WORLD BANK GROUP

ID4D
IDENTIFICATION FOR DEVELOPMENT

G20
ARGENTINA 2018
BUILDING CONSENSUS FOR FAIR AND SUSTAINABLE DEVELOPMENT

Digital ID in Financial Sector

Harish Natarajan
World Bank

Arab Fintech Working Group
June 24th 2019, Abu Dhabi

GPFI Global Partnership for Financial Inclusion

Agenda

1. Characteristics of a Digital ID
2. Why is ID important for the Financial Sector
3. Benefits of Digital ID
4. Country Examples
5. Risks and Key Findings
6. Policy Considerations

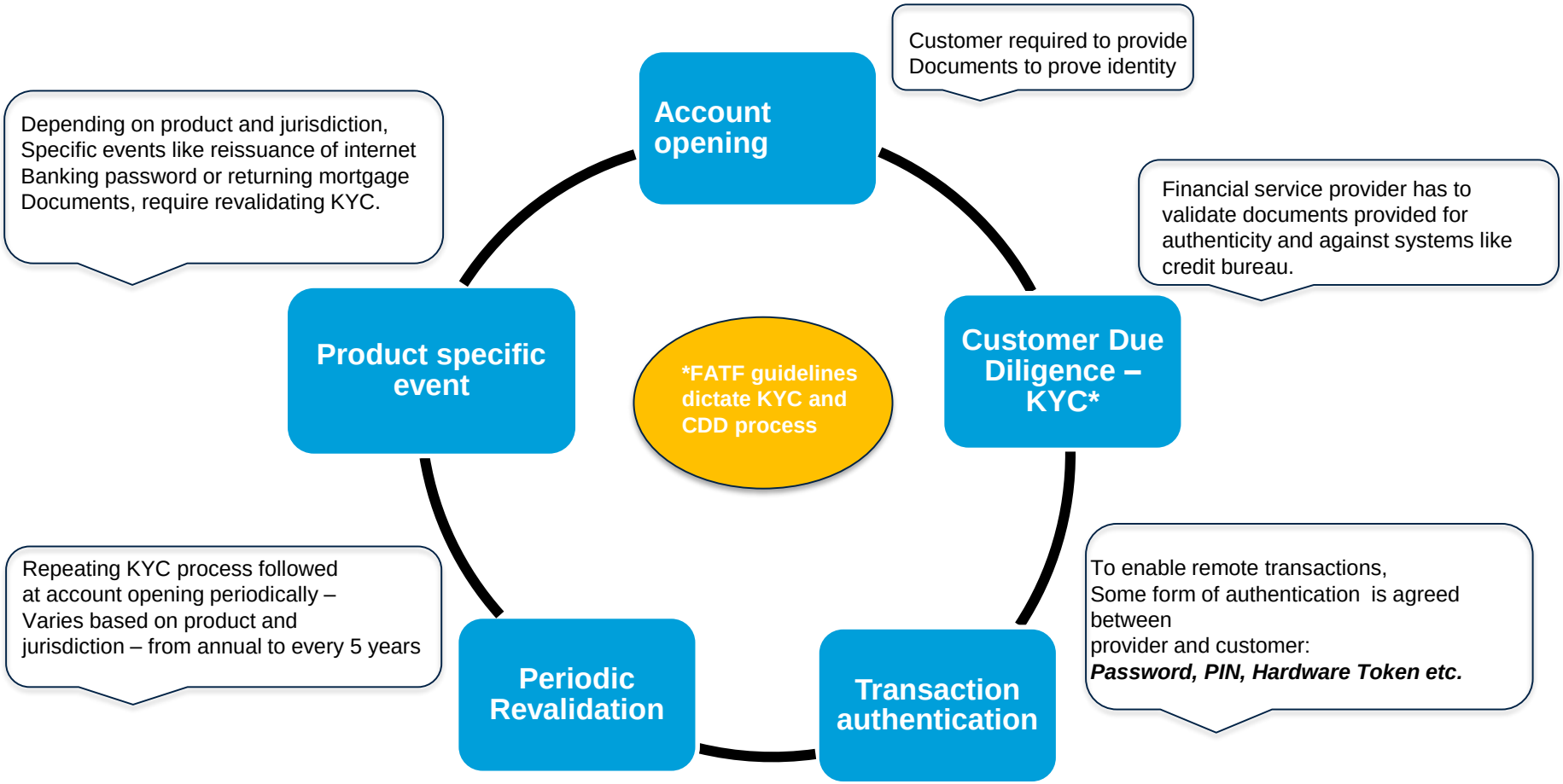
