DIGITAL IDENTITY
Curacao, November 2019

Fredes Montes, Senior Financial Sector Specialist

WORLD BANK GROUP

CONTENT

- The Problem
- Evidence from surveys
- Relevance in Financial Sector
- Global Policy Response
- The FATF Digital ID Guidance Note
- International Experience

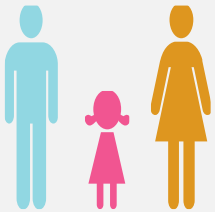
THE PROBLEM

The Identification Gap

SDG Target 16.9: By 2030, **provide legal identity for all**, including birth registration

Globally, an estimated 1.1 billion people are unable to prove their identity

2 billion people do not have access to financial services



Digital payments are growing at an estimated 12.7% annually, and are forecast to reach 726 billion transactions annually by 2020.

The Verification Gap

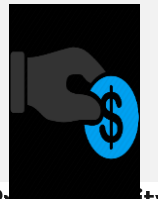
Even with ID, 3.4 Billion people are not able to use it effectively it may be impossible to verify validity + authenticate holder against claimed identity

Credentials that cannot be verified will only provide a limited level of assurance, and may not be widely accepted

Exclusion

In UK for example 25% of financial services applications do not go through due to difficulties with KYC process.

Open Accounts with Financial Service Providers



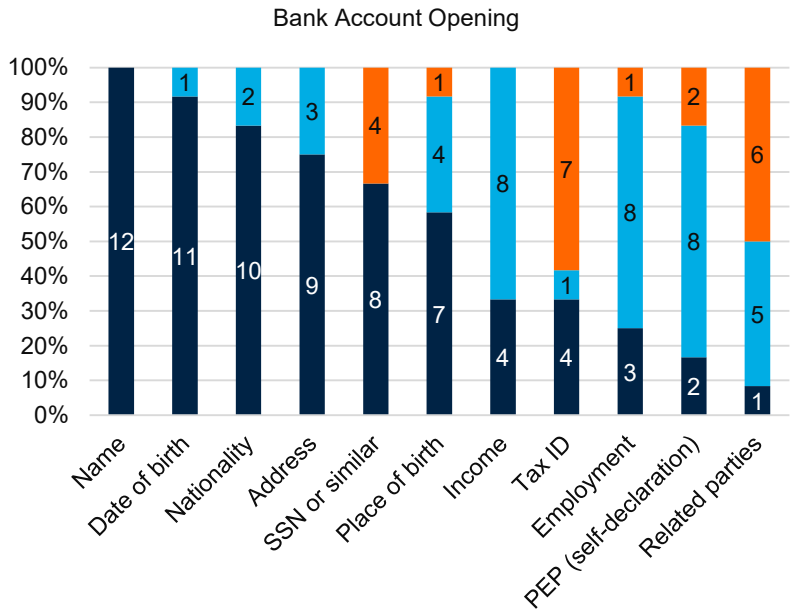
Prove eligibility for and access social and health benefits

