G20

ARGENTINA 2018

BUILDING CONSENSUS FOR FAIR
AND SUSTAINABLE DEVELOPMENT

G20 Digital Identity Onboarding

WORLD BANK GROUP

GPFI
Global Partnership
for Financial Inclusion

© 2018 The World Bank Group

1818 H Street NW
Washington, DC 20433
Telephone: 202-473-1000
Internet: www.worldbank.org
All rights reserved.

This volume is a product of the staff and external authors of the World Bank Group. The World Bank Group refers to the member institutions of the World Bank Group: The World Bank (International Bank for Reconstruction and Development); International Finance Corporation (IFC); and Multilateral Investment Guarantee Agency (MIGA), which are separate and distinct legal entities each organized under its respective Articles of Agreement. We encourage use for educational and non-commercial purposes.

The findings, interpretations, and conclusions expressed in this volume do not necessarily reflect the views of the Directors or Executive Directors of the respective institutions of the World Bank Group or the governments they represent. The World Bank Group does not guarantee the accuracy of the data included in this work.

Rights and Permissions

The material in this publication is copyrighted. Copying and/or transmitting portions or all of this work without permission may be a violation of applicable law. The World Bank encourages dissemination of its work and will normally grant permission to reproduce portions of the work promptly.

All queries on rights and licenses, including subsidiary rights, should be addressed to the Office of the Publisher, The World Bank Group, 1818 H Street NW, Washington, DC 20433, USA; fax: 202-522-2422; e-mail: pubrights@worldbank.org.

Photo Credits: Shutterstock

TABLE OF CONTENTS

ACKNOWLEDGEMENTS V

GLOSSARY VII

ABBREVIATIONS AND ACRONYMS XI

EXECUTIVE SUMMARY XIII

INTRODUCTION 1

- Objective 1
- Background and Definitions 1
- Methodology 4

THE ROLE OF DIGITAL IDENTITY IN THE FINANCIAL SECTOR 7

- The Importance of Identity 7
- Important Characteristics of ID for the Financial System 9
- Risks and Challenges in Implementing Digital ID 11
    - Exclusion Risks 11
    - Privacy and Data Protection 11
    - Cost and sustainability 12

APPROACHES TO INTEGRATE ID INTO THE FINANCIAL SECTOR 13

- Using Existing Legal IDs 13
- Private Sector Initiatives 14
- Social Data for Identity Proofing 14
- Blockchain and Digital ID Identity 15

APPLICATIONS OF IDENTITY IN FINANCIAL SERVICES 19
- Account Opening 21
- Customer Authentication 21
  - Personal Identification Number (PIN) 22
  - Smartcards 23
  - Mobile SIM Authentication 23
  - Biometric Based Authentication 24
- Payment Systems and Services 26
  - Combining ID and Payment Applications 26
  - Using the Digital ID Infrastructure for Authentication 26
  - Using the ID Credential as An 'Address' 27
  - Government To Person (G2P) Payments 28
  - Role in Humanitarian Assistance 28
- Credit Reporting 31
- Record-Keeping, Document Management and Digital Signature 32
- Small Businesses 33
- Insurance 34

KEY FINDINGS 37

POLICY CONSIDERATIONS 41

ANNEX 1: LEVELS OF ASSURANCE 45

ANNEX 2: THE IDENTITY LIFECYCLE 47

ANNEX 3: UNHCR ID SYSTEM 51

ANNEX 4: REFUGEE DIGITAL ID CASE STUDIES 53

ANNEX 5: COUNTRY CASE STUDIES 55
- Canada 55
- Mexico 57
- Nigeria 59
- Norway 59
- Pakistan 60
- Peru 61
- United Kingdom 62

ENDNOTES 65

LIST OF BOXES

Box 1: G20 High-Level Principles for Digital Financial Inclusion 1
Box 2: Defining Digital Identity 3
Box 3: Digital Identity and Gender Equality 5
Box 4: Historical Evolution of the Concept of Customer Due Diligence 8
Box 5: Case Studies Highlighting the Benefits of Digital ID to Governments 10
Box 6: Legal IDs: NADRA, Peru ID, Aadhaar, SPID 13
Box 7: Private Sector Initiatives: FIDO, BVN, Gov.UK Verify, BankID 15
Box 8: Case Study: India *'JAM Trinity'* 21
Box 9: Case Study: Peru *'Modelo Pero'* 22
Box 10: Near Field Communication (NFC) and Radio Frequency Identification (RFID) 23
Box 11: GSMA's Mobile Connect 24
Box 12: Cross Border Systems 25
Box 13: Biometrics 25
Box 14: Case Study: Singapore *'SingPass'* 27
Box 15: Case Study: Pakistan *'NADRA'* 27
Box 16: Case Study: Pakistan *'NADRA'* 31
Box 17: Case Study: Norway *'Bank-ID'* 32
Box 18: Case Study: Canada *'BN9'* 33
Box 19: Case Study: Serbia *'UBI Digital ID'* 33
Box 20: Legal Entity Identifier (LEI) 34
Box 21: Case Studies: Estonia 34
Box 22: Case Study: Mexico *'CURP'* 39
Box 23: eiDAS 49

LIST OF FIGURES

Figure 1: Universal Financial Access by 2020 2
Figure 2: Document Type Needed for Account Opening 2
Figure 3: Representation of Digital and Legal IDs and the Overlaps 4
Figure 4: Acceptance of Simplified Customer Due Diligence Requirements 8

Figure 5: Dimensions of ID System Type 9
Figure 6: Lack of Appropriate Identity Characteristics and Its Impact on the Financial System 11
Figure 7: Assessment of Authentication Robustness of Blockchain 17
Figure 8: Financial Service Stages and Phases 19
Figure 9: Benefits of Digital ID 20
Figure 10: Overview of Humanitarian Assistance 28
Figure 11: Digital Identity Lifecycle and Key Roles 47

LIST OF TABLES

Table 1: Comparisons of Different ID Systems for Refugees 29
Table 2: Comparison of ID Registration Processes 30
Table 3: Principle on Identification for Sustainable Development: Towards the Digital Age 40
Table 4: Identification When Signing on Products (Accounts, Loans and Transactions) 58

ACKNOWLEDGEMENTS

This report was written and coordinated by a diverse range of stakeholders across the World Bank Group (WBG), Global Partnership for Financial Inclusion (GPFI) and G20 countries. The WBG, as an Implementing Partner for the Subgroup on Regulation and Standard-Setting Bodies, took leadership on this paper, with involvement from Subgroup members including CGAP (Consultative Group to Assist the poor), DFID (Department of International Development) and other implementing partners. The WBG core team was led by Harish Natarajan and consisted of team members: Sharmista Appaya (lead author) and Sriram Balasubramanian. Vyjayanti Desai, Seth Ayers, Julia Michal Clark, Jonathan Daniel Marskell, Emile De Willebois, Fredesvinda Montes and Margaret Miller (all WBG) provided inputs all through the process and Lauren Kaley Johnson supported on the graphics and publication. Mahesh Uttamchandani provided managerial oversight. Loretta Michaels (WBG), Minita Mary Varghese (WBG) and a Consult Hyperion team led by Paul Makin contributed to the development of the outline, early drafts and research. We are grateful for the leadership and support from the Argentinian G20 representative Gabriel R. Bizama and Francesca Brown (DFID) who chaired the discussions, as well as the GPFI committees, namely the Subgroup on Markets and Payment Systems, the Subgroup on Financial Consumer Protection and Financial Literacy, the Temporary Steering Committee on Forcibly Displaced Persons and the Subgroup on Regulations and SSB, and to the heads and team members of member countries such as Germany, Italy, India, Norway, Mexico, Canada, and the UK, among others. These include Rajesh Kumar Sharma (India), Monika Sethi (India), Hege Rottingen (Norway), Dr. José Luis Negrín (Mexico), Alexandra Rudolph (Germany), Francoise Felipe Dube (Canada), Joni Brennan (Canada), Tim Bouma (Canada) inter alia.

