) 60% rejected due to low credit score	300	Outsourced to SP and in-house AI application 20-25% rejected due to low credit score		Outsourced quality assurance (1) 20% rejected due to blurry KTP, invalid social profile account, or duplicate account	
Activation	Lenders	Outsourced to service provider for digital signature				Partnership with banks for virtual account opening	
	Borrowers	Outsourced to SP for digital signature and credit bureau		Outsourced to SP for digital signature and the Operations team for exception handling 22-30% cases for exception handling due to delayed response			

Lenders Borrowers

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)

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

Key issues in merchant (business entity) KYC

Multiple NMID and QRIS	Bank account verification	Business verification
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.	Most players do not verify bank account details. Some use the services of a switching agent to verify and match the name.	Currently, no standards are set for business verification. The data points checked across players are different.

*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

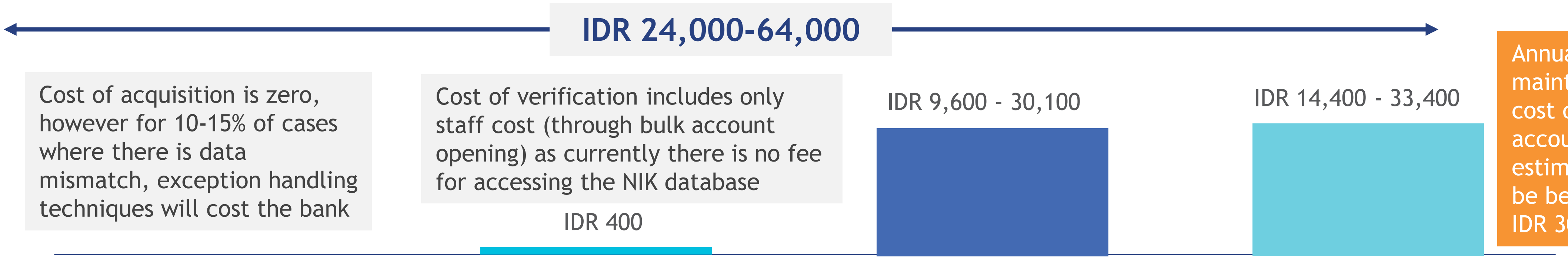
1. Social assistance program delivery (G2P)
2. Agent (Laku Pandai) assisted customer onboarding
3. Agent onboarding

Bionta Paling ciiiir !!
"Membangun Pabrik Pupuk Di Dalam Tanah"
Produknya Baik, Hasilnya Naik
APONG
EDAH
MAS
YAMAHA

Banks - Social assistance program delivery (G2P)

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

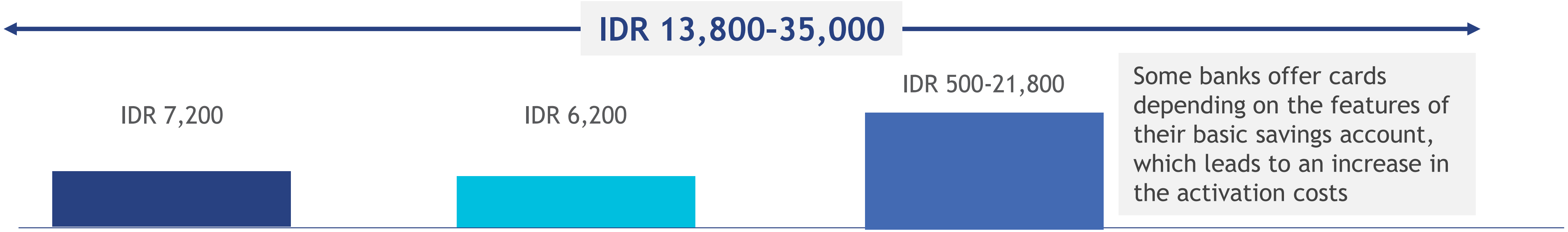
Annual maintenance cost of the account is estimated to be between IDR 30-50k

	Acquisition		Verification		Activation		Socialization	
Costing details	Particulars	Amount	Particulars	Amount	Particulars	Amount	Particulars	Amount
	Beneficiary data shared by the government stakeholder (MoSA)		Verification cost	N/A	Staff costs	6,000-8,000	Staff costs	12,400
			Staff costs	400	Printing costs*	2,750-21,300	Marketing and communication	2,000-21,000
					Courier costs	800		
			Total	IDR 400	Total	IDR 9,600-30,100	Total	IDR 14,400-33,400

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

The highest amount is spent on the verification of basic savings account holders

Costs incurred per BSA customer throughout the process

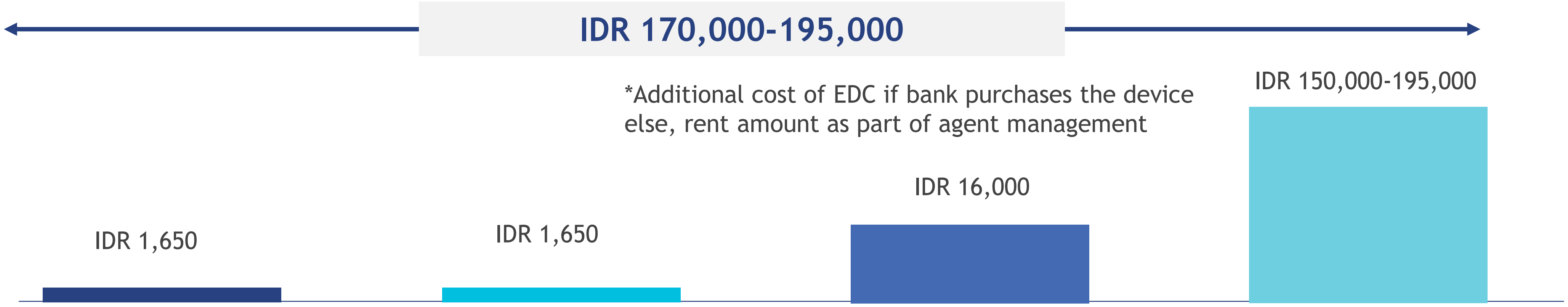


Some banks offer cards depending on the features of their basic savings account, which leads to an increase in the activation costs