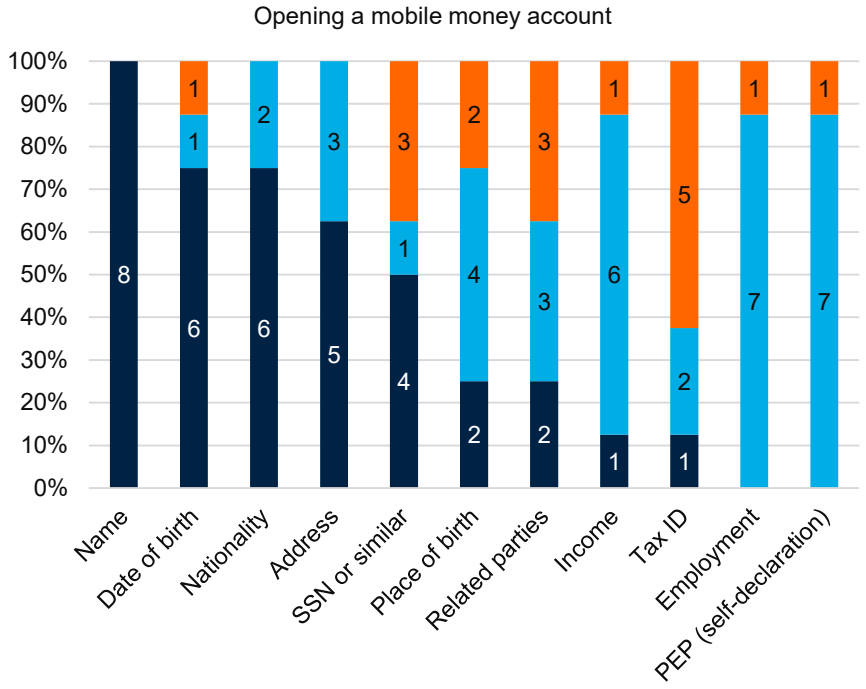
Legal Compliance

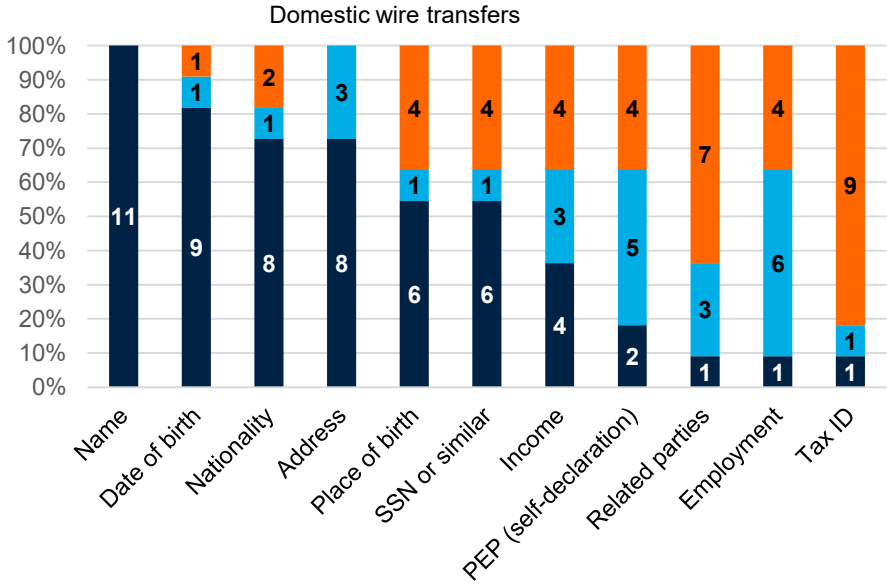
Send and Receive Payments

Provide consent to share data through APIs

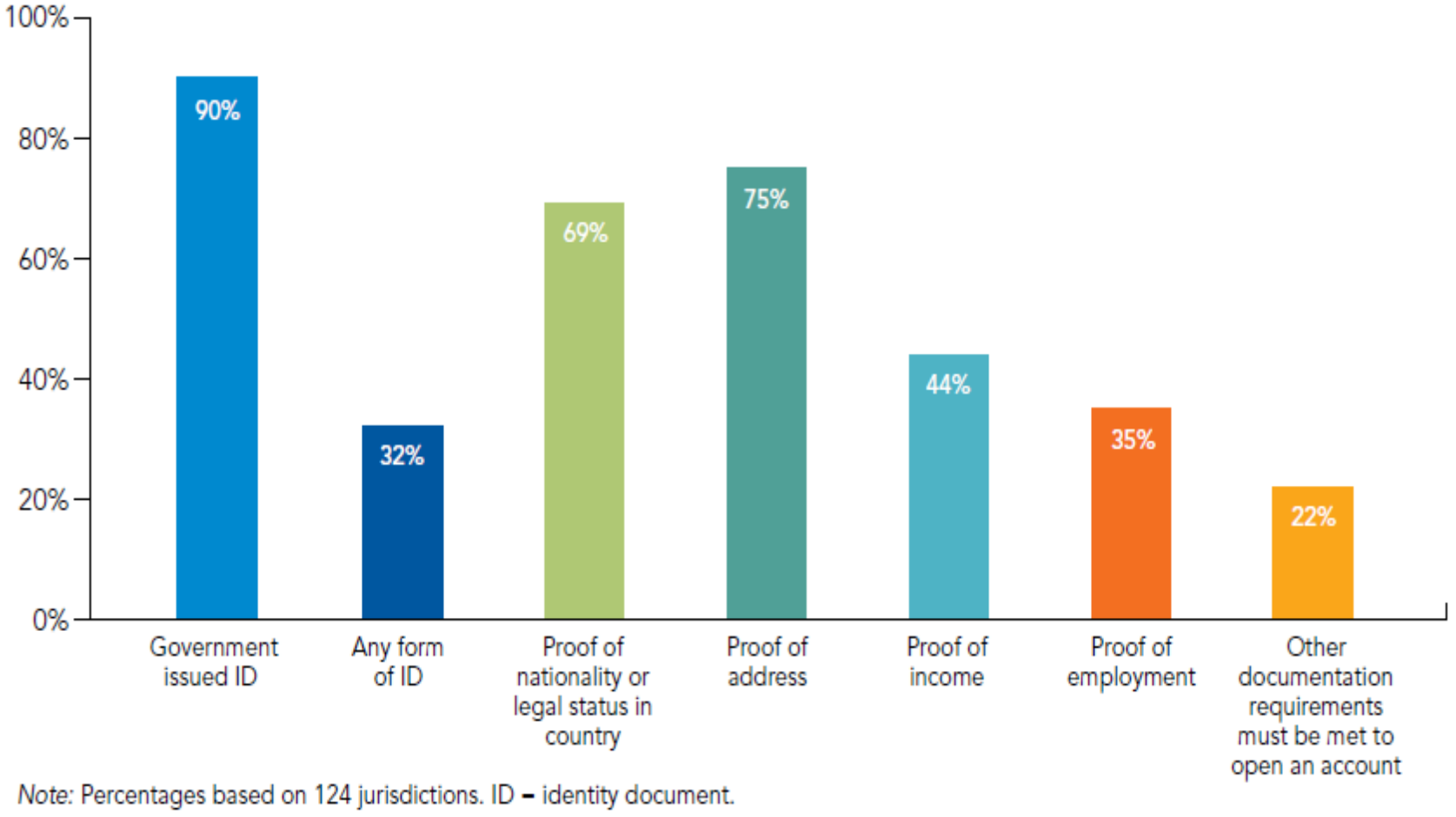
TYPE OF DATA REQUIRED







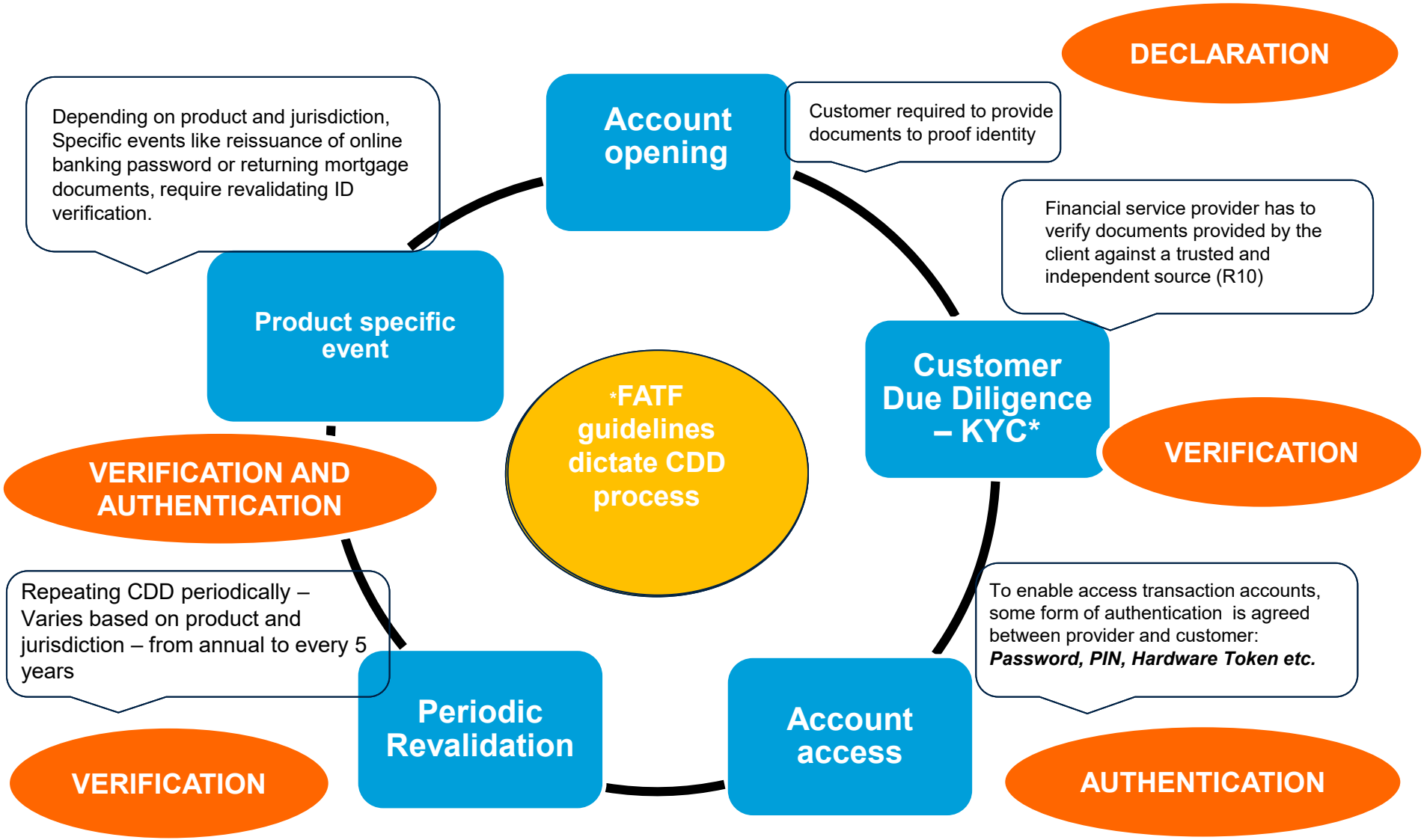
TYPE OF ID DOCUMENT TO OPEN ACCOUNTS IN COMMERCIAL BANKS



Note: Percentages based on 124 jurisdictions. ID – identity document.

2017 Global Financial Inclusion and Consumer Protection Survey

ID IN ACCOUNTS CYCLE



GLOBAL POLICY RESPONSE

UN SDO 16.9: “Have a **legal ID for all by** 2030 including registry at birth”

GPFI Global Partnership for Financial Inclusion

The G20 High Level Principles on Digital Financial Services acknowledge the need to **foster ID systems to enable access and usage of** de DFS. (Principle 7)

FATF

Financial Action Task Force (FATF)-40 Recommendations for KYC and CDD. **Guidance Note on Digital ID .**Unserved and underserved people have to be financially active and may be forced to conduct their transactions through unregulated channels when they lack access to formal financial services.