We would also like to thank the following WBG staff and consultants and G20 country representatives for research support and peer review: Anita Mittal (ID4D), Joscha Albert (Germany), Ricardo Settimo (Italy), Fabio Teramo (Italy), Sonia Guida(Italy), Angela Caporrini (Italy), Edgar Cortes (Mexico), Diego Lombardo (Argentina), Nadezhda Prasolova(Russia), Paul Nelson (US AID), Timothy Lyman (CGAP), Nadine Chehadi (CGAP), Antonio Navarro (CGAP), Laura Ellison (DFAT), Maria Do Ceu Pereira (WBG), Matei Dohotaru (WBG), Kuntay Celik (WBG), Emilie Van der Does (WBG), Himanshu (Bill Gates Foundation) and Yannis Theodorou (GSMA). Lastly, we thank Aichin Lim Jones and Amy Quach for overall design and production services.

The findings, interpretations, and conclusions expressed in the paper and case studies are entirely those of the authors. They do not necessarily represent the views of the World Bank Group and its affiliated organizations or those of the Executive Directors of the World Bank or the governments they represent.

D45CB
B84CA
HELP
https://www.

GLOSSARY

Attribute: A named quality or characteristic inherent in or ascribed to someone or something. In identification systems, common personal identity attributes include name, age, sex, place of birth, address, fingerprints, a photo, a signature, an identity number, date and place of registration, etc.[1]

Authentication: The process of proving that a person is who they claim to be. Digital authentication generally involves a person electronically presenting one or more "factors" or "authenticators" to "assert" their identity—that is, to prove that they are the same person to whom the identity or credential was originally issued. These factors can include something a person is (e.g., their fingerprints), knows (e.g., a password or PIN), has (e.g., an ID card, token, or mobile SIM card), or does (e.g., their handwriting, keystrokes, or gestures).[2]

Biometrics: Physical or behavioral attributes of an individual, including fingerprints, irises, facial images, gait, signatures, keystrokes, etc.[3]

Biometric identification: Digital biometric identification involves comparing a template generated from a live biometric sample to a previously stored biometric in order to determine the probability that they are a match. One-to-one (1:1) matching is a comparison against a single template (e.g., one stored on an eID card) and is typically used for authentication and verification. One-to-many (1:N) matching is a comparison against all or a subset of templates stored in a database, and can be used for identification (e.g., a criminal record search) or deduplication (i.e., ensuring that each individual exists only once in the database). In principle, 1:N deduplication allows identity providers to establish statistical uniqueness in a population.[4]

Blockchain: A 'blockchain' is a particular type of data structure used in some distributed ledgers which stores and transmits data in packages called "blocks" that are connected to each other in a digital 'chain'. Blockchains employ cryptographic and algorithmic methods to record and synchronize data across a network in an immutable manner.[5]

Credential: A document, object, or data structure that vouches for the identity of a person through some method of trust and authentication. Common types of identity credentials include—but are not limited to—ID cards, certificates, numbers, passwords, or SIM cards. A biometric identifier can also be used as a credential once it has been registered with the identity provider.[6]

Customer Due Diligence: FATF Recommendation 10 on CDD is based on four pillars, requiring: 1) identification and verification of customers, 2) identification and verification of beneficial owners, 3) understanding the nature and purpose of transactions, 4) monitoring the clients and their transactions on an ongoing basis.

Customer On-Boarding: The process of a financial services provider establishing a business relationship with a customer.

De-duplication: In the context of identification systems, it is a technique to identify duplicate copies of identity data. Biometric data—including fingerprints and iris scans—are commonly used to de-duplicate identities in order to identify false or inconsistent identity claims and to establish uniqueness.[7]

Digital identity: A set of electronically captured and stored attributes and/or credentials that uniquely identify a person.[8]

Digital identification (ID) system: An identification system that uses digital technology throughout the identity lifecycle, including for data capture, validation, storage, and transfer; credential management; and identity verification and authentication.[6]

Distributed Ledger Technology: refers to a novel and fast-evolving approach to recording and sharing data across multiple data stores (or ledgers). This technology allows for transactions and data to be recorded, shared, and synchronized across a distributed network of different network participants.[5]

Foundational identification system: An identification system primarily created to provide general identification and credentials to the population for public administration and a wide variety of public and private sector transactions, services, and derivative credentials. Common types of foundational ID systems include civil registries, national IDs, universal resident ID systems, and population registers.[9]

Functional identification system: An identification system created to manage the identity lifecycle for a particular service or transaction, such as voting, tax administration, social programs and transfers, financial services, and more. Functional identity credentials—such as voter IDs, health and insurance records, tax ID numbers, ration cards, driver's licenses, etc.—may be commonly accepted as proof of identity for broader purposes outside of their original intent, particularly when there is no foundational ID system.[9]

Identification: The process of establishing, determining, or recognizing a person's identity.[7]

Identification (ID) system: The databases, processes, technology, credentials, and legal frameworks associated with the capture, management, and use of personal identity data for a general or specific purpose.[10]

Identity: A set of attributes that uniquely identify a person.[10]

Identity lifecycle: The process of registering, issuing, using and managing personal identities, including enrollment of identity data; validation through identity proofing and deduplication; issuing credentials; verification and authentication for transactions; and updating and/or revoking identities and credentials.[6]

Identifiers: Unique data used to represent a person's identity and associated attributes. A name or a card number are examples of identifiers.[11]

Interoperability: The ability of databases, devices, or systems to talk with each other, exchanging information or queries. In some cases, interoperable databases or systems may be directly connected, allowing for the real-time exchange or updating of information; in others, databases or systems may be interoperable via a trusted third-party exchange layer that facilitates communication across disparate systems.[4]

KYC Registry: A KYC Registry refers to a centralized repository of CDD records of customers in the financial sector. It allows inter-usability of the CDD records across the sector with the objective to reduce the burden of producing CDD documents and getting those verified each time the customer creates a new relationship with a financial entity.

Legal Entity Identifier: A 20-character, alpha-numeric code, to uniquely identify legally distinct entities that engage in financial transactions.[12] The organizational structure of the LEI consists of a federated group of registrars, Local Operating Units (LOUs); a central operational body, the Global LEI Foundation (GLEIF); and a regulatory body charged with oversight of the LEIs, the Regulatory Oversight Committee (ROC). The GLEIF is a Swiss foundation inaugurated in June 2014 and founded by the Financial Stability Board (FSB). It is overseen by 70 global regulators in the Regulatory Oversight Committee (ROC).