	Acquisition		Verification		Activation		Socialization	
Costing details	Particulars	Amount	Particulars	Amount	Particulars	Amount	Particulars	Amount
	Application form	500	Staff costs (face-to-face verification)	6,200	Welcome letter	500	Annual maintenance cost is estimated to be between IDR 30-50k	
	Staff costs	1,650			Printing costs for cards*	2,750-21,300		
	Agent commission	4,000-5,000						
	Total	**IDR 7,200**	**Total**	**IDR 6,200**	**Total**	**IDR 500-21,800**		

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



*Additional cost of EDC if bank purchases the device else, rent amount as part of agent management

	Acquisition		Verification		Activation		Socialization	
	Particulars	**Amount**	**Particulars**	**Amount**	**Particulars**	**Amount**	**Particulars**	**Amount**
Costing details	Staff costs	1,650	Staff costs	1,650	Courier charges for deploying EDC machines	16,000	Training cost	IDR 100,000-125,000
					EDC machines*	3,000,000	Marketing material	IDR 50,000-70,000
							Agent support	TBD
	Total	**IDR 1,650**	**Total**	**IDR 6,186**	**Total**	**IDR 16,000**	Total	**IDR 150,000-195,000**

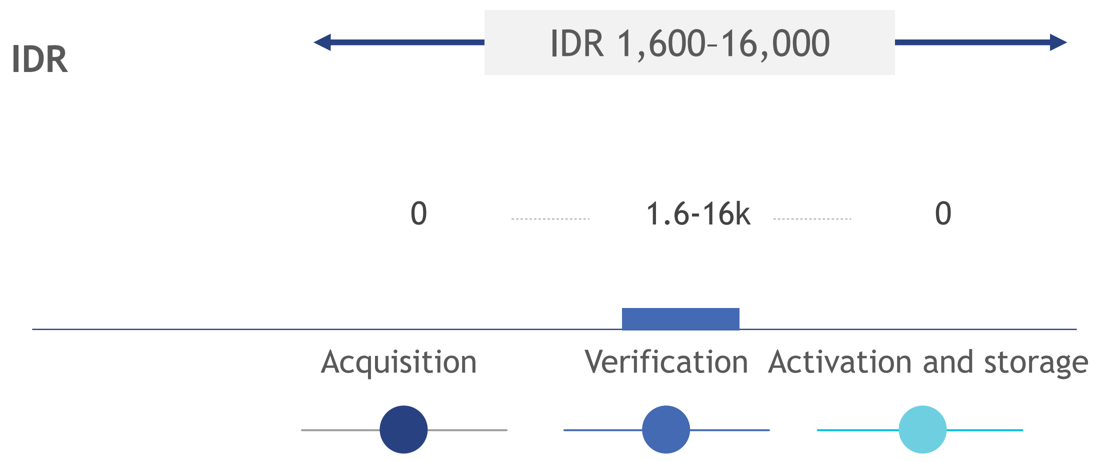
Note: Staff costs calculated as per time taken to complete process and average salary depending on team locations

FinTechs

1. Customer and merchant onboarding for e-money players
2. Lender and borrower onboarding for P2P players

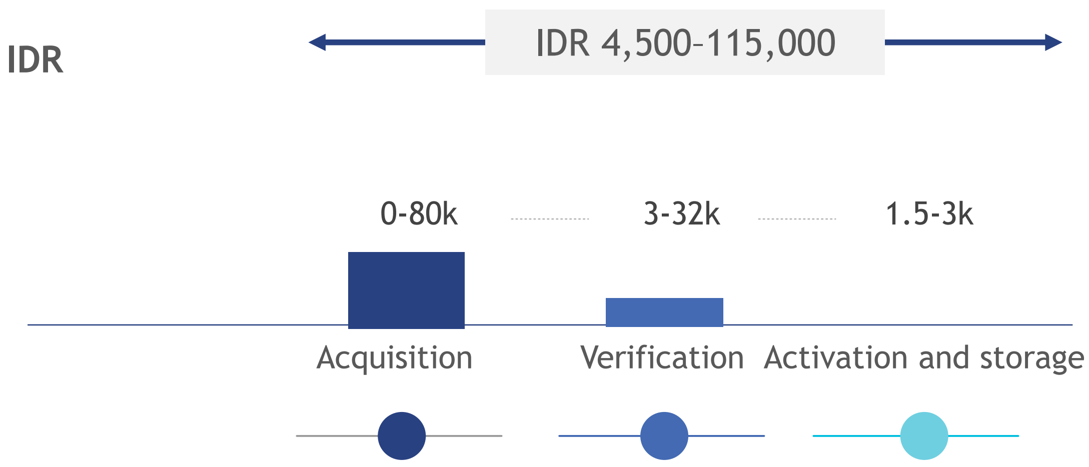
While verification contributes significantly to the overall costs for onboarding e-money customers, merchant acquisition can be a substantial cost if third-party acquirers are used

E-money customer



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

E-money merchant

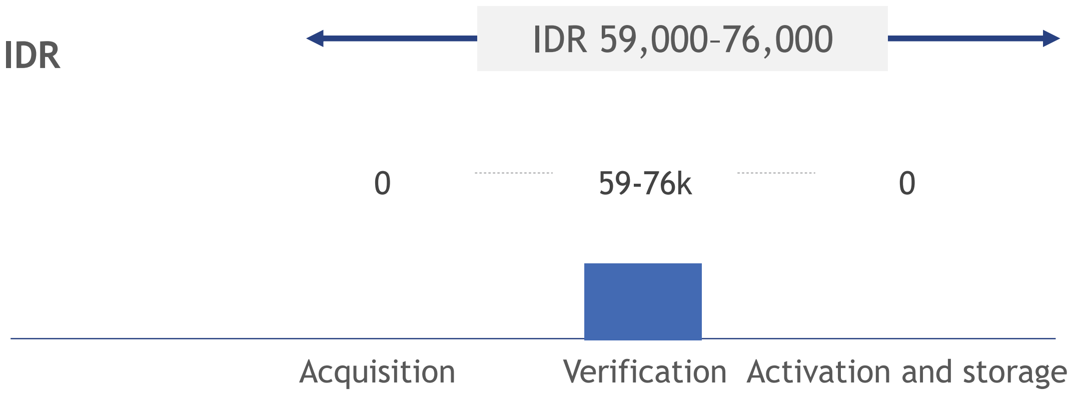


Cost drivers:	High costs due to third-party agencies with on-the-ground field teams while other merchants self-initiate onboarding through the app	Range due to in-house automated verifications compared to outsourced providers	Activation includes bank account check through switchers