BIS

Payments Aspects of Financial Inclusion. **Digital ID a key supporting infrastructure** to advance Payments**.**

THE WORLD BANK

ICCR. Policy Guidance on Financial Inclusion . Need to **uniquely identify each individual and legal entity** in the database.

G20 DIGITAL ID ONBOARDING:FINDINGS

Digital IDs are important to public policy and service delivery and require significant support and investment

Digital Identity Can Be A Critical Enabler for Financial Inclusion: Easier CDD/account opening, streamlined authentication, more cost effective onboarding, simplified agent services, easier credit monitoring, lower cost payments & remittances

There may be gains from decoupling identity verification from other functions

The Private Sector Can Build Digital Identity Layers onto a Legal Identity System

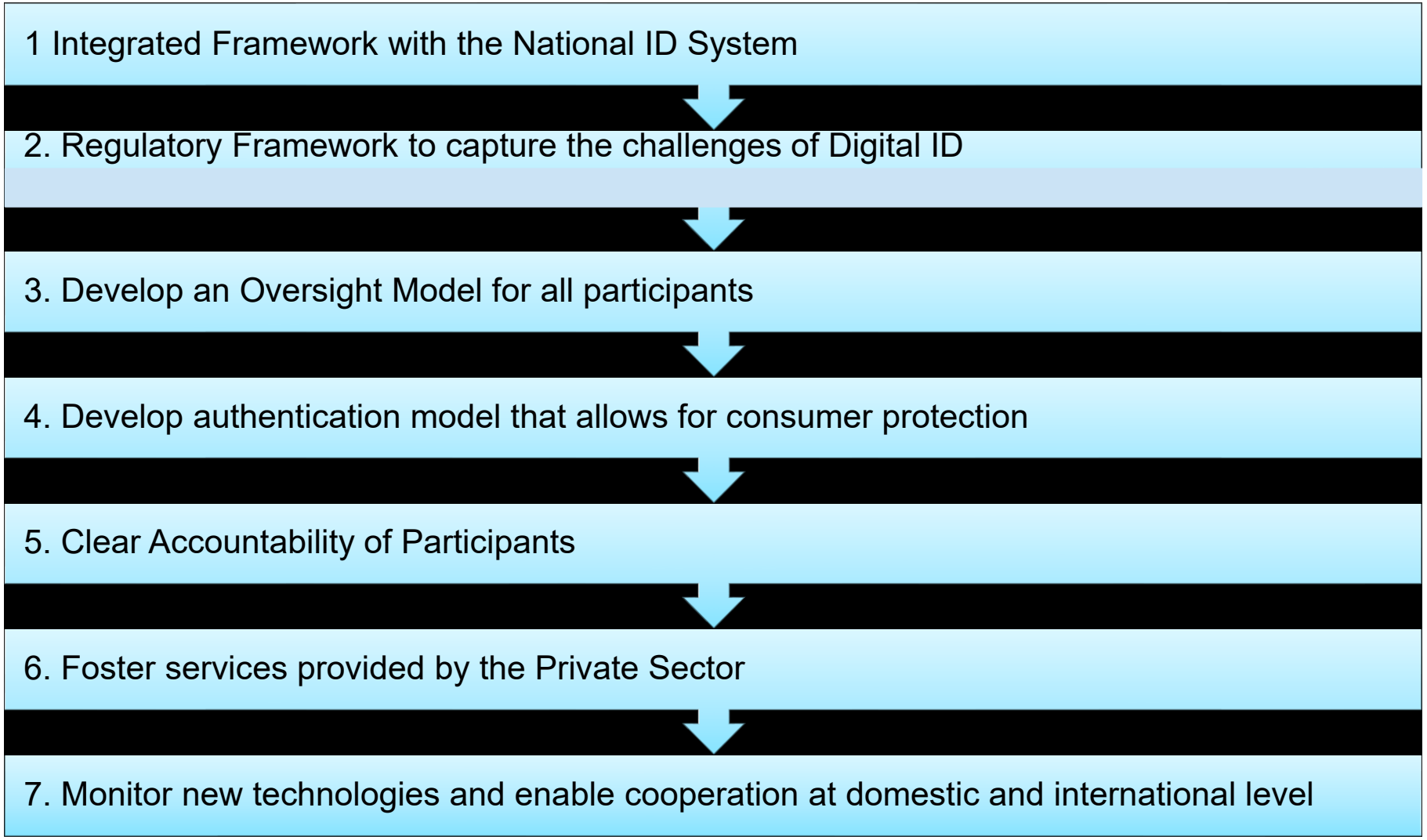
Digital IDs Can Help Bring More MSMEs Into the Formal Financial Sector: Formalization opens access to credit, working capital and payment services