Legal identification (ID) system: Identification systems that register and identify individuals to provide government-recognized credentials (e.g., identifying numbers, cards, digital certificates, etc.) that can be used as proof of identity.[13]

Levels of Assurance: The ability to determine, with some level of certainty or assurance (LOA), that a claim to a particular identity made by some person or entity can be trusted to actually be the claimant's "true" identity. Each LOA is broken down into three component parts that are scored individually. Please refer to Annex 1

Protocol: Set of rules and formats, semantic (meaning), and syntactic (format), that enable information systems to exchange information.[14]

Relying Party: An individual or organization that relies on another party to verify the identity of the user; the validity of the public key, associated algorithms and any relevant parameters; and the user's possession of the corresponding private key.[15]

Revocation: The process of permanently ending the binding between a certificate and the identity asserted in the certificate from a specified time forward.[16]

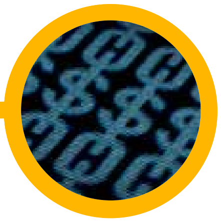
Self-Sovereign Identity: The concept of a lifetime portable digital identity, completely controlled by the individual, that does not depend on any central authority and can never be taken away.[17]

Unique ID number (UIN): In the context of identification systems, a number that uniquely identifies a person—i.e., each person only has one UIN and no two people share the same UIN—for their lifetime. UINs are typically assigned after validating a person's identity and statistical uniqueness through a process such as biometric deduplication.

User: Individual or (system) process authorized to access an information system.[14]

Verification: The process of confirming or denying that a claimed identity is correct by comparing the credentials (something you know, something you have, something you are) of a person requesting access with those previously proven and stored and associated with the identity being claimed.[18]

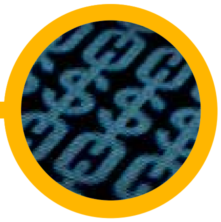
Protected



ABBREVIATIONS AND ACRONYMS

AI	Artificial Intelligence
AEBA	Aadhaar Enabled Bank Accounts
API	Application Programming Interface
AML	Anti-Money Laundering
APB	Aadhar payment bridge system
BVN	Bank Verification Number
CBN	Central Bank of Nigeria
CDD	Customer Due Diligence
CFT	Combating the Financing of Terrorism CNIC Computerized National Identity Card
CRS	Credit reporting systems
CTF	Combating Terrorist Financing; an alternative acronym to CFT
DBT	Direct Benefit Transfer
DFS	Digital Financial Services
DLT	Distributed Ledger Technology
eCIB	Electronic Credit Information Bureau
eIDAS	electronic Identification, Authentication and Trust Services
EU	European Union
FATF	Financial Action Task Force
FIDO	Fast Identity Online (Alliance)
FinTech	Technology application to finance
FSB	Financial Stability Board
FSP	Financial Service Provider
G20	Group of Twenty
G2P	Government to Person
GPCR	General Principles for Credit Reporting
GSMA	Groupe Spéciale Mobile Association
GPFI	Global partnership for Financial Inclusion
ICAO	International Civil Aviation Organization
ID	Identity
ID4D	Identity for Development

ICCR	International Committee on Credit Reporting
IIN	Institution Identification Number
ISO	International Organization for Standardization
ITU	International Telecommunications Union
KRA	Know Your Client Registration Agency
KYC	Know Your Customer
LEI	Legal Entity Identifier
LOA	Levels of Assurance
MF-CIB	Microfinance Credit Information Bureau
MMO	Mobile Money Operator
MNO	Mobile Network Operator
MSME	Micro, Small and Medium Enterprises
NADRA	National Database and Registration Agency (Pakistan)
NFC	Near Field Communication
NIMC	National Identity Management Commission
NIRA	National Identification and Registration Agency
NIST	National Institute of Standards and Technology, US Department of Commerce
NPCI	National Payments Corporation of India
PASA	The Payments Association of South Africa
PIN	Personal Identification Number
PoS	Point of Sale
RAIS	Refugee Assistance Information System
RBI	Reserve Bank of India
RENIEC	National Registry of Identification and Civil Status (in Spanish, Registro Nacional de Identificación y Estado Civil)
Regtech	Technology as applied to regulation
RIMS	Refugee Information Management System
RFID	Radio frequency identification
RSD	Refugee status determination
SCA	Strong customer authentication
SDG	Sustainable Development Goals
SEBI	Securities and Exchange Board of India
SIM	Subscriber Identity Module
SSID	Self-sovereign identity
UFA	Universal Financial Access
UIDAI	Unique Identification Authority of India
UIN	Unique Identification number
UNHCR	United Nations High Commissioner for Refugees
UNRWA	United Nations Relief and Works Agency for Palestine Refugees in the Near East



EXECUTIVE SUMMARY

A unique, legal identity is necessary to allow all individuals to participate fully in society and the economy. The ability to prove one's identity underlies the ability to access basic services and entitlements from healthcare through to pensions and agriculture subsidies. This is especially true for marginalized segments of society such as women, poor rural farmers, refugees and also extends to MSMEs (micro, small and medium enterprises). The importance of legal identity has been acknowledged by the international community through agreement of target 16.9 of the Sustainable Development Goals, which calls for all UN member States to "provide legal identity for all, including birth registration" by 2030.

National and subnational governments play a primary role in the registration and recognition of a legal identity. Without such official recognition, the authenticity of an identity may lack a formal or legal basis (referred to as legal ID in this document). However, a number of developing countries have no robust official legal ID system that is universally available. The inability to credibly prove one's identity can be a source of economic, political and social exclusion. In the financial sector, it hampers access to basic services such as bank accounts and loans.

According to the 2017 Global Findex Survey, the lack of documentation was the primary barrier to access to financial services cited by 26 percent of unbanked individuals in low income countries. Beyond extending legal ID in order to address these gaps, the introduction of a legal, digital ID could potentially increase the adoption of financial services, furthering the financial inclusion agenda and supporting development goals. Digital ID lowers barriers by: a) making it easier for the unbanked to open a transaction account[19] in conjunction with simplifying documentation requirements, b) enabling more cost-effective customer onboarding that can be conducted remotely and c) contributing to financial sector embedding by supporting the delivery of additional services to the individual.

Governments are adopting electronic means of cash transfer to streamline processes and prevent leakage. Digital IDs can substantially strengthen the efficiency and effectiveness of the state in providing critical services such as Government to Person (G2P) payments and supporting the provision of humanitarian aid. A legal digital ID for those forcibly displaced not only provides them with a sense of identity but also supports efficient benefit distribution reducing fraud and duplication while allowing them to participate in the real economy. Another vulnerable population especially bolstered by a digital ID is women; while a legal ID is seen as increasingly essential to both men and women to drive socio-economic development, of the 1 billion[20] people without access to an ID, a disproportionate number are women and girls. The 2017 Global Findex survey found that the poorest 40 percent of women in low income countries are less at least 30 per cent less likely to have an ID than men in the same wealth quintiles. The absence of ID documents is both, an effect and the cause of gender inequalities. A universal ID with digital capabilities will enable women to open accounts at low cost and will also substantially reduce the cost for the financial services providers (FSP). Digital ID also has clear benefits for small businesses. This is relevant at both the level of the company directors and senior management as well as at the level of the entity, helping reduce costs and time for registration as well as introducing efficiencies in conducting financial transactions.

This report analyzes the role that robust, inclusive and responsible ID systems can play in enhancing financial access and inclusion. With a focus on digital ID, this paper is intended to guide interventions at country level and outlines some key policy considerations. Building on previous work by the Global partnership for Financial Inclusion (GPFI) and World Bank Group, adhering to the mandate set by the Group of 20 (G20), the report looks at how financial services can leverage digital ID systems to increase efficiency, enhance effectiveness and enable new ways of conducting existing business processes in the financial sector. The analysis is underpinned by the 'G20 High-Level Principles of Digital Financial Inclusion'[21] (HLP) and the 'Principles on Identification for Sustainable Development'[22] developed by the World Bank Group and endorsed by over 20 international organizations and development agencies since 2017. Principle 7 of the G20 HLP specifically refers to ID and will form the guiding principle for this report.