Costing estimates do not include digital marketing costs

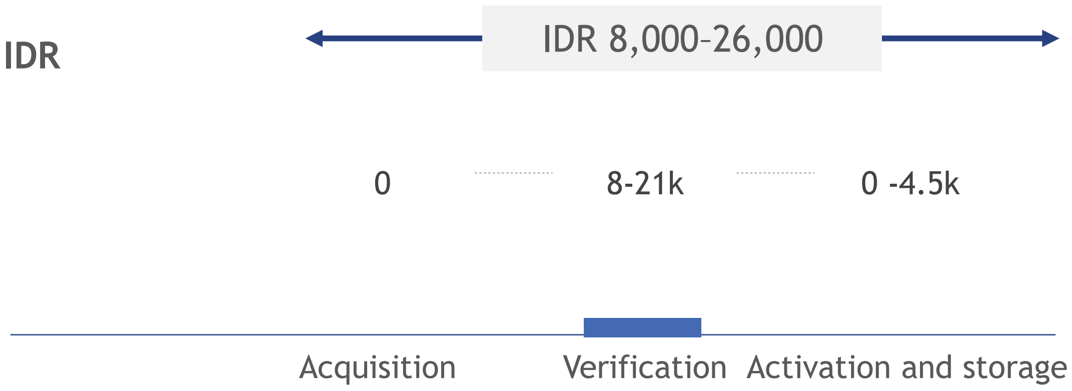
Verification is the highest contributor to the operational costs of onboarding a customer to a P2P platform

P2P lenders



Cost drivers:	Self-initiated process on the app	Third-party agent costs including enhanced due diligence and digital signature verification	Automatic system activation and in-house storage

P2P borrowers



Cost drivers:	Self-initiated process on the app	Third-party agent costs	Automatic system activation and in-house storage

Costing estimates do not include digital marketing costs

Bionta Paling ciiiir !!
"Membangun Pabrik Pupuk Di Dalam Tanah"
Produknya Baik, Hasilnya Naik

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

Bionta Paling ciiiir !!
"Membangun Pabrik Pupuk Di Dalam Tanah"
Produknya Baik, Hasilnya Naik
ARONG

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

Account opening

- 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.

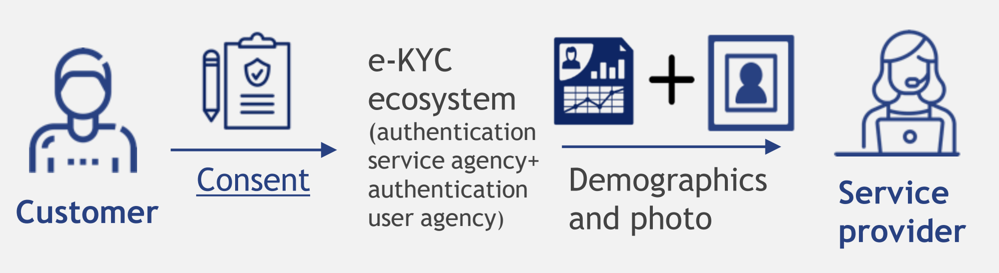
Customer due diligence

- CDD 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.**

Transaction authentication

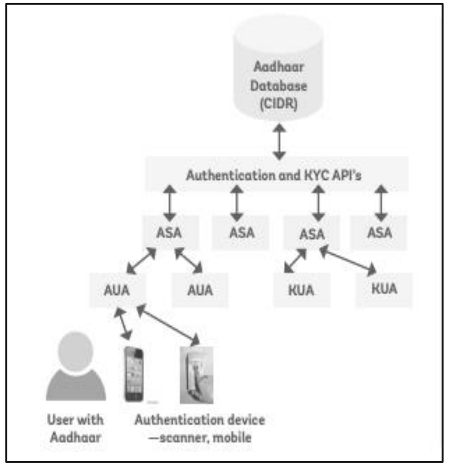
- **An OTP** with a limited time validity is sent to the mobile number, e-mail address, or both of the *Aadhaar* number holder registered with the Authority. The *Aadhaar* number holder provides this OTP along with his *Aadhaar* number during authentication, which is then matched with the OTP generated by the Authority.
- Fingerprint-based or iris-based authentication or other biometric modalities are based on biometric information stored in the CIDR.

CIDR- Central Identities Data Repository
https://rbidocs.rbi.org.in/rdocs/notification/PDFs/NOTI190B865EC9E06464105A4A9318119A7455B.PDF


Customer
Consent
e-KYC ecosystem (authentication service agency+ authentication user agency)
Demographics and photo
Service provider

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.

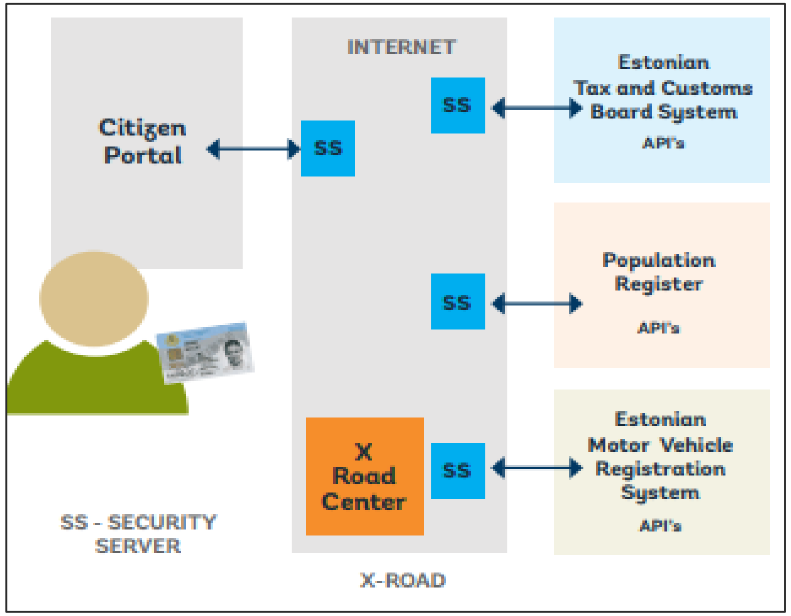

Aadhaar Database (CIDR)
Authentication and KYC API's
ASA
ASA
ASA
ASA
AUA
AUA
KUA
KUA
User with Aadhaar
Authentication device —scanner, mobile

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.