WORLD BANK GROUP

Characteristics of ID

- Lack of Legal ID feature impacts access leading to financial exclusion;
- Lack of Unique ID (UID) feature leads to no full view of customer and also impacts the provision of credit and insurance and can lead to instances of fraud;
- Lack of a Digital UIDs feature adds inefficiencies and cost impacting affordability.

Role of ID in Financial Sector

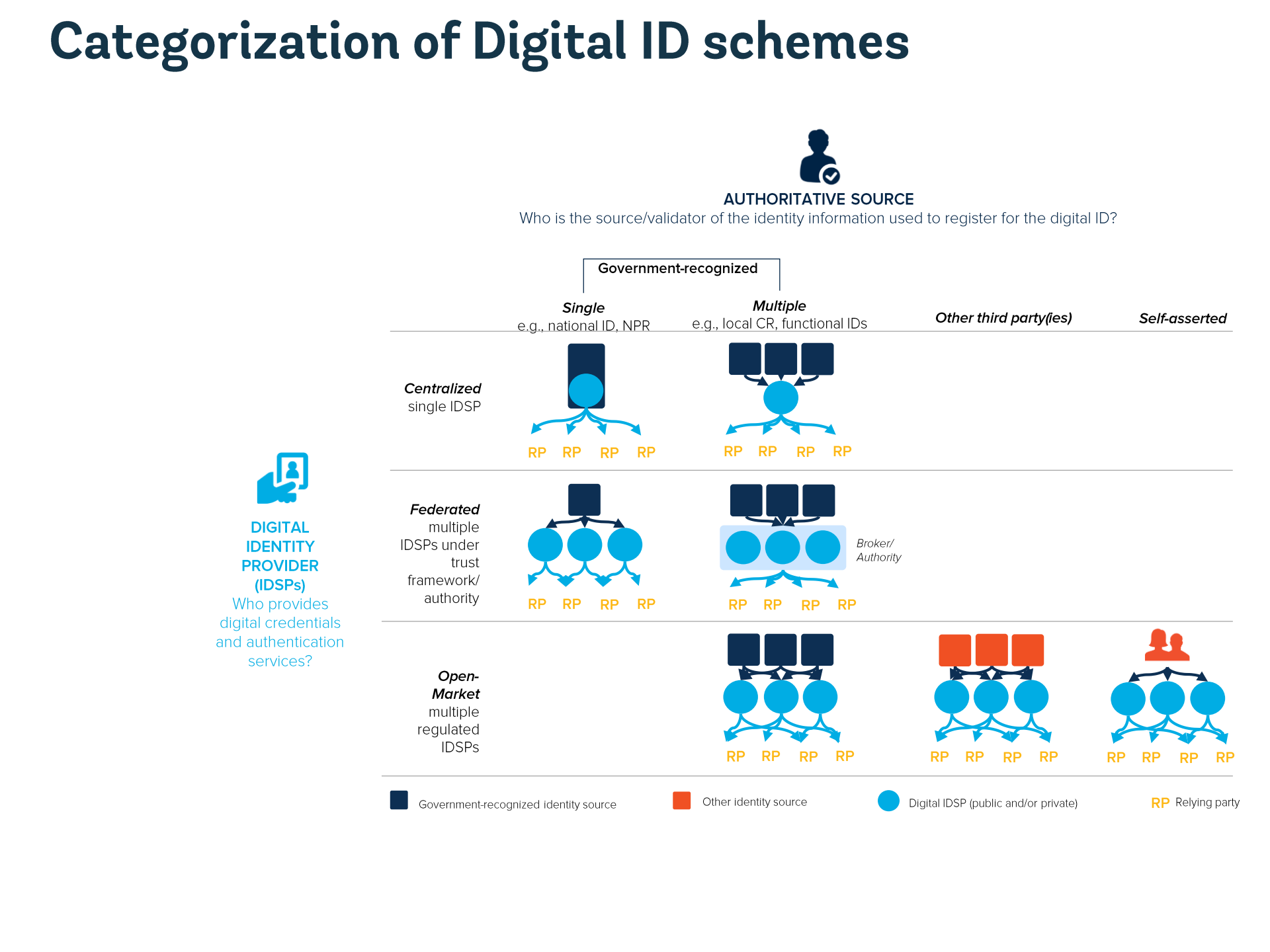
ID is integral to financial services, ensuring safety and integrity of the financial system