Three characteristics of an identification system that matter most for financial services are a **legal** basis, **uniqueness** and the ability to exist in a **digita**l format. Digital IDs are important to broaden public policy, especially for financial inclusion and can help bring more MSMEs into the formal financial sector. It needs to be noted that there are several other implicit aspects that are essential, notably that the ID should be robust and secure. In many jurisdictions, not all IDs have all the attributes, and even those that possess them might not have universal coverage in the jurisdiction. The analysis points out, that while the absence of any form of legal ID impacts all access to basic financial services, a lack of unique ID obscures a reliable view of customer activity and can impact access to the full range of financial services, especially credit and insurance. Meanwhile, the lack of a unique digital ID increases the costs of providing financial services to certain segments of society, thereby impacting financial inclusion. Finally, for financial inclusion and inclusion more broadly, universal coverage of legal ID in a given jurisdiction is paramount. Traditionally, countries have two types of ID systems: *foundational ID systems*, which are typically the source of 'legal identity documents' and provide proof of legal identity in accordance with national law- these can include civil registries and unique national IDs; and *functional ID systems*, which cover population subsets and are introduced in response to a demand for a particular service or transaction such as voter registration and can, in some cases, provide proof of legal identity including serving as a *de facto* national ID when a national ID system does not exist.[23] On the proviso that an identity has uniqueness and a legal basis, with universal coverage (either at an individual level or collectively across all IDs in the jurisdiction) then, there is potential for the government or private sector entities to overlay them with digital features.

Digital IDs however, come with risks which need to be managed and mitigated to build trust and harness the benefits of identification responsibly. Foremost among the risks that arise, is the issue of data privacy and the potential for leakage, theft or misuse of personal data and the risks that arise from non-regulated players outside the traditional financial system. It is of vital importance to secure the data while at rest and in transit. The appropriate classification of data and adherence to data governance rules and procedures are the main ways that this can be contained. Data classification and its associated rules ensure that the more sensitive the data, the more stringent the security controls and the rules regarding the access and sharing of the data; hence, the process of classifying and categorizing data is imperative to maintaining a robust digital ID framework. While the high initial infrastructure cost is a hurdle that must be crossed, the importance of having a robust and effectively functioning system instead of several suboptimal initiatives cannot be stressed enough. Another important challenge that merits consideration is the rapidly evolving nature of the technologies, and it is important that central authorities and public bodies consistently incorporate new technologies and business models while protecting the financial sector and its customers.

Digital ID has immense potential and it is important that country's financial service supervisory framework recognizes this. Financial sector regulations, specifically those related to AML/CFT, have longstanding requirements related to identity validation, authentication and retention of records, to ensure the safety and integrity of the financial system, based in large part on the Financial Action Task Force (FATF)[24] recommendations. Furthermore, of the ten Principles on Identification for Sustainable Development,[25] three specifically focus on the issue of governance, including of the regulatory framework.

Seven policy measures, that governments should consider in order to have an identity effective ID system that meets the needs of the financial sector, have been identified:

1. **Ensure an integrated identity framework;**
2. **Consider the appropriateness of the regulatory framework to capture the challenges related to digital ID, and risks to its appropriate implementation; deliberate updates to the regulatory framework including the issuance of new regulations where necessary;**
3. **Establish a reliable oversight model to include stakeholders beyond the traditionally regulated financial institutions who can introduce risks to digital identity systems;**

4. **Build authentication and service delivery systems that protect user privacy, and provide individuals with the right to access rheir data and oversight over how their data is shared;**
5. **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;**
6. **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;**
7. **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.**

The report is divided into four broad sections; first, the section on the role and need for digital ID focusses on the importance, principles, characteristics, risks and challenges of digital ID in the financial sector as related to the G20 HLP and the Principles on Identification. Next, the paper delves into the approaches of how ID could be successfully integrated into the financial sector from the use of government issued ID to private sector initiatives as well as social ID proofing and the role of blockchain. We then move onto the applications of digital ID and the different authentication techniques available from the traditional to the more advanced. The aim of this section is to provide a comprehensive perspective of the several authentication techniques and the varied applications of digital ID which include payments systems and services, credit reporting, insurance, document management and digital signatures, ID for small businesses as well as the role of ID in humanitarian assistance. The paper seeks to showcase the multifaceted nature of applications for digital ID in the financial sector with strong emphasis on examples from country specific case studies. The last two chapters focus on the synthesis of key findings from public and private sector initiatives in digital ID and finally key policy recommendations for consideration.

The process of showcasing the fundamentals of digital ID and applications in both private and public enterprises, with country specific case studies examples throughout, helps the authors identify specific policy interventions which can boost implementation and usage of digital ID and positively impact the financial sector.

https:/

INTRODUCTION

Objective

The G20 recognizes the key role of financial inclusion in supporting the move towards an Innovative, Invigorated, Interconnected and Inclusive World Economy.[21] The World Bank Group was requested by its G20 partners under the 2018 Argentine presidency, to produce this report as part of the Global Partnership for Financial Inclusion (GPFI) forum- an inclusive platform to carry forward work on financial inclusion.

The primary objective of this paper is to analyze the role of a robust, inclusive and responsible digital identification system in financial sector development; in particular, the role it plays in furthering global financial inclusion commitments. This paper will provide insights and recommendations for country-level implementation by policymakers in line with Principle 7 of the G20 HLP developed by the GPFI.

This report is neither intended to inform nor interpret the work of the global financial sector standard-setting bodies.

Background and Definitions

The GPFI, the Alliance for Financial Inclusion (AFI) as well as several other multilateral forums have advocated and launched initiatives for furthering financial inclusion. Financial inclusion is one of the critical drivers of poverty reduction and economic growth in emerging markets and developing economies. Currently, an estimated 1.7 billion adults globally do not have access to the formal financial economy. Virtually all these unbanked adults live in the developing world. Indeed, nearly half live in just seven developing economies: Bangladesh, China, India, Indonesia, Mexico, Nigeria, and Pakistan.[26] The World Bank Group in partnership with public and private sector institutions set an ambitious target to achieve Universal Financial Access (UFA) for adults globally to a have access to a transaction account[27] to store money and send and receive payments by 2020 as a stepping stone to broader financial inclusion.[28]

A transaction account is a foundation for financial inclusion because it serves as a gateway to other financial services including savings, insurance, and credit. One of the primary barriers to opening a transaction account is the ability to prove one's identity.