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

Account opening	Customer due diligence	Transaction authentication
• Opening a **bank account online** is possible using **e-ID or e-Residency card**, a video interview recording, and **facial recognition technology.** • 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.	• The eID provides full legal status for any interaction in Estonia that requires identity confirmation, such as e-commerce, electronic banking, and signing contracts. • Estonian residents **willingly allow** government entities and service providers to use their digital identity information in exchange for trusted and high-quality services.	• 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. • To read the records, the terminal has to send several Application Protocol Data Unit (APDU) commands to the smart card and read the responses. • To identify the cardholder, the personal ID code is the best option as it does not change during the cardholder's lifetime.



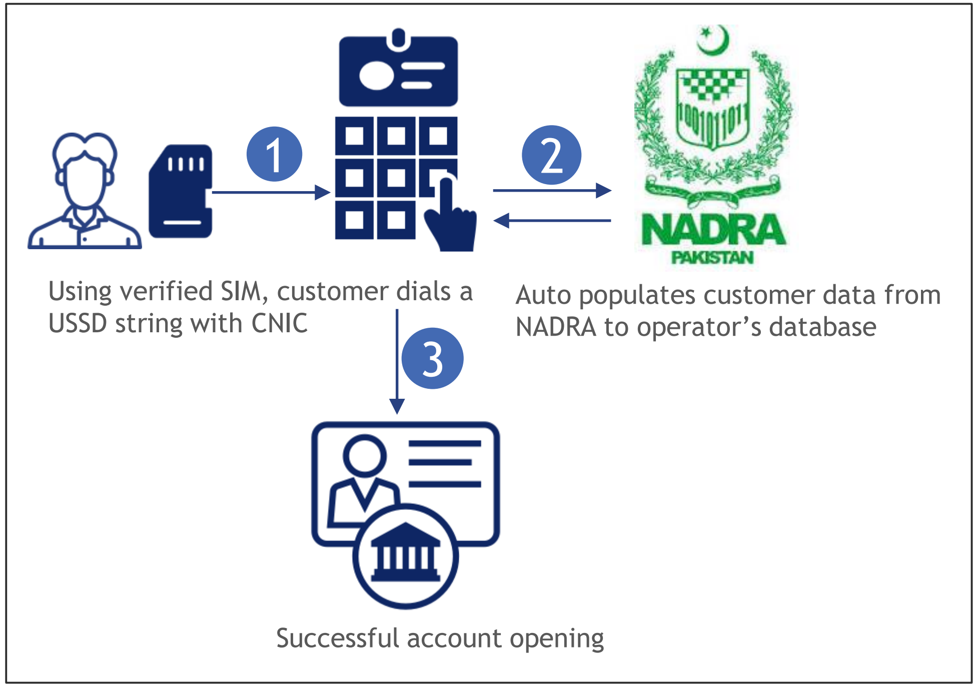
Data exchange platform for e-Estonia

- 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.
- Any institution can use the public key infrastructure.

https://eprint.iacr.org/2017/880.pdf

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

Account opening	Customer due diligence	Transaction authentication
• 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. • The national ID cards allowed opening of bank accounts and reliable enforcement of transaction limits, which enabled the growth of branchless banking agents	• NADRA data is used to verify the identity of individuals for both **bank account opening and mandatory mobile SIM card registration**. • NADRA provides an online verification system where, for a fee, FSPs can verify the identity of a customer.	• NADRA has facilitated different stakeholders like **banks, mobile operators**, and other companies through biometric verification. • This facility includes the following: • Secure verification service for third-party service providers • Integration with telcos, banks, e-Sahulat, security companies, etc. • Real-time fingerprint verification



Using verified SIM, customer dials a USSD string with CNIC

Auto populates customer data from NADRA to operator's database

Successful account opening

Account opening process using NADRA's CNIC

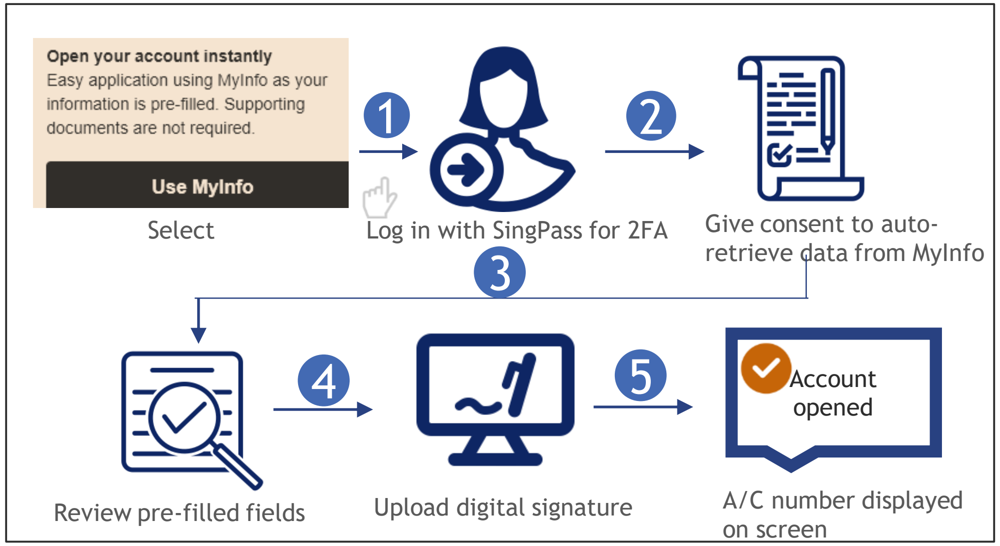
NADRA has developed its own financial service solutions designed to provide the following services:

- Utility bill payment or collection
- Billing gateway
- Mobile banking
- Secure remittance platforms
- Electronic point of sales solutions

https://www.nadra.gov.pk/services/financial-service-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	Customer due diligence	Transaction authentication
• Logging in using their SingPass, customers consent to the bank using their **My Info 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.	• 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.	• **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.