Benefits of Digital ID

WORLD BANK GROUP

Categorization of Digital ID schemes



Country Case Studies

Peru

Issuing Authority: National Registry of Identification and Civil Status - **RENIEC**

Non-smart National ID Card

- 99.9% coverage
- Expired in 2016, natural point to upgrade
- Card-holder provides identity number (printed on the card)
- Present finger-print for authentication with fingerprint held in RENIEC database

Electronic National ID Card

- Initially targeted specific groups (e.g. lawyers, judges)
- Mid 2015 – decision to scale up distribution of electronic ID card
- 5 year target of 12 million cards
- Supports offline biometric verification
- Needs to be placed in a card reader

Use Cases:

- Banks – KYC onboarding
- Agents and participating financial institutions - Registration for BiM (mobile wallet through Modelo Peru)
- Pension and scholarship payments
- Record each time a citizen votes (voting mandatory in Peru)

India

Issuing Authority: Unique Identification Authority of India – **UIDAI**

Aadhar

- More than 1 billion Indians have been registered
- Registration is based on:
  1) Availability of two supporting existing ID documents [passport, DL etc]
  or
  2) Introducer system – in which two individuals registered for Aadhar can vouch for the identity of another person
- Registration process

- Card-holder presents Aadhar number and authentication is done online using fingerprint
- On successful authentication, Aadhar service provides the identification data to the service provider
- Aadhar authentication is online, for both face to face and remote transactions

Aadhaar – Use cases

- **Bank account opening**: Sufficient for using basic bank accounts and was central to the mass account opening campaign - PMJDY (Pradhan Mantri Jan Dhan Yojana). Over 250 million accounts opened in 2 years.

G2P: De-duplication and targeting of Government subsidies and making Aadhar the “payment address” – enabling paying subsidies by mapping Aadhar number to bank account – Public Distribution System (ration), LPG Cylinders, Social Safety Net programs etc.

- **Aadhar based authentication of payment transactions and Digitally signing legal documents**: replacement of PIN for ATM transactions; Signing Tax Returns, Registering Title documents, registering lease-rentals etc.

- **Digital locker service**: Mobile based, intended to provide secure access to Government-issued documents and released based on approval of individual:

  4.2 M users; 6 M uploads; 1.6 B issued documents

Pakistan

Issuing Authority: National Database and Registration Authority - **NADRA**

Computerized National Identity Card (CNIC)

- Estimated coverage of the adult population approximately 99%
- CNIC has a unique identifier that is seeded into different government databases
- Chip based card
- At the time of registration, facial and fingerprint biometrics registered and stored, both on the card and in the central NADRA database
- Contents on the face of the ID card are also in the chip
- Four best fingerprints and the digitized photograph captured at time of registration are held on the chip
- For authentication purposes, match-on-chip has been implemented, so that a fingerprint (say) is submitted, and the app returns either yes or no – the registered biometrics never leave the card.

Pakistan – Use Cases

- **Account opening and remittances**: Adequate for opening basic bank accounts and required for sending and receiving remittances.

- **G2P**: Benazir Income Support Program (BISP) to ensure robust identification of beneficiaries and Prime Minister health program

- **Elections**: Voter identification (CNIC mandatory)

- **Fight against terrorism**: Required Mobile operators to register SIM in the aftermath of terrorist attack on military base and schools.