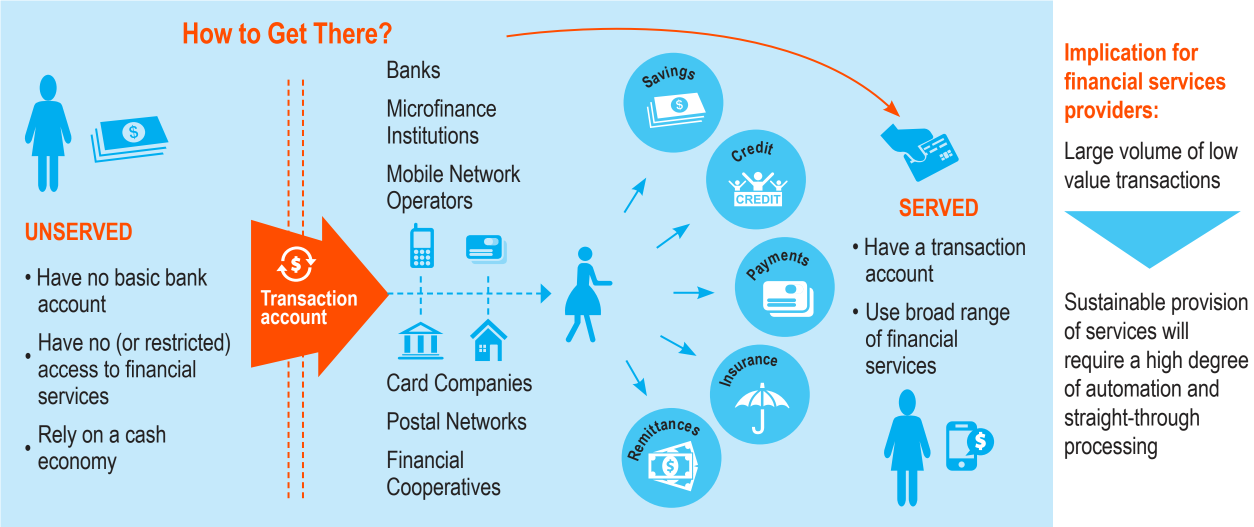
Proof of identity is required for the financial service provider (FSP) to verify who the customer is. As such, the lack of trusted IDs remains one of the chief obstacles to financial inclusion across the world. The 2017 Global Findex data shows that in the developing world, the share of adults with a transaction account varies from about 15 percent in parts of Sub- Saharan Africa, going up marginally to 20 percent in Cambodia, Mauritania and Pakistan. Of those individuals without an account,

Box 1: G20 High-Level Principles for Digital Financial Inclusion

Principle 7: Facilitate Customer Identification for Digital Financial Services

Facilitate access to digital financial services by developing or encouraging the development of customer identity systems, products and services that are accessible, affordable, and verifiable and accommodate multiple needs and risk levels for a risk-based approach to customer due diligence.

Figure 1: Universal financial Access by 2020


How to Get There?
UNSERVED
• Have no basic bank account
• Have no (or restricted) access to financial services
• Rely on a cash economy
Transaction account
Banks
Microfinance Institutions
Mobile Network Operators
Card Companies
Postal Networks
Financial Cooperatives
Savings
Credit
CREDIT
Payments
Insurance
Remittances
SERVED
• Have a transaction account
• Use broad range of financial services
Implication for financial services providers:
Large volume of low value transactions
Sustainable provision of services will require a high degree of automation and straight-through processing

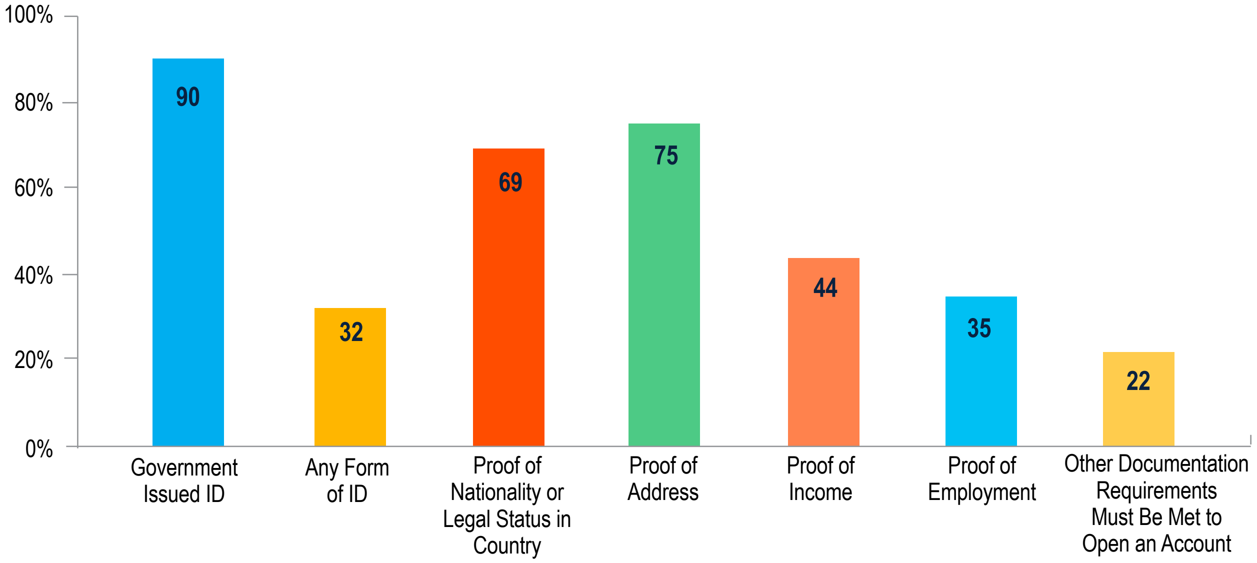
Source: UFA2020 Overview- World Bank

26 percent for unbanked adults in low income countries, and 19 per cent in developing countries cited the lack of documentation as the main barrier.[29] 30 percent reported that financial institutions are too far away. This has been to some extent mitigated by opening the market to non-bank players; however, this will only be successful and reduce financial services barriers only if such non-bank players have lower/different identification requirements. Beyond access to documentation, the high cost incurred in validating to the appropriate degree, identity documents constrain FSPs in expanding access to finance and hence, stunts financial inclusion. When the identity authentication can be carried out automatically using technology, this reduces costs for FSPs and enables the use of agents, which also reduces distance.

The following graph depicts the different documentation requirements required for opening a transaction account as based on data collected from 124 separate jurisdictions.

Figure 2: Document Type Needed for Account Opening

% of responding jurisdictions that require documentation type to open an account at a Commercial Bank



Source: 2017 Global Financial Inclusion & Consumer Protection (FICP) Survey, WBG. 124 jurisdictions participated in the survey

Many jurisdictions require customers to provide additional information beyond basic identification in order to open an account.

However, the ability to securely validate and verify a customer's details against a reliable database remains imperative, and a large portion of those in the developing world lack basic IDs. The ability to prove one's identity is increasingly recognized as the basis for participation in social, political, economic, and cultural life. Yet, the World Bank estimates that more than 1.1 billion individuals do not have any form of officially recognized ID.[30] This problem disproportionally impacts rural residents, poor people, women, children, and other vulnerable groups.[31] Furthermore, poor identification systems mean that states have difficulty collecting taxes, targeting social programs, and ensuring security. Achieving inclusive development therefore requires a sustained effort to address the world's identity gap. These goals have been recognized in the 2030 Sustainable Development Goals (specifically SDG 16.9) and by other multilateral bodies.

Globally, various efforts have been undertaken to address the inability to access the financial system, from less arduous requirements regarding customer identity - such as only requiring a functional ID such as a paper-based voter's registration card or an introduction from a respected member of the community-, to separate categories of transaction accounts with lower documentation requirements and opening up the market to non-bank players to expand the pool of suppliers. However, a sizable portion of those in the developing world lack basic IDs, and the ability to securely validate and verify a customer's details against a verifiable database remains imperative. The introduction of a unique, reliable—and particularly—digital ID could provide universal coverage while enabling more efficient processes for validating ID documentation, for example by enabling system based online validation including validation at agent locations. Identity includes not only the original acquisition of identity credentials, but also the many aspects of how and why that identity is used and maintained.