Open your account instantly

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

Use MyInfo

Select
1
Log in with SingPass for 2FA
2
Give consent to auto-retrieve data from MyInfo
3
Review pre-filled fields
4
Upload digital signature
5
Account opened
A/C number displayed on screen

Digital account opening process using SingPass

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.

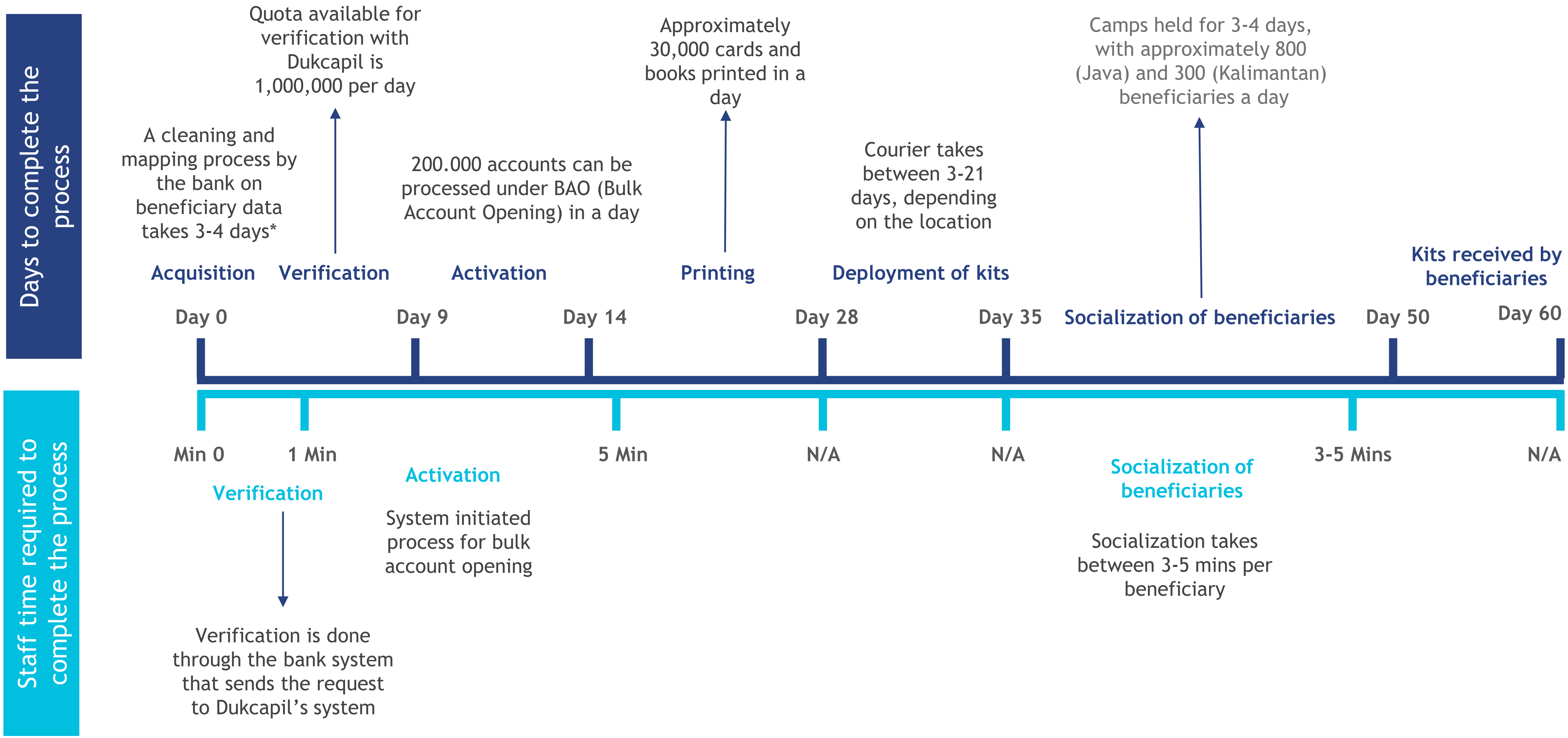
- It is a easy and secure gateway to hundreds of government digital services and some from private sectors.
- It can be used to check the balance of CPF (pension fund), file tax returns, view personal information, and receive notification from government agencies.

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



Days to complete the process

Acquisition – Day 0: A cleaning and mapping process by the bank on beneficiary data takes 3-4 days*

Verification: Quota available for verification with Dukcapil is 1,000,000 per day

Day 9

Activation: 200.000 accounts can be processed under BAO (Bulk Account Opening) in a day

Day 14

Printing: Approximately 30,000 cards and books printed in a day

Day 28

Deployment of kits: Courier takes between 3-21 days, depending on the location

Day 35

Socialization of beneficiaries: Camps held for 3-4 days, with approximately 800 (Java) and 300 (Kalimantan) beneficiaries a day

Day 50

Kits received by beneficiaries – Day 60

Staff time required to complete the process

Min 0

1 Min – Verification: Verification is done through the bank system that sends the request to Dukcapil's system

Activation: System initiated process for bulk account opening

5 Min

N/A

N/A

Socialization of beneficiaries: Socialization takes between 3-5 mins per beneficiary

3-5 Mins

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

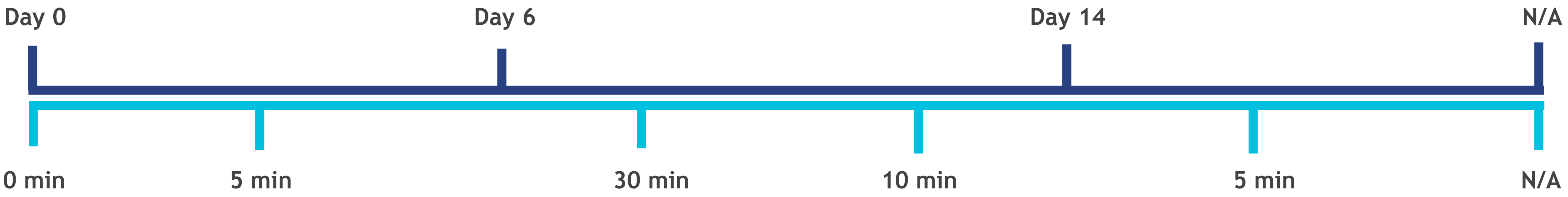
Days to complete the process

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.