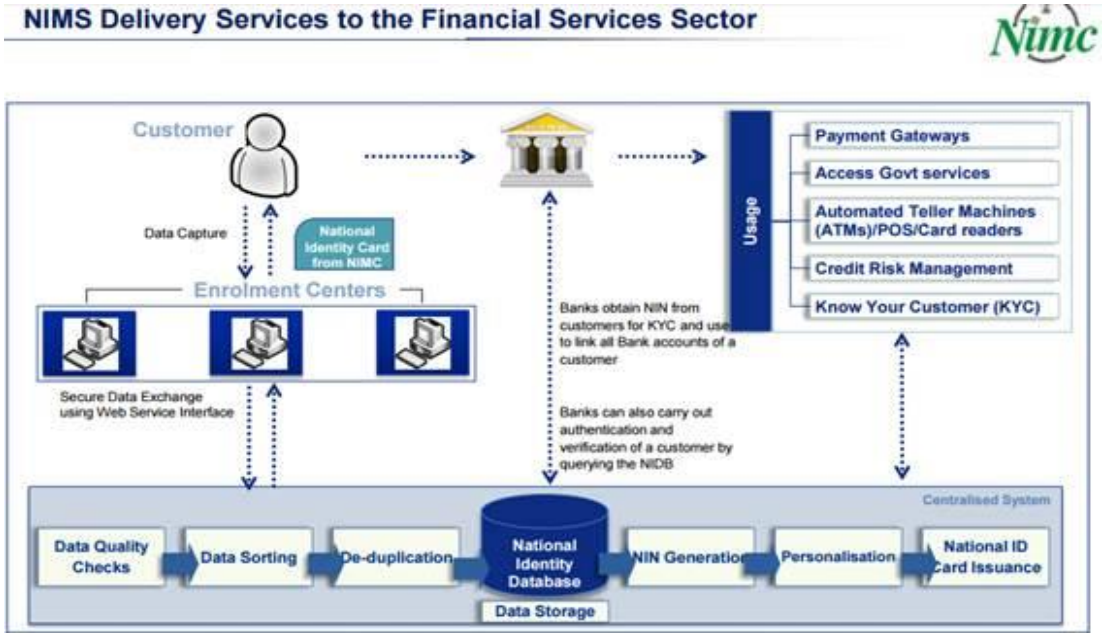
Nigeria

Two ID systems being developed in parallel

1) Issuing Authority: National Identity Management Commission - **NIMC**

National Identification Number (NIN)

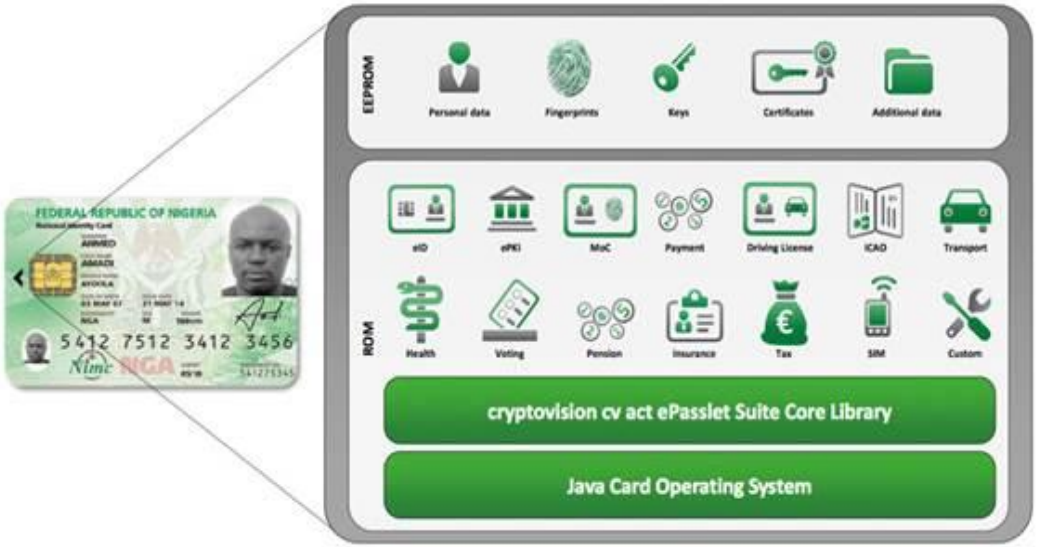
- Upon successful enrolment, electronic card is issued
- Enrolment consists of recording of an individual's demographic data and capture of ten fingerprints, facial picture and a digital signature
- The card was developed in liaison with Mastercard, with Prepaid Mastercard functionality included in the e-ID