As the issuance of identity grows in importance for policymakers, regulators and the private industry, various reports use different terms and definitions. It is therefore important to clarify the terminology used in this report. As mentioned previously, traditionally, countries have two types of ID systems: *foundational ID systems*, which provide general identification covering the entire population these include birth certificates, identity cards, unique identity numbers or digital certificates,[33] and functional ID systems, which usually cover population subsets. Moreover, a non-public authority issued identity, if recognized as valid by the government as a proof of identity, would be included in the definition of legal ID. It is important to note that under this inclusive definition, legal ID need not be linked with nationality or citizenship. The uniqueness of the ID (i.e.) the ability to relate an ID to a singular person (or entity) and one person receiving only one such ID is paramount to ensure the usefulness of the ID.

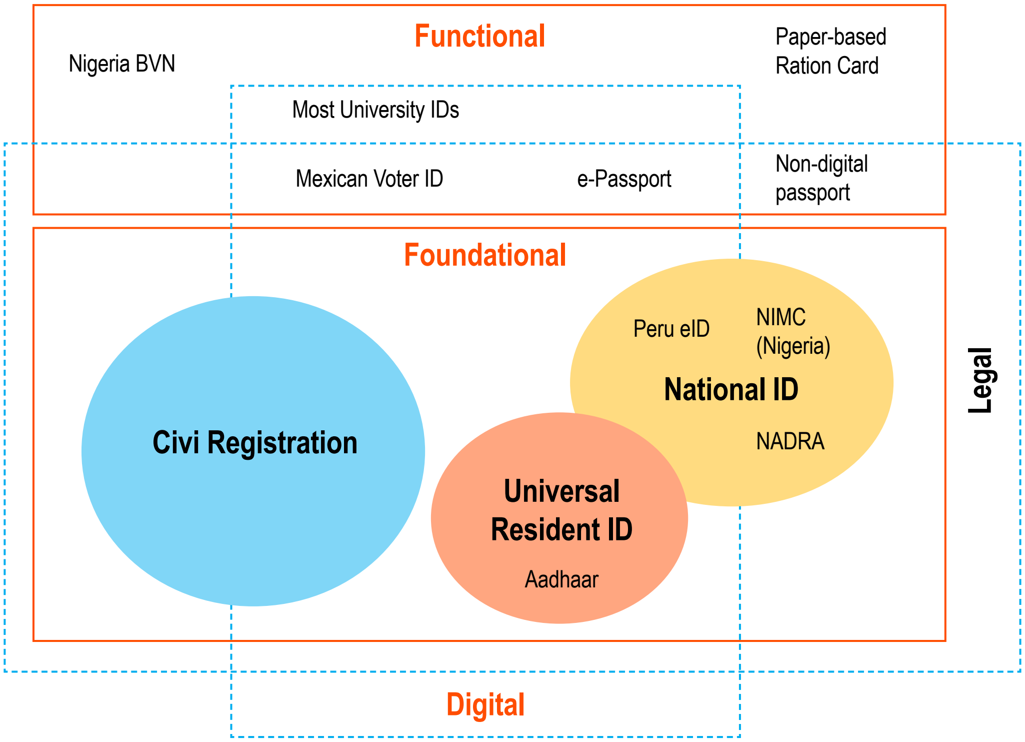
While this report considers identity as a whole and its role in financial inclusion, particular focus has been placed on digital ID and the emerging areas in the financial sector where identity systems can be leveraged to increase efficiency, enhance effectiveness and enable innovative ways of conducting existing business processes. Notably, digital ID is increasingly becoming central to the effectiveness of technology innovations like open banking and marketplace lending; both of which have impacts on financial inclusion by enabling customers to securely share their banking data with trusted third parties, giving

Box 2: Defining Digital Identity[32]

A **digital identity** is a collection of electronically captured and stored identity attributes that uniquely describe a person within a given context and is used for electronic transactions. It provides remote assurance that the person is who they purport to be. A digital identification system refers to the systems and processes that manage the lifecycle of individual digital identities.

A person's digital identity may be composed of a variety of attributes, including biographic data (e.g., name, age, gender, address) and biometric data (e.g., fingerprints, iris scans, hand prints) as well as other attributes that are more broadly related to what the person does or something someone else knows about the individual. When these data are collected and verified, they can be used to identify a person by answering the question "who are you?". These attributes, along with credentials issued by the service provider (e.g., unique ID number, eDocument, eID, mobile ID) can then also be used as authentication factors to answer the question "are you who you claim to be?". The attributes and authentication factors used in a digital identity may vary from one context or country to the next depending on the type of identity system.

Figure 3: Representation of Digital and Legal IDs and the Overlaps


Functional
Nigeria BVN
Paper-based Ration Card
Most University IDs
Mexican Voter ID
e-Passport
Non-digital passport
Foundational
Civi Registration
Peru eID
NIMC (Nigeria)
National ID
NADRA
Universal Resident ID
Aadhaar
Legal
Digital

Source: Adapted from ID4D glossary, WBG May 2018.

rise to a new generation of tools that will help individuals make better decisions based on their data.

Digital ID, combined with the extensive use of mobile devices in the developing world, offers a transformative solution to this global challenge and promotes efficiency gains, financial savings, social inclusion and access to basic services and rights. However, they come with their own unique set of challenges especially that of data protection, privacy and a sustainable business model. These are elaborated further in the document.

Moreover, digital ID has been instrumental in playing a key role in reducing gender gaps in various societies, especially in emerging markets and developing countries. The following box item provides an overview of its benefits:

Methodology

Analysis of developments in different country settings, current views on best practices and dialogue with key stakeholders have informed this report. Country specific case studies have contributed to the understanding of the application and role of ID in the financial sector. Interpretation of international practices, specifically the FATF Recommendation 10, has strongly influenced the policy considerations put forward. It should be noted, however, that case studies have been chosen to showcase and to compare and contrast market practices, and that their inclusion does not necessarily endorse them as examples of best practice.

This report also discusses some private sector led digital initiatives, including those by FIDO (Fast Identity

Box 3: Digital Identity and Gender Equality

The widespread lack of official identification in developing countries disproportionality affects women and girls due to higher barriers they face for obtaining an ID. The 2017 Global Findex [27] report indicates that women in developing economies remain 9 percentage points less likely than men to have a bank account. While lack of sufficient funds is the most commonly cited reason reported by more than half of unbanked adult women, a large proportion also cite the lack of documentation as another key reason. The other barriers include distances involved, along with the restrictions on the freedom to travel, opposition from family members, financial cost, time constraints and illiteracy combined with the lack of awareness. An efficient digital ID system has the ability to overcome the most common barriers to opening a bank account.

In combination with simplified CDD, digital ID enables women to more easily open transaction accounts and when combined with agent models also enables easier access to account services. A digital ID can also empower women to register to vote, claim inheritance rights, register the ownership of business and land and access government benefits and services.

With the use of digital ID, governments can transfer G2P payments, intended for women, directly into their accounts. For example, in Pakistan, the use of biometric IDs is a precondition for accessing cash transfer programs, ensuring that payments to female beneficiaries are delivered directly to them rather than to their husbands or brothers- as was traditionally the case. Not only did this boost their social standing, it also served as trigger for greater social freedoms within their societies.[34]

The use of these digitized G2P payments together with the integration with mobile platforms holds great promise for the achievement of financial independence for women. More than 80 percent of women in Kenya now have access to a mobile account which is being increasingly leveraged to reduce the gender gap.[26] Through the integration of digital ID and mobile money (M-Pesa), substantial progress has been made in enabling women to gain access to social protection and financial saving schemes.[35]

As an additional benefit, the use of a digital ID can help authorities better monitor gender targets via the use of electronic databases and the collection of transaction data remotely, supporting the ability to provide better oversight and monitoring of national targets.