Acquisition | **Verification** | **Activation** | **Deployment of kits** | **Kits received by customers**



Staff time required to complete the process

Acquisition | **Verification** | **Activation** | **Deployment of kits**

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.

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.

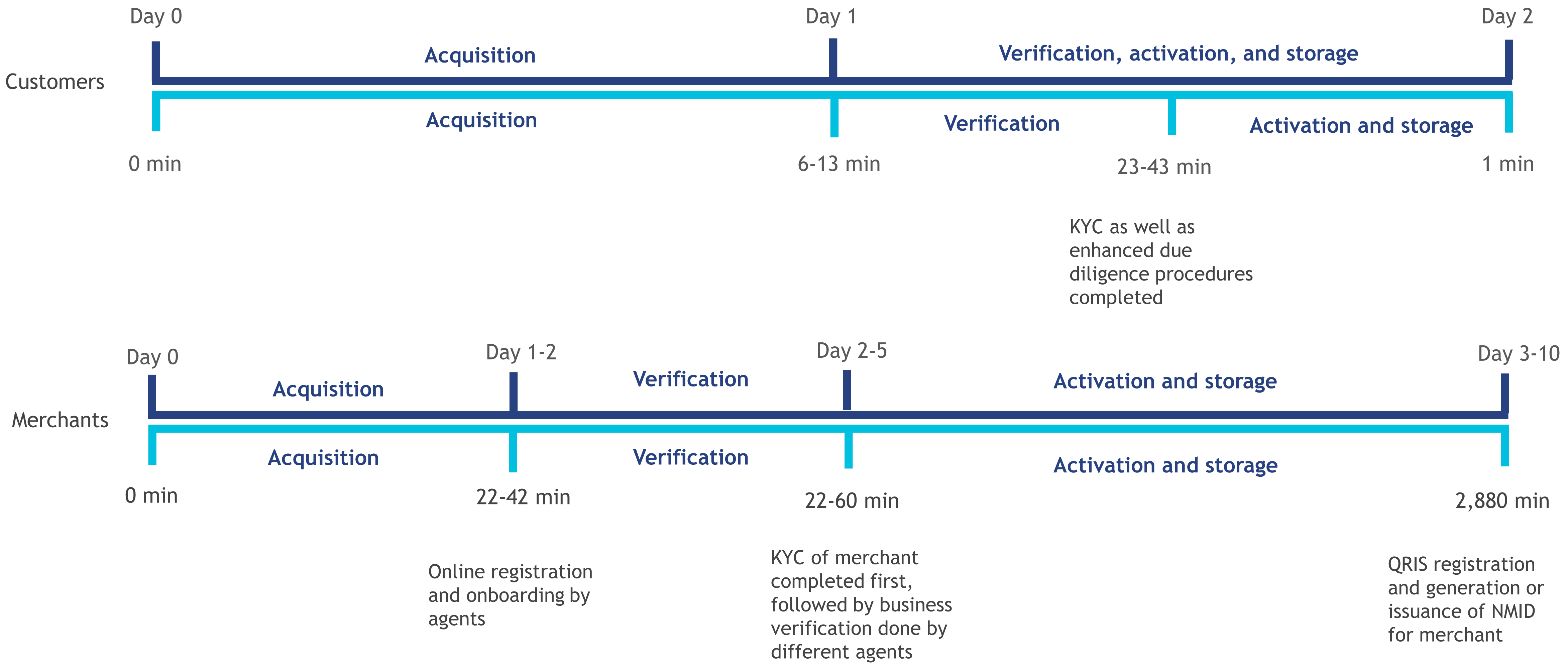
Staff at the branch is in charge of account activation

Since SRs are required to visit agents once a week, a week-long time lag is possible

E-money - Customers and merchants

Activation and setting up of accounts for merchants consumes the longest time on E-money platforms

E-money players



Customers

Day 0 — Acquisition — Day 1 — Verification, activation, and storage — Day 2

Acquisition — Verification — Activation and storage

0 min — 6-13 min — 23-43 min — 1 min

KYC as well as enhanced due diligence procedures completed

Merchants

Day 0 — Acquisition — Day 1-2 — Verification — Day 2-5 — Activation and storage — Day 3-10

Acquisition — Verification — Activation and storage

0 min — 22-42 min — 22-60 min — 2,880 min

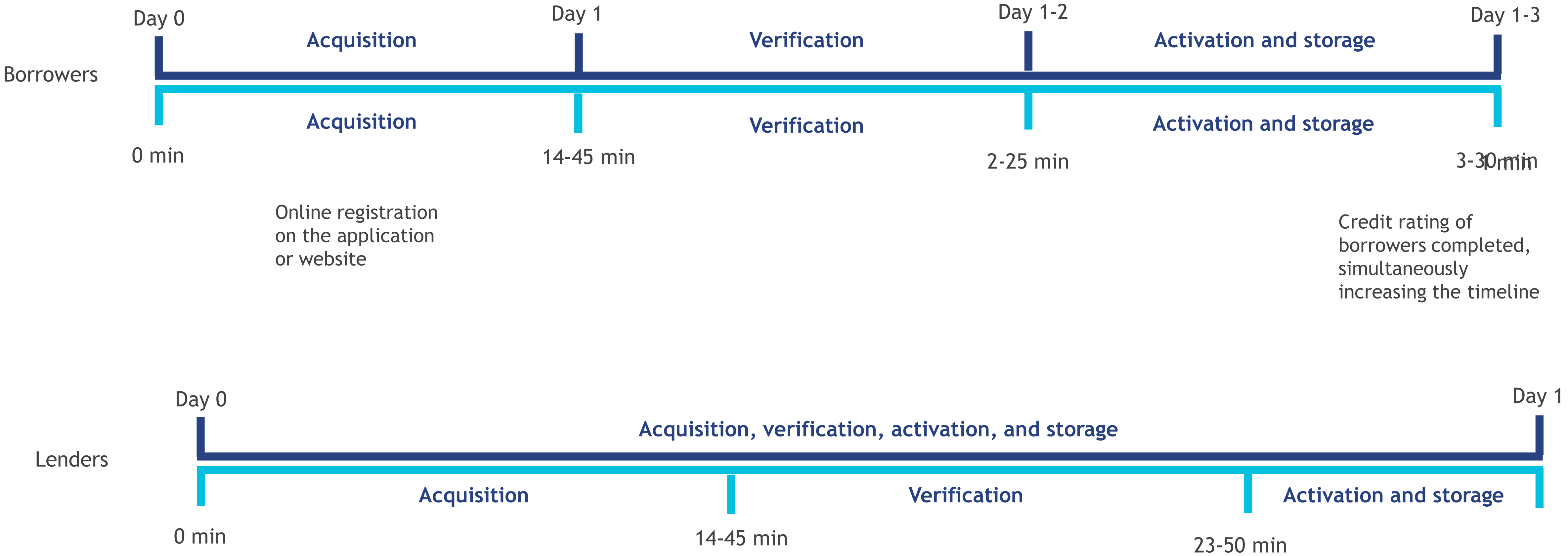
Online registration and onboarding by agents