Digital IDs Can Support the Establishment of e-CDD Registries

Digital IDs Help Financial Service Providers Streamline Their Business Operations: Registration, transaction monitoring, credit risk assessment, compliance, reporting Lower overall business costs can help lower fees

Maximum benefits are achieved when ID is applied to all residents and not just citizens

G20 DIGITAL ID ONBOARDING: POLICY CONSIDERATIONS



FATF RECOMMENDATIONS FOR CDD

R 10 FATF

- Financial institutions should be prohibited from keeping anonymous accounts or accounts in obviously fictitious names
- Fis should conduct CDD under the following circumstances
  - (i) Onboarding of new clients;
  - (ii) Occasional transactions above 15,000 USD-Euros; or (ii) Electronic Transfers based on R16;
  - (iii) Suspicious illegal activity of ML or TF; or
  - (iv) When the FI has doubts about the veracity and reliability of the clients' data

R 10 FATF (REQUIREMENTS)

- Identify the client and the ultimate beneficiary **using data, documents and reliable information from independent sources.**
- Ultimate Beneficiary and Client
- CDD must be done with an risk based approach (RBA)

DIGITAL ID GUIDANCE (2019)

- Framework for adequacy of Digital ID Systems to R10
- Currently under consultation until November 29.

CDD Requirements	Key Components of Digital ID
Identification/Verification R.10(a)	**Identity Proofing-** Who are you? Step 1 Obtain identifiers and ID evidence for those attributes. Step 2 Validate. Step 3- Verify ID evidence Step 4- Resolve Identity Proofed person
	Binding- Issue credentials or authenticators linking the person in possession of the credentials to the on-boarded customer/account
	Authentication- Are you the identified person? Who you claim to be? This applies if the regulated entity is conducting identification of a pre-existing ID system

FATF GUIDANCE NOTE ON DIGITAL IDENTITY

ANALOGUE IDENTITY

Identity – Set of phisical and context atributes that allow to differentiate one person from another.

Legal Identity/Official Identity- Set of characteristics of a person that are recognized by the government (through a CRVS of National ID system) as key atributes to differentiate one person from another and enables the person to Access rights and meet obligations.

DIGITAL IDENTITY

Official Identity as the specification of a unique natural person that:

(i) is based on characteristics that are unique to one individual and context

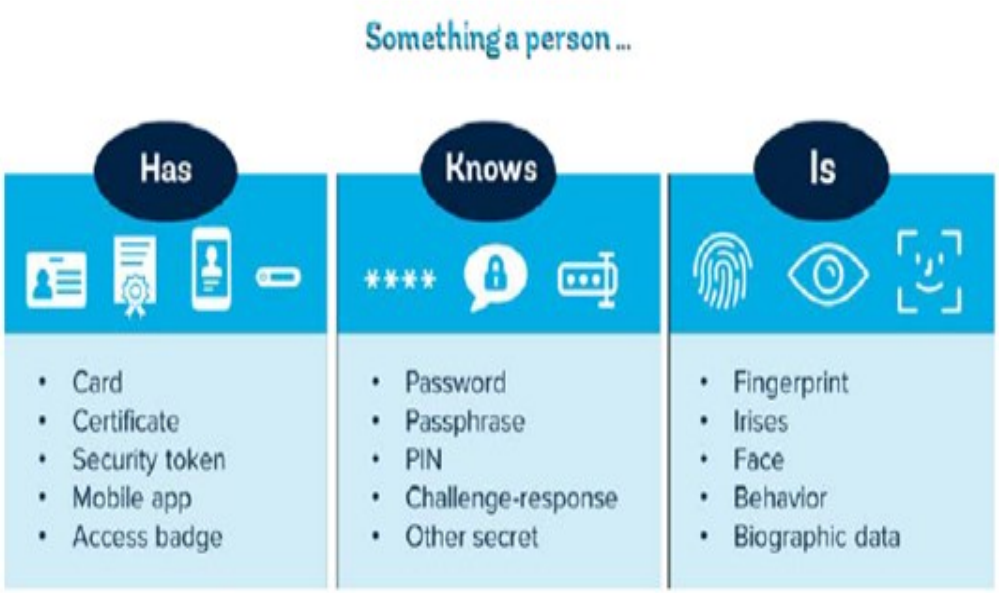
(ii) Recognized by the State of regulatory authorities for oficial purposes

(iii) Which can be created electronically or documentary but binding, authentication credentialing and portability is don eelectronically. (APIs, Databases, biometrics)

In the context of e-signatures it is also necessary to validate the identity of the individual who signed the document.

Identitas identitatis (=to be) vs Identification (=be recognized)

FATF GUIDANCE NOTE ON DIGITAL ID: AUTHENTICATION



Reduce Risk of Fraud

Vulnerabilities of some authentication factors used

- Credential stuffing, phishing, PIN code capture and replay, forged logging attacks