- Only about 15% of the adult population (14,491,000) had been registered for NIN, yet much lower estimate of 3-4% of the population has been issued an eID card

NIN – Use Cases

- Passport application
- Satisfies KYC requirements to open a bank account
- Getting a driver's license or permanent voter card
- National health insurance
- Tax payments and pension scheme contributions
- Access to welfare services provided by the government



Nigeria

Bank Verification Number (BVN)

Issuing Authority: Nigeria Inter-Bank Settlement System - **NIBSS**

- Was initiated in response to very slow roll out of NIN
- Unique identifier linked to a Nigerian bank account
- The service launched in early 2014, with full compliance by all participating banks completed by October 2015 and have now enrolled more than 27 million BVNs as of November 2016.
- Ten fingerprints and facial image biometrics captured at the time of registration
- The customer's mobile phone number captured during registration is linked to the BVN
- Customers are notified by SMS when their registration is complete, and can use a NIBSS-operated USSD service to recall their BVN

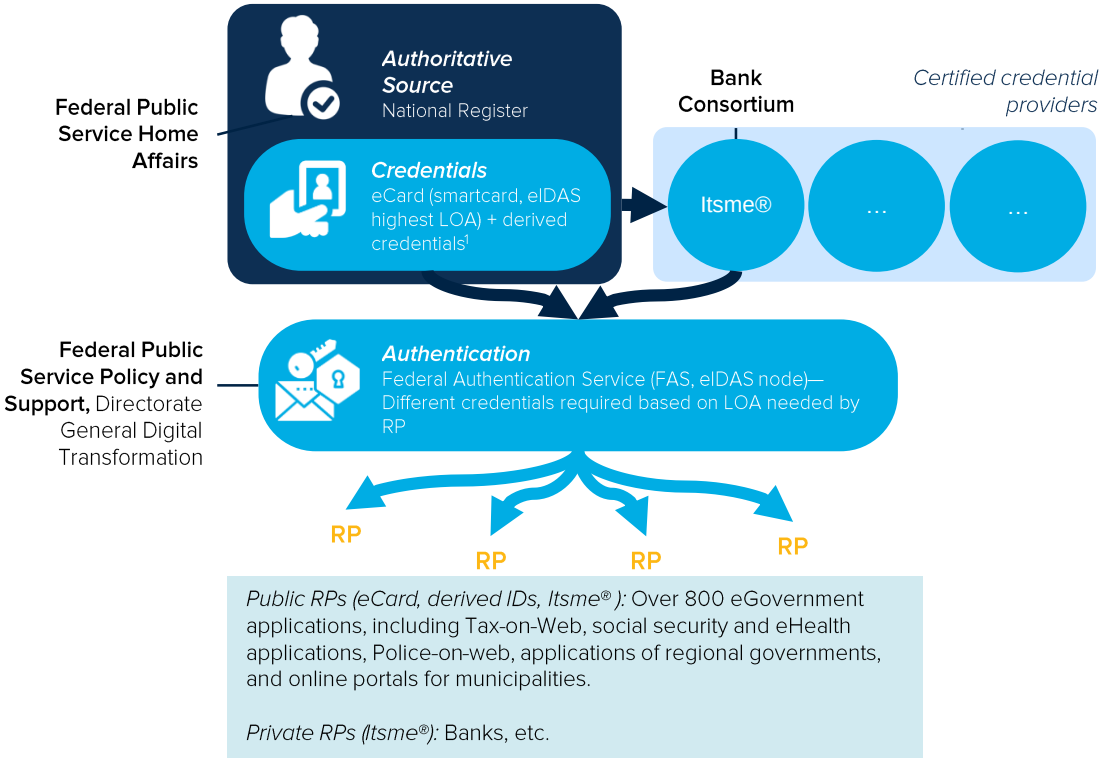
Nigeria

Use Cases:

- Customer with a BVN can open an account with any bank in Nigeria without providing any additional documentation and remotely.
- Transaction authorization and AML / CFT monitoring
- Securities and online commerce
- Government is using BVN for tax payments, identify social benefit beneficiaries and for government employee salaries
- Credit reference or credit scoring

Belgium

Centralized eCard and authentication + federated/certified credentials, based on foundational ID system



[1]After initial log-in to FAS with eCard/reader, people can request other ***derived*** authenticators (OTPs via mobile app or text, tokens, username/password) accepted by some apps that require lower levels of assurance

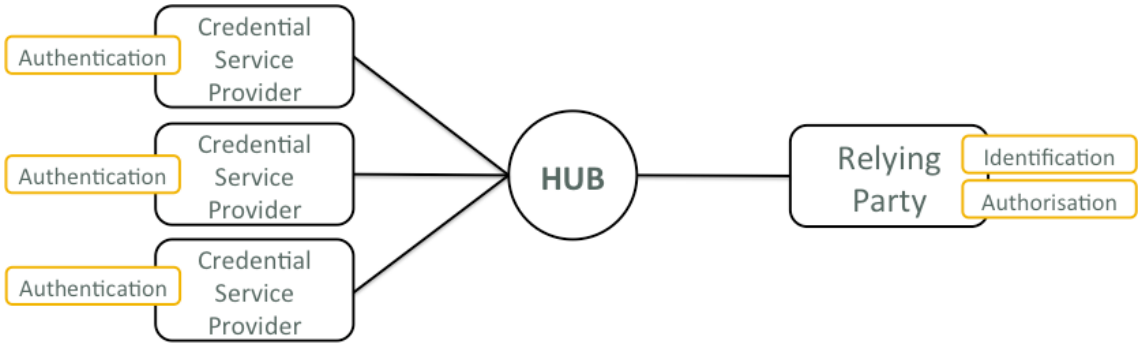
Private Sector initiatives

FIDO (Fast Identity Online) Alliance

- Focused on establishing standards that provides better technical authentication for users across many websites and mobile services
- One participating institution issues credentials and is valid across other participating institutions.
- Defined open specifications and an associated certification program for:
  - UAF (“Universal Authentication Framework”) for when the authentication is being done through the same device that the digital service is being delivered – **Passwordless Experience**
  - U2F (“Universal Second Factor”) for when the authentication is being done through a different device from the one through which the digital service is being delivered, typically a dongle or other authentication device – **Second Factor Experience**
- No link-ability between services or accounts
- **Members: Internet** – Google, Microsoft; **Payments industry** - AmEx, Bank of America, PayPal, Mastercard, VISA, USAA; **Device manufacturers** - Samsung, LG, Lenovo, Fujitsu, Sharp, Huawei; **Identity vendors** - RSA, Synaptics, NokNok, Yubico

SecureKey Concierge

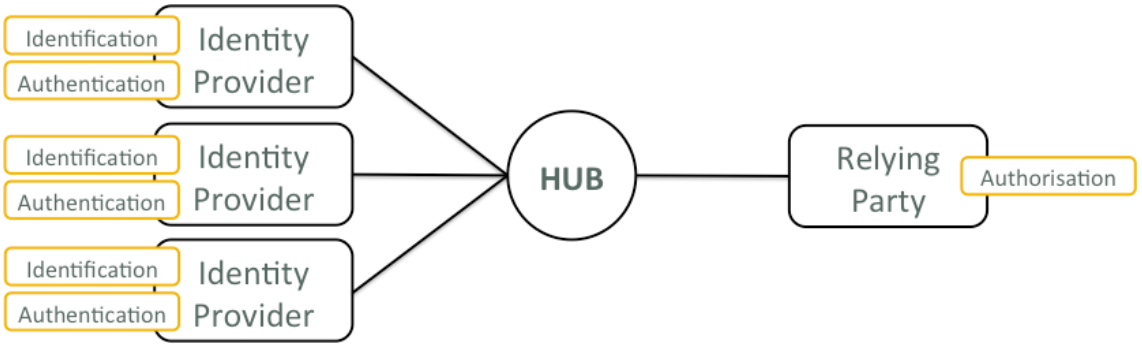
- Canadian credential brokerage service
- Operated by SecureKey
- Acts as an anonymizing broker between organizations needing to verify the identity of a customer, and those able to provide assurances around identity