Online) Alliance – created by a consortium of private sector players to achieve interoperability between authentication mechanisms, Mobile Connect - a GSMA initiative and Digital Identification and Authentication Council of Canada (DIACC). The paper delves into the identity solutions that leverage these private sector initiatives and looks at the fundamental dependence on an individual's ability to present a legal ID on which basis the digital ID is created.

This report covers digital ID as applicable to all financial services provided by banks and non-banks including e-money services and microfinance institutions, with a focus on those areas most pertinent to financial inclusion.

The use of digital ID in the humanitarian context and the operational efficiencies it provides is also studied. In addition, developments on the horizon such as social data derived identity and applications of innovative technologies including distributed ledger technologies in identity management are briefly discussed.

This note builds on previous work by the World Bank, specifically the note on Technology Landscape for Digital Identification published by ID4D,[36] which explores the technology linkages between unique IDs, the permeation of digital IDs, digital onboarding and customer identification in the financial sector,[37] the G20 HLP and discussions with GPFI membership.

» SECUR

THE ROLE OF DIGITAL IDENTITY IN THE FINANCIAL SECTOR

The Importance of Identity

In 2016, the G20 endorsed the High-Level Principles for Digital Financial Inclusion which specifically asked that ‘Governments worldwide acknowledge the importance of identity as a fundamental necessity for daily life. For approximately 1.1 billion people,[38] the majority of them living in Asia and Africa, the inability to prove their identity prevents them from accessing basic services, enjoying their full rights, and participating in the formal economy.

Evidence shows that individuals who lack official forms of identification are typically the most vulnerable people in the poorest countries. The recent Global Findex Report[26] cites that 26 percent of unbanked adults in low income countries, and 19 per cent in developing countries without an account at a financial institution reported lacking the documentation needed to open one. Lack of ID was an even more commonly-cited barrier in countries like Zambia (35 percent), the Philippines (45 percent), and Zimbabwe (49 percent). Inclusive, robust, and responsible legal ID systems are needed to close this gap. Beyond paper-based legal ID systems, however, digital IDs have additional benefits, including the potential to provide entities with new and efficient ways to reach and serve their populations, especially the poorest and most disadvantaged. Identity systems that have universal coverage, have a legal basis and ensure uniqueness—as noted previously—also play an important role in the improvement of government efficiency, accountability and transparency. Further, through online transactions and other e-services, digital capabilities of these systems reduce operational costs and the corruption and theft that can occur in paper-based systems, such as entitlement payments siphoned off from their intended recipients.[39] As countries increasingly rely on digital networks for delivering important public and private services, the ability of consumers to remotely access those services through digital identification becomes acutely important.

Accessible, robust, and verifiable ID systems can help service providers carry out Customer Due Diligence (CDD) requirements and expand the use of financial services. One of the key components of financial inclusion strategies in many countries is to introduce a basic account—offered by either banks or non-bank entities—with very stringent limits on number of transactions and value of transactions. The main objective behind introducing this type of account is to prevent identity theft, financial fraud, money laundering and terrorist financing, while at the same time enhancing access to transaction accounts. A digital ID enables an efficient means of meeting the CDD needs for a basic account and further it enables enforcing transaction limits and monitoring how many accounts a person has.

The Reserve Bank of India has permitted the Entities regulated under it to accept Aadhaar identification number issued by the Government of India as proof of identity as well as address to meet the regulatory CDD requirements of opening accounts. Including the Jan-Dhan[40] basic savings accounts.[41] In Pakistan, the national ID cards allowed opening bank accounts and reliably enforcing transaction limits, which coupled with growth of branchless banking agents, contributed to an increase in financial inclusion. Incidentally, the agents were also leveraged to register all cellphone SIM cards as part of a national security initiative.

Box 4: Historical Evolution of the Concept of Customer Due Diligence

The Financial Action Task Force (FATF) 40 recommendations, which constitute the international standards on anti-money laundering and counter-terrorist financing, were first issued in 1990. The first version of the FATF 40 Recommendations included a section on 'Customer Identification and Record Keeping'. The section had a limited scope that focused on identifying and verifying the customers and the beneficial owners of the legal persons and financial transactions.

The FATF Recommendations have gone through major revisions in 1996, 2001*, 2003, and 2012. The limited and relatively static scope of customer identification in the 1990 version was expanded during these revisions, evolving towards a much more comprehensive and dynamic set of requirements. FATF introduced the concept of "Customer Due Diligence" (CDD) in the 2003 Recommendations to define the full range of requirements that aims to understand, know, and monitor all natural and legal person clients, their transactions, and beneficial owners. The CDD concept has been maintained by the current version of the FATF Recommendations (2012) with further refinements.

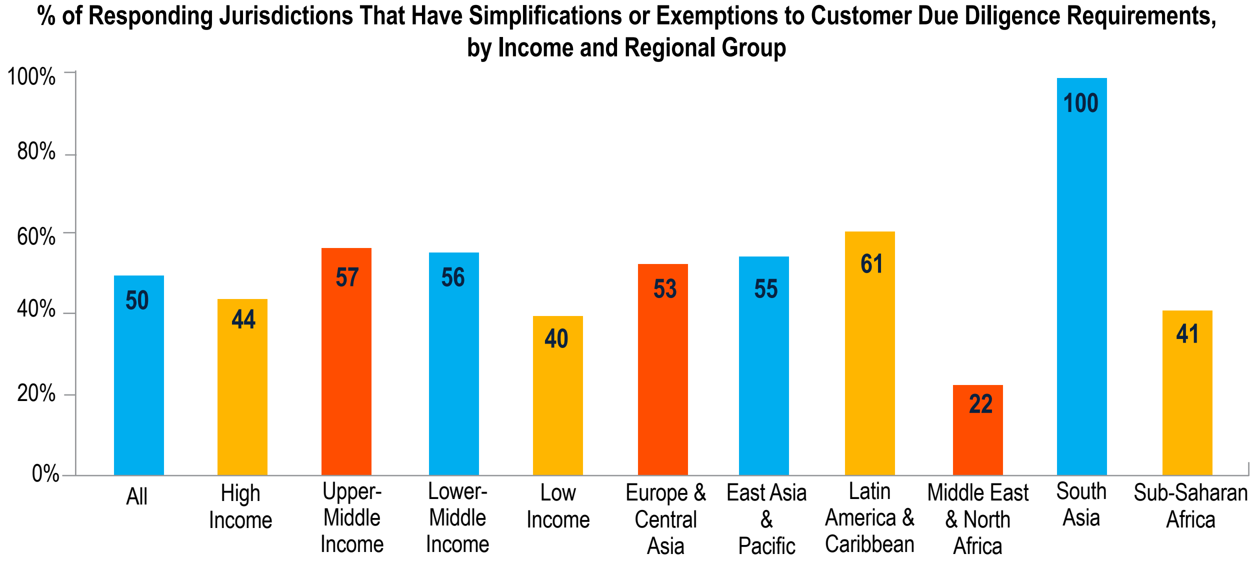
Currently, FATF Recommendation 10 on CDD is the most comprehensive and elaborate among the 40 Recommendations. It is based on four pillars, requiring: 1) identification and verification of customers, 2) identification and verification of beneficial owners, 3) understanding the nature and purpose of transactions, 4) monitoring the clients and their transactions on an ongoing basis.