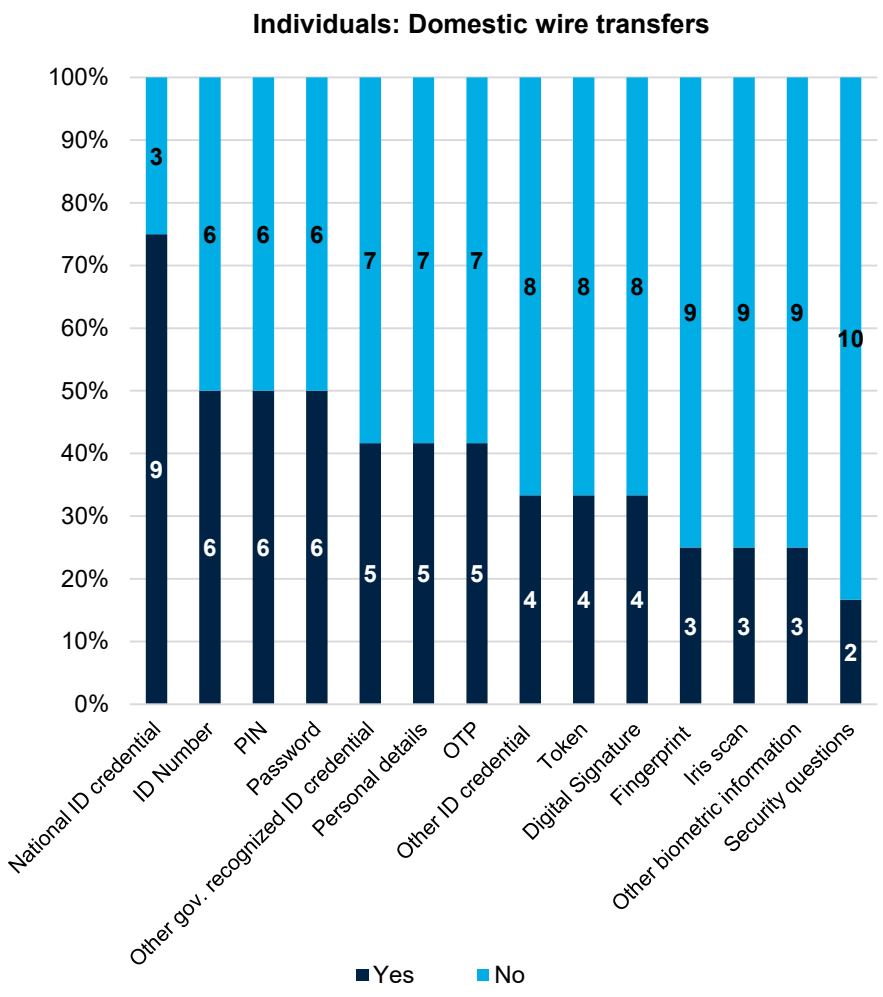
Consider potential exclusion aspects

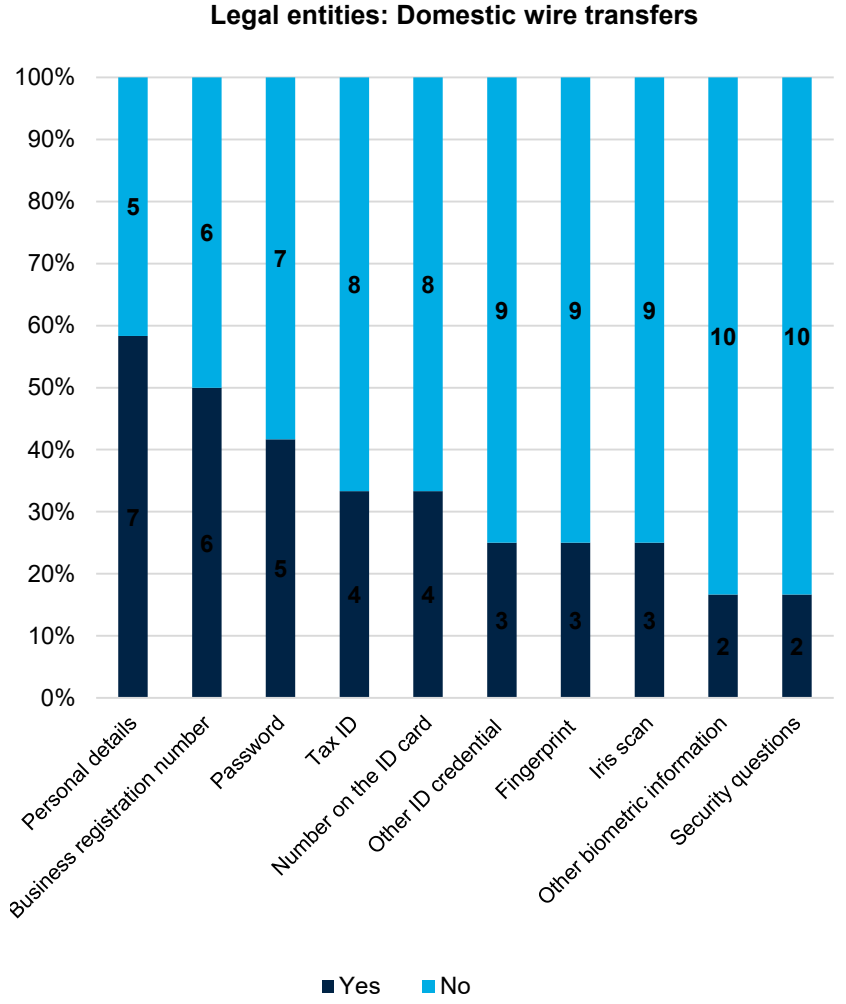
- Lack of biometrics, or specific groups that facial recognition might encounter failures
- Allow for alternatives

Authentication is responsibility of the regulated entity

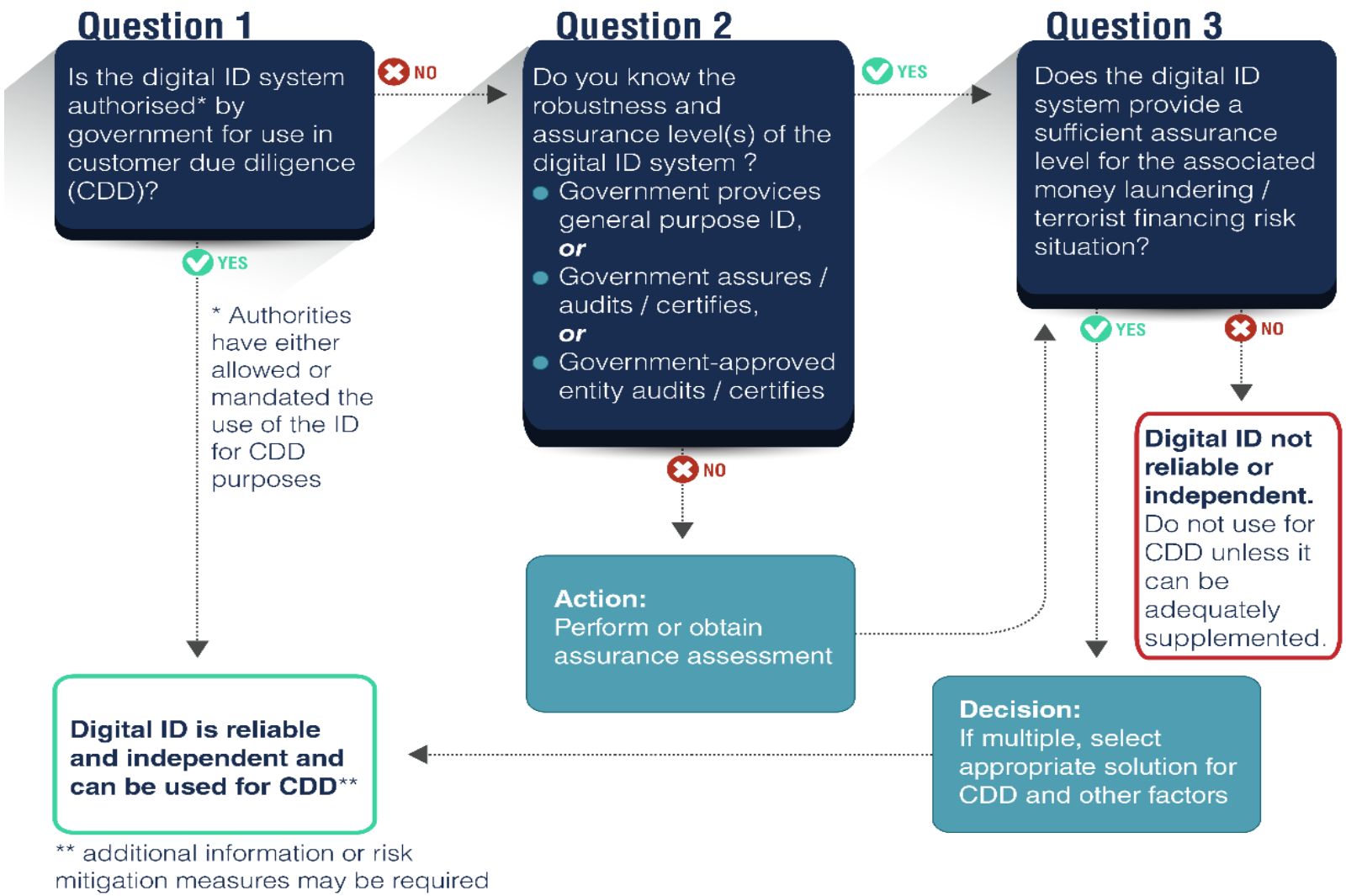
- MFA
- SCA under RTS of the PSD2 (Strong Customer Authentication)