- Individual service provider is still required to perform KYC steps in order to link the authentication credential with the relevant identity (or citizen) within the service provider's systems
- No link-ability between services or accounts
- Provides password-less experience – user only needs a single credential to logon to multiple services across institutions.

Gov.UK Verify

- UK government initiative to establish a private sector marketplace where private sector organizations will create and manage digital identities on behalf of citizens
- Private sector identity providers are connected via a hub to a growing number of government digital services.



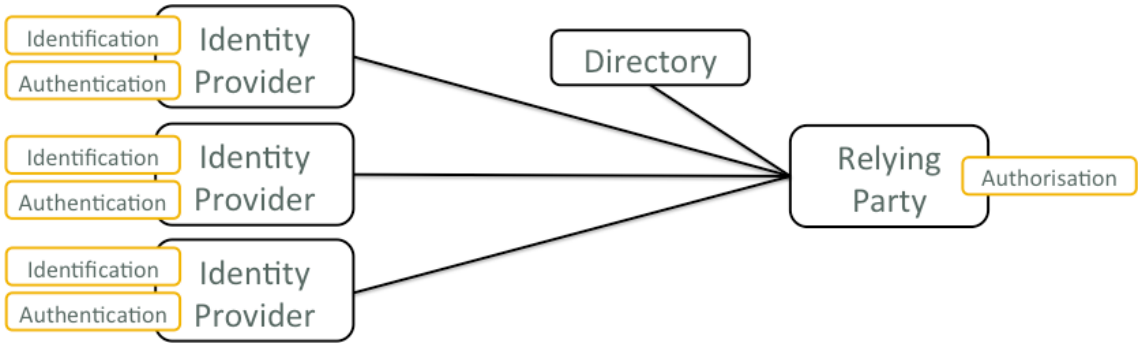
- User can potentially choose from multiple identity providers
- Data related to an asserted identity is delivered via hub which performs the function of standardizing the messaging as well as routing to the relevant service provider.
- No link-ability between service provider and identity provider

BankID

- Consortium of Banks, established to provide ID services to banks in Sweden
- Replicated in many Nordic and European countries
- ID certificate issued by banks participating in BankID
- Equivalent to a national eID in terms of technology and usage
- Banks use PKI based authentication to issue digital certificates to account holders
- Certificate validity is determined by checking both the certificate expiry (contained within the certificate) and checking an OCSP (Online Certificate Status Protocol) server
- Cryptographic keys are stored in the cloud, with access to those keys controlled through OTP-based authentication
- Government and other relying parties adopted BankID as a convenient digital identity solution