KYC of merchant completed first, followed by business verification done by different agents

QRIS registration and generation or issuance of NMID for merchant

Whereas the entire process is fairly quick for P2P players and is usually completed within a day

P2P players



Borrowers

Day 0

Day 1

Day 1-2

Day 1-3

Acquisition

Verification

Activation and storage

Acquisition

Verification

Activation and storage

0 min

14-45 min

2-25 min

3-30 min

1 min

Online registration
on the application
or website

Credit rating of
borrowers completed,
simultaneously
increasing the timeline

Lenders

Day 0

Day 1

Acquisition, verification, activation, and storage

Acquisition

Verification

Activation and storage

0 min

14-45 min

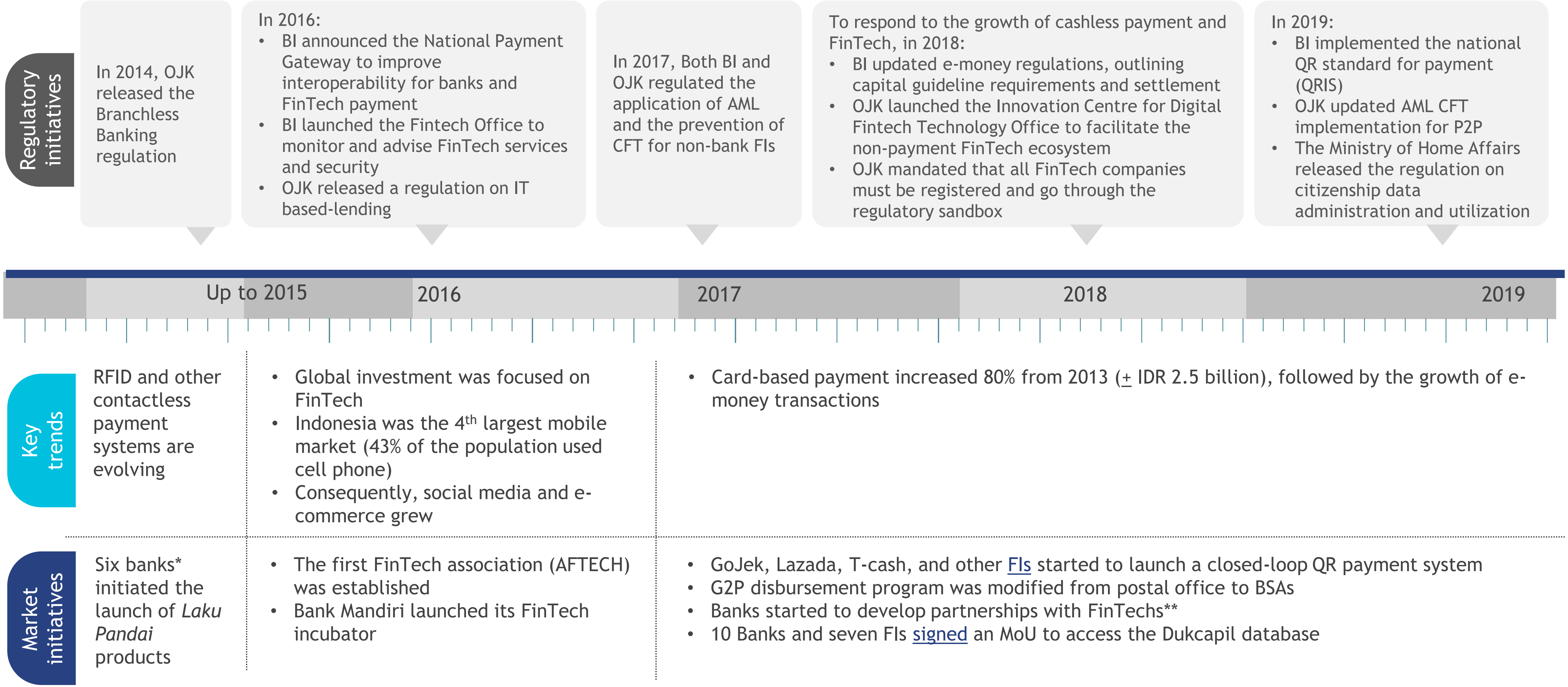
23-50 min

Slight increase in time
due to digital signature
verification

P2P - Borrowers and lenders

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

Up to 2015

In 2014, OJK released the Branchless Banking regulation

2016

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

2017

In 2017, Both BI and OJK regulated the application of AML and the prevention of CFT for non-bank FIs

2018

To respond to the growth of cashless payment and FinTech, in 2018:
- BI updated e-money regulations, outlining capital guideline requirements and settlement
- OJK launched 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

2019

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

2017–2019

- Card-based payment increased 80% from 2013 (± IDR 2.5 billion), followed by the growth of e-money transactions

Market initiatives

Up to 2015

Six banks* initiated the launch of *Laku Pandai* products

2016

- The first FinTech association (AFTECH) was established
- Bank Mandiri launched its FinTech incubator

2017–2019

- 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

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

Data points used in the model	Value
Current number of customers: a) E-money b) P2P	125 million 16.4 million
Growth rate for the e-money sector Assumed mean revert rate	15% for 5 years 5%
Growth rate for the P2P sector Assumed mean revert rate	10% for 5 years 2%
Population growth	1.01%
Interest-free rate used for present value calculations (across all years)	6.73%