Survey Responses: Authentication Methods





ASSURANCE DECISION FRAMEWORK



RECOMMENDATIONS FOR AUTHORITIES

- Develop clear guidelines or regulations allowing the appropriate, risk-based use of reliable, independent digital ID systems by regulated entities for AML/CFT purposes.
- Assess whether existing regulations and guidance on CDD accommodate digital ID systems.
- Adopt principles or outcomes-based criteria when establishing the required attributes, identity evidence and processes for proving official identity for the purposes of CDD
- Foster an efficient, integrated approach to digital ID through adequate supervisory tools.
- Encourage a flexible, risk-based approach to using digital ID systems for CDD that supports financial inclusion. Guidance for Tiered CDD

RECOMMENDATIONS FOR AUTHORITIES

- Assess risks and develop a framework to effectively address such risks. Assessment and mitigating measures might involve coordination with all the stakeholders in the ID ecosystem.
- Consider a certification or auditing framework or by approving expert bodies to perform such role.
- Government authorities providing Digital ID should also be transparent regarding their assurance framework.

RECOMMENDATIONS FOR REGULATED ENTITIES

- Take an informed risk-based approach to relying on digital ID systems for CDD that includes:
  a. understanding the digital ID system's assurance level/s, particularly for identity proofing and authentication, and
  b. ensuring that the assurance level/s are appropriate for the ML/TF risks associated with the customer, product, jurisdiction, geographic reach.
- Consider whether digital ID systems with lower assurance levels may be appropriate for simplified due diligence in cases of low ML/TF risk.
- Non face-to-face customer identification is considered high risk by default. Under a robust Assurance framework it might be standard and even low risk.

RECOMMENDATIONS FOR SERVICE PROVIDERS

- Understand the AML/CFT requirements for CDD (particularly customer identification/verification and ongoing due diligence) and other related regulations, including requirements for regulated entities for record keeping.
- Seek assurance testing and certification by the government or an approved expert body, or where these are not available, another internationally reputable expert body.
- Provide transparent information to AML/CFT regulated entities about the digital ID system's assurance levels for identity proofing, authentication, and, where applicable, federation/interoperability.

INTERNATIONAL EXPERIENCES

Financial Inclusion

Access: *Meet CDD requirements*

Enhanced: *Build a transaction history*

IndiaStack

financial inclusion went from 35% in 2011 to 80% in 2017

Electronic Payments

Enrolment; *Fostered enrolment of users*

Efficiency: *Reduced time in completing transactions*

พร้อมเพย์ PromptPay

increased electronic payments in 83% in 2018

Social Protection

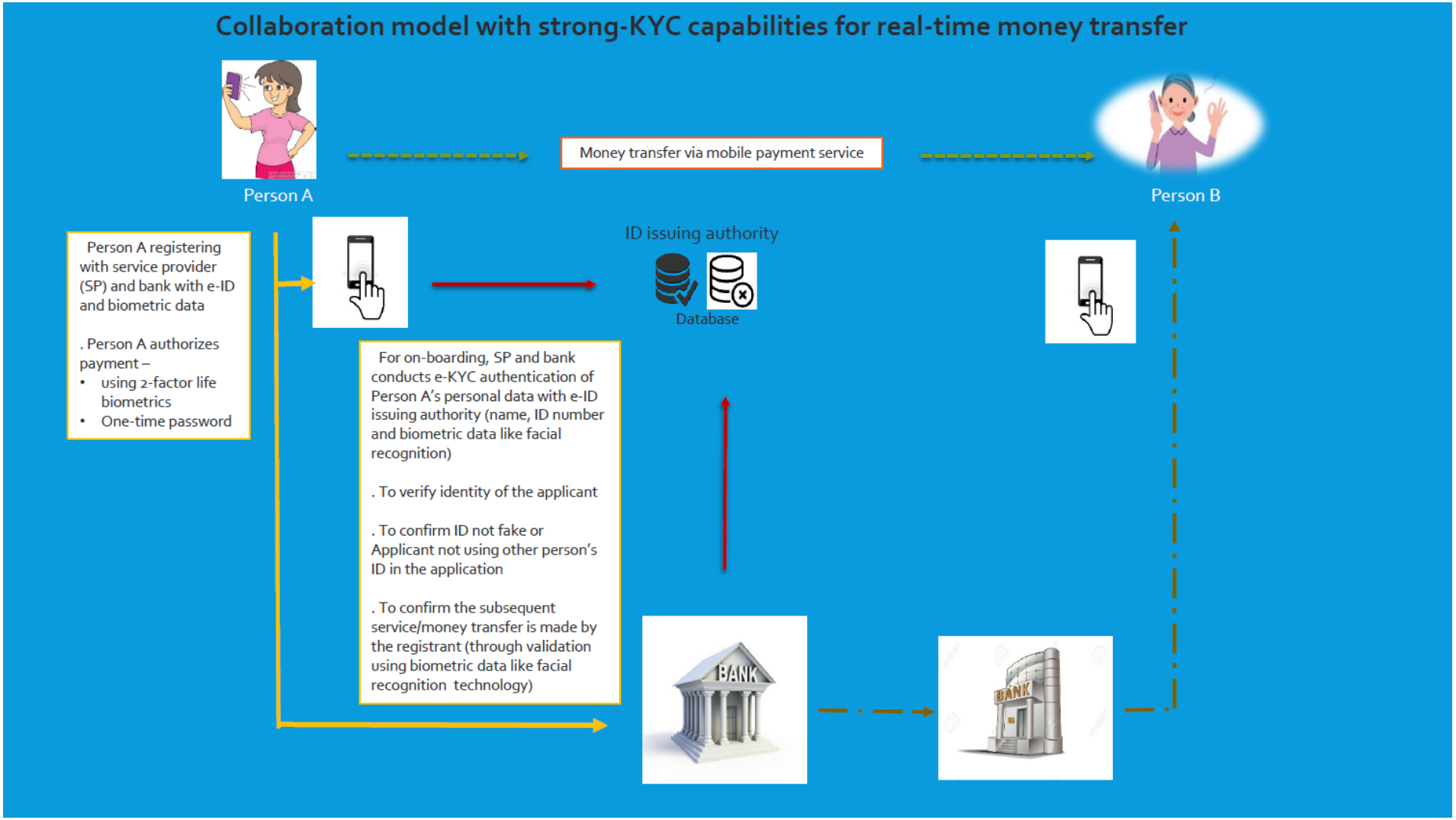
Identifying correct beneficiaries: *Those that meet criteria*