MobileConnect

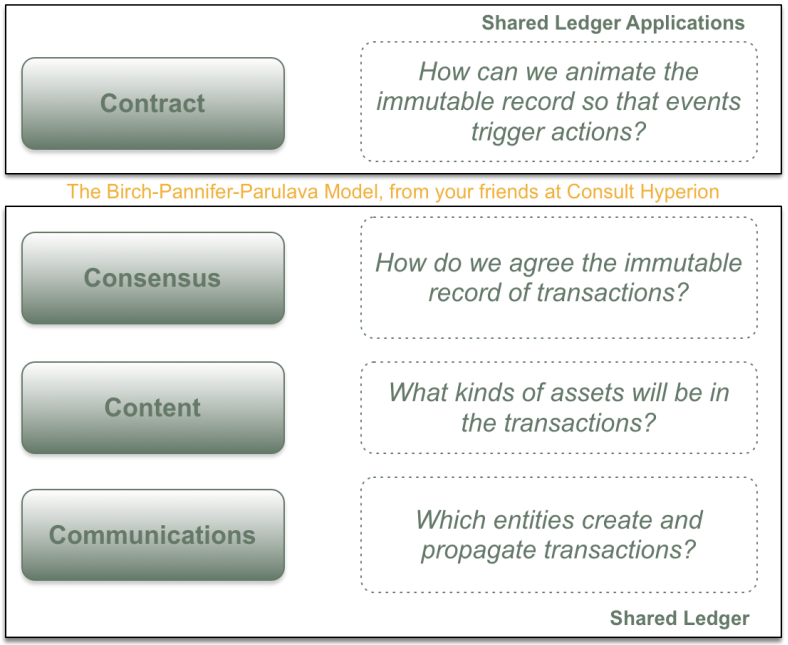
- GSMA program to enable customers to create and manage a digital universal identity via a single log-in solution
- Leverages security afforded by the SIM
- Employs user's unique mobile number, combined with a unique PIN for more secure use cases, to verify and grant online access to mobile and digital services subscribing to Mobile Connect
- Services cover e-commerce, banking, health and digital entertainment, and e-government, via their mobile phones using a federated model



- All operators and online service providers using Mobile Connect have signed up to the GSMA Mobile Connect privacy principles
- Mobile Connect initiatives are being developed within specific markets and with particular mobile operators – Including in India, Pakistan and Peru

Distributed Ledger Technology

- Provides an unchangeable transaction history, backed by a transaction-executing protocol universally available across parties
- Digital identity held using distributed ledger technology can be used to assert identity
- Distributed ledger can store attestations by third-parties of identity



"Consensus Computer"

Applications:

- Enabling portability of identity
- Create "Identity" derived from social and economic interactions
- Control what information is shared with whom.

Risks and Policy Considerations

Risks and Challenges in Implementing Digital ID

Exclusion Risks

An effective digital ID is inclusive, but there might be certain segments of the population from whom collecting biometric information is difficult, inaccurate or impossible including vulnerable populations as well as those with low digital literacy or lack of connectivity.

Privacy and Data Protection

The (most likely) centralized nature of sensitive data storage also exacerbates the cybersecurity concerns and privacy risks associated with digital IDs. Preservation of the confidentiality and integrity of the data should be the primary responsibility of the data collector; although the data processor and others involved in accessing, storing and using personal data also have a role to play.

Cost and sustainability

The infrastructure required to build a digital ID system and registration of the eligible population can be a costly and time-consuming process that is likely to require extensive investment in building or updating infrastructure and technology, buy-in from key stakeholders especially consumers, adequate knowledge and understanding of the system.

Key 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 KYC/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 authentication 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 KYC 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

Policy Considerations

Ensure an integrated identity framework

Consider the appropriateness of the regulatory framework to capture the key challenges related to digital ID, including risks to its appropriate implementation and updates to the regulatory framework, including the issuance of new regulations, where necessary

- Does digital ID meet prevailing AML/CFT requirements
- Legal (un)certainty around digital signatures
- Recognition of third party authentication services
- Mandates around use of specific ID
- Privacy and consumer protection issues

Establish a reliable oversight model to include stakeholders beyond the traditionally regulated financial institutions who can introduce risks to digital identity systems

- Data security, technology/systems standards, privacy, data governance

Build authentication and service delivery systems that protect user privacy, and provide individuals with the right to access their data and oversight over how it is shared

Policy Considerations (2)

Establish clear and well-publicized procedures for citizen redress, including defining where the onus of responsibility lies in the event that errors emerge or that the security of a person's identity is compromised;

Support and empower development of private sector led services to leverage the legal ID infrastructure for building out digital layers.
In doing so, the public authorities should ensure that these services are safe, reliable and efficient; these services are interoperable; and that the market is competitive

- Promote open APIs, interoperable platforms that private sector can build upon;
- Allows faster service development while letting public authorities focus on foundational ID and save cost

New approaches to ID are constantly emerging and public authorities should closely monitor these developments with a view to share knowledge and establish common legal frameworks at both the domestic and international level.

- Social media data, distributed ledger technologies
- Early days but capable of rapid development that policymakers should be aware of

Thank you