Comparison of different technologies for biometric authentication (1/2)

Parameters	Fingerprint authentication	Iris recognition	Facial recognition
Engagement	Contact-based	Contactless	Contactless
Accuracy	Moderate	High	Low
Performance	High	High	Moderate
1. False acceptance rate (unauthorized people are accepted incorrectly)	Low (0.01%)	Lowest (0. 0001%)	High (0.2%)
2. False rejection rate (authorized people are rejected incorrectly)	High (2-3% for one finger, 0.09% for 10 fingers) (Age can affect results)	Low (0.0%) (Possible in bright sunlight/subject wearing glasses or lenses)	Moderate (Less than 0.1%) (Different rates for different demographic groups)*
Cost	Relatively Inexpensive	Expensive	Relatively Inexpensive
Usability	Easy	Moderate	Easy
Scalability (depending on the tech and type of matching)	High (approximately a billion matches per second)	High (matching rate of approximately 200,000 templates per second)	Low
Security	Low	High	Moderate
Technology challenges	Struggles to capture damaged prints	Requires highly specific positioning of the subject	Variable capture conditions
Resistance to circumvention	Low (Easy to spoof)	High (Very difficult to spoof)	Moderate (Easy to spoof)

Sources: 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

Comparison of different technologies for biometric authentication (2/2)

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

Sources: 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

>850 publications

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

Implemented >850 DFS projects

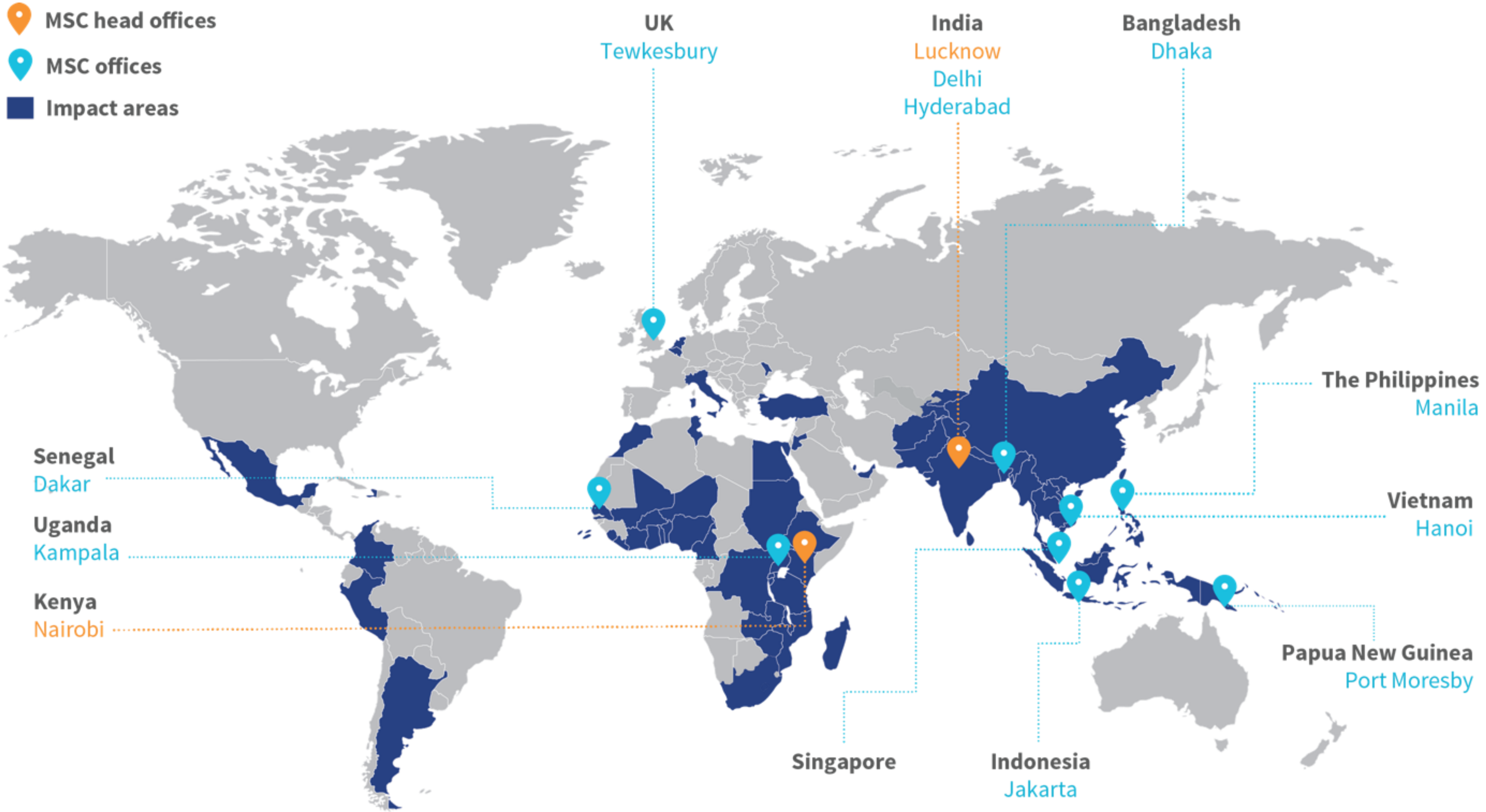
Developed 275+ FI products and channels now used by 55 million+ people

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 WORLD BANK GROUP
UN CDF
USAID FROM THE AMERICAN PEOPLE
WORLD BANK GROUP
CGAP
OMIDYAR NETWORK
ADB ASIAN DEVELOPMENT BANK
NPCI
NITI Aayog
dfcu
EQUITY Bank
FamilyBank
FirstBank Since 1894
Safaricom
Centenary Bank
m-pesa
MTN Mobile Money
Center for Global Development
airtel
vodafone
moov no limit
UKaid from the British people
Michael & Susan Dell FOUNDATION
OJK OTORITAS JASA KEUANGAN
Ecobank The Pan African Bank
CESAG
BURO Bangladesh

MSC
MicroSave Consulting



MSC corporate brochure | Contact us at info@microsave.net

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

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

MSC

MicroSave Consulting