Delivery: *Ensuring that those who received the subsidy are the ones tat effectively qualify for such subsidy*

~US$248mn

WORLD BANK GROUP

USE OF DIGITAL ID : MONEY TRANSFERS

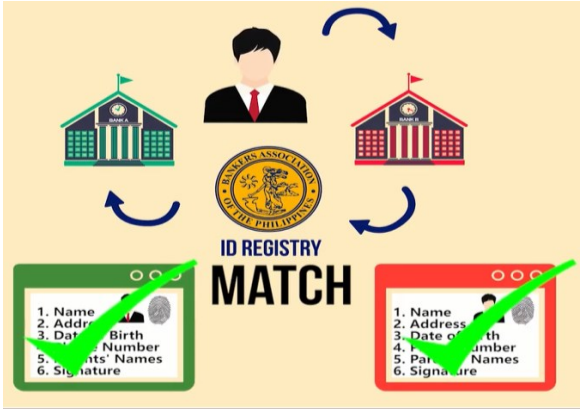


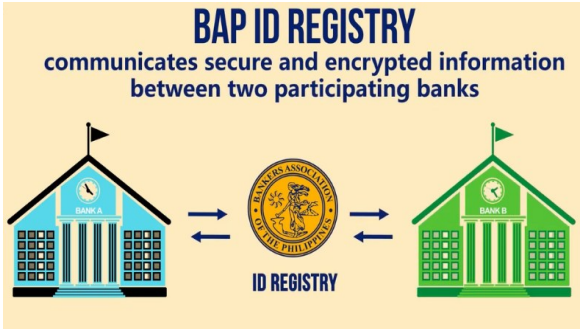
Digital ID can serve also to establish e-KYC registries or CDD utilities

Philippines

- The Bankers' Association of the Philippines (BAP) is expected to launch its blockchain-powered e-KYC and ID registry in 2019.
- The registry is only for individual account holders.
- A customer would need to present a valid government ID or provide biometric information, and authorize any participating bank to access validated information another participating bank with whom the customer already has an account.
- All information is expected to be stored in the respective banks' own secure systems and no information is to be stored in the registry.
- Individual banks continue to be responsible for data privacy and for accuracy of customer information.
- This facility, however, is only available to banks that are members of the BAP. At present, it is not clear if other financial institutions will be able to access the registry.
- The project has the 'blessings' of the Bangko Sentral ng Pilipinas.

Advertised Features of the BAP ID Registry



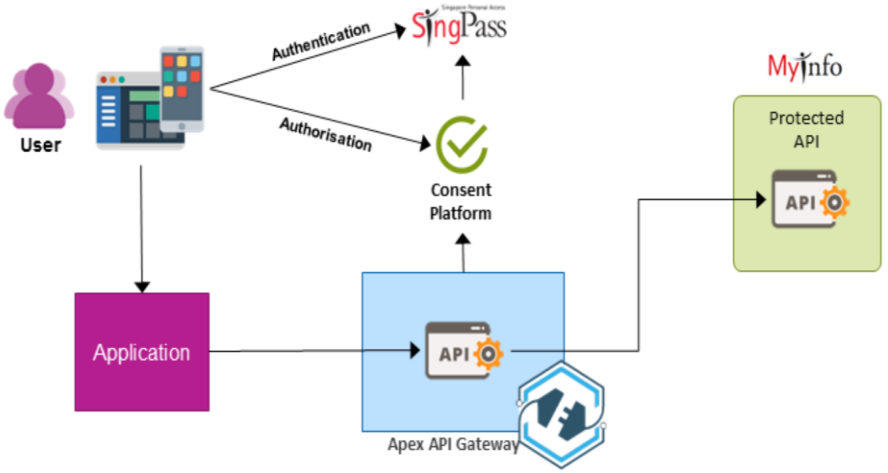


Source: Promotional video of the BAP ID Registry

Singapore

- The Monetary Authority of Singapore (MAS) had unveiled a plan to pilot of a national KYC utility for financial services, based on the MyInfo digital identity service – which was jointly developed by the Ministry of Finance and GovTech, the lead agency for digital and data strategy in Singapore.
- The KYC utility was meant to be a shared service among banks, to make it easier for financial institutions to get customer verification done in a more seamless way.
- A pilot had been run in the first quarter of 2017 year with four Singaporean banks expanding the MyInfo service to the financial industry for more efficient KYC using trusted, government-collected personal data.
- This project was eventually shelved in late 2018 as costs surpassed estimates.

Steps in E-KYC through MyInfo



Source: MyInfo Developer Portal (https://myinfo-api.app.gov.sg/dev/landing).

Steps in Consent-based Data sharing

1. AUTHENTICATE

Log in via SingPass to authenticate yourself.

2. PROVIDE CONSENT

Keep track of what you're sharing. The application asks for your consent before retrieving the data in your MyInfo profile.

3. PRE-FILL FORMS

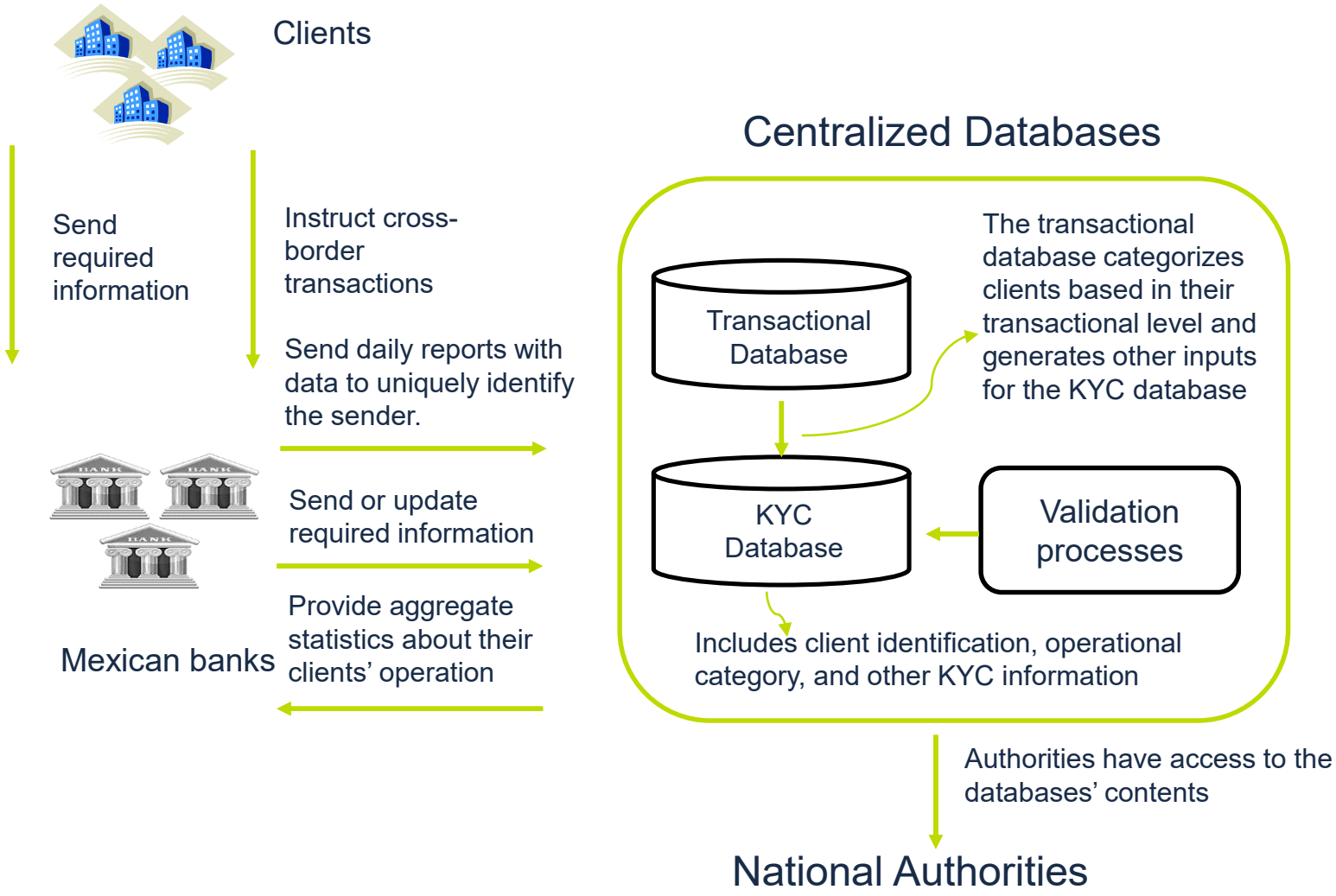
It's as easy as clicking a button! The application will be populated with data retrieved from your MyInfo profile at the click of your mouse.

Source: DBS website (https://www.dbs.com.sg/personal/deposits/bank-with-ease/dbs-myinfo)

Nigeria

- The Central Bank of Nigeria in collaboration with all banks in Nigeria on February 14, 2014, launched a centralized biometric identification system for the banking industry tagged Bank Verification Number (BVN). It is a unique ID number that is issued to every bank customer at enrolment and linked to every account at a Nigerian Bank.
- The objectives of the project include: to provide a uniform industrially accepted unique identity for bank customers, to authenticate transactions without the use of cards using only biometric features and PIN, and identification of blacklisted customers.
- It involves identifying an individual based on physiological or behavioral attributes, such as fingerprint, signature and others. This is meant to avoid identity theft and track suspicious transactions
- It is believed that harmonization of all private and government agency databases could save the country about USD 110 million in operational costs by the different government agencies for their stand-alone data collection and evaluation.
- As of 2019, Nigerian passports are also being linked to the BVN.

Mexico


Clients
Send required information
Instruct cross-border transactions
Send daily reports with data to uniquely identify the sender.
Send or update required information
Provide aggregate statistics about their clients' operation
Mexican banks
Centralized Databases
Transactional Database
The transactional database categorizes clients based in their transactional level and generates other inputs for the KYC database
KYC Database
Validation processes
Includes client identification, operational category, and other KYC information
Authorities have access to the databases' contents
National Authorities

RELEVANT MATERIALS ON DIGITAL ID

- https://www.gpfi.org/publications/g20-digital-identity-onboarding

- FATF (2013-2017), *Anti-money laundering and terrorist financing measures and financial inclusion - With a supplement on customer due diligence*, FATF, Paris www.fatf-gafi.org/publications/financialinclusion/documents/financial-inclusion-cdd-2017.html
- World Bank (2018), Private sector economic impacts from identification systems, http://documents.worldbank.org/curated/en/219201522848336907/Private-Sector-Economic-Impacts-from-Identification-Systems.pdf

- https://www.fatf-gafi.org/publications/fatfrecommendations/documents/consultation-digital-id-guidance.html
- Forthcoming FIGI toolkit on Digital ID (The World Bank)

List of Consulted Institutions

1. Banco de México
2. Bangko Sentral ng Pilipinas
3. Central Bank of Armenia
4. Central Bank of Jordan
5. Central Bank of Nigeria
6. Czech National Bank
7. Latvijas Banka
8. National Bank of the Republic of Belarus
9. Otoritas Jasa Keuangan (OJK), Indonesia
10. Saudi Arabian Monetary Authority
11. South African Reserve Bank
12. The Central Bank of Russia
13. UK Financial Conduct Authority/ UK Cabinet Office

Fredes Montes
Senior Financial Sector Specialist
fmontes@worldbank.org
+1 202907644