The term "Know Your Customer" has been used widely by some government authorities and the private sector since the 1990s to express the broader set of requirements that go beyond identification and verification. However, this term has never been officially used or defined by the FATF Recommendations. There fore, the meaning attributed to KYC can differ based on users and national contexts.

*In 2001, with the addition of 8 (later 9) special recommendations the mandate of the FATF Recommendations has been expanded to counter-terrorist financing.

The graph below shows that a significant amount of exceptions are made to CDD requirements in the 120 different jurisdictions sampled. While all responding jurisdictions in the South Asia region report that FSPs—mainly banks- have simplifications or exemptions in place; in the Middle-East and North Africa region, only 22 percent of jurisdictions indicate that similar simplifications exist. A digital ID can provide a unified CDD regime. This means that once a CDD check is conducted for a person linked with a digital identity, the identity and its corresponding check can be held on a KYC registry (see glossary). Later, should that individual wish to

Figure 4: Acceptance of Simplified Customer Due Diligence Requirements



Source: 2017 Global Financial Inclusion & Consumer Protection (FICP) Survey, WBG subscribe to a new financial product or service, they will not need to go through the burdensome process of submitting various documents to prove their identity again.

It is important to note here that information collected and verified for CDD purposes can be extensive and a KYC registry might not have all the required or up-to-date information highlighting the need for effective supervision and oversight of KYC registries and third-party identity services by the financial sector authorities and FSPs to conduct their own due diligence. KYC registries can enforce transaction limits for individuals across all FSPs and this has been illustrated through the use of mobile money platforms in Jordon (JoMoPay) and Peru. This mitigating measure can provide financial sector authorities with a great degree of confidence in mitigating risks from AML/CFT measures.

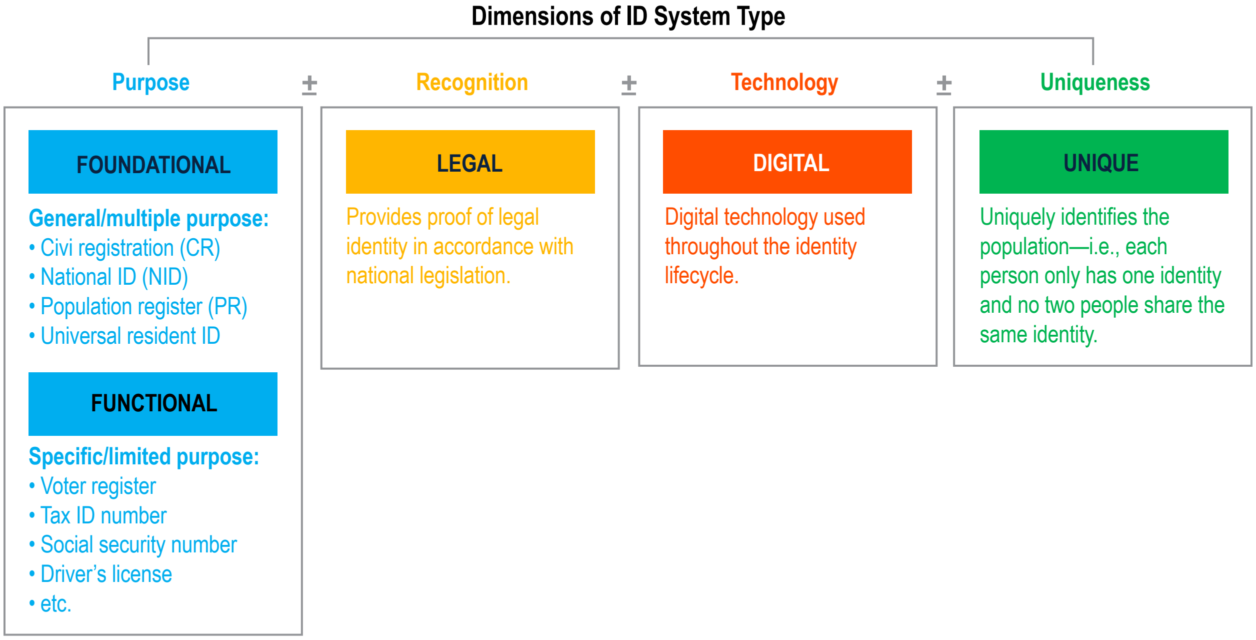
Simplifying CDD however, does not do away with physical, in person applications and verification of an acceptable form of ID. Paper records will often still need to be maintained to provide a document trail for audits. Both the verification and paper records add additional costs to the process. Further, there is also the risk of fraudulent documents and the ability to evade controls if there is no assurance of a customer's unique identity. The introduction of a digital ID solves both the issue of costs as well as the security and reliability concerns. Even if the verification is done in person, the digital process can reliably prove that validation was completed. Furthermore, efforts to enhance flexibility on where and who can open an account can be accelerated with a reliable digital ID system. Thus, a digital ID can empower financial sector regulators and public authorities to simplify the CDD requirements and thus removing one of the enduring barriers to expanding financial inclusion.

Important Characteristics of ID for the Financial System

There are three main characteristics of an identification system/credential that matter most for financial services and transactions: (1) *legality*, (2) *uniqueness* and (3) the ability to be in a *digital format*, each of which has implications on the quality and utility of the identity within the financial sector. These characteristics are not mutually exclusive, and an ID credential can possess one or all of these characteristics to varying degrees.

Legal: National and local governments play the primary role in issuing legal identity documents—those recognized as providing proof of legal identity in accordance with national law. Without such official recognition, the value of an identity credential may lack a formal or legal basis, and therefore be unreliable for CDD checks in the financial sector. However, as mentioned

Figure 5: Dimensions of ID System Type


Dimensions of ID System Type
Purpose
+
Recognition
+
Technology
+
Uniqueness
FOUNDATIONAL
General/multiple purpose:
• Civi registration (CR)
• National ID (NID)
• Population register (PR)
• Universal resident ID
FUNCTIONAL
Specific/limited purpose:
• Voter register
• Tax ID number
• Social security number
• Driver's license
• etc.
LEGAL
Provides proof of legal identity in accordance with national legislation.
DIGITAL
Digital technology used throughout the identity lifecycle.
UNIQUE
Uniquely identifies the population—i.e., each person only has one identity and no two people share the same identity.

Source: ID4D Glossary: Definitions and Usage, May 2018.

previously, sometimes an ID issued by a private entity can become a legal ID if the government recognizes the validity of it.

Generally, jurisdictions require an individual to have a form of legal ID to open and operate a transaction account, the most basic of financial services. A lack of suitable legal identity restricts this access and as such access to the wider financial ecosystem contributing to financial exclusion.

Uniqueness: FSPs prefer to use an identity credential that has the characteristic of being 'unique'—i.e., that no individual (or entity) will have the same identifier, and that there is only one identifier associated with one individual. The utility of uniqueness is significantly enhanced when it is also universally available. An example of a common ID with the 'unique' and 'universal' characteristics would be the Aadhaar system in India. The characteristic of uniqueness in an ID allows for a particular financial institution to have a single view of the customer in their internal system and also across the entirety of the financial ecosystem. This is also valid for legal entities as recognized by the G-20 adoption of the establishment of an LEI in June 2012, to be able to better identify counterparty and contagion risks, particularly those related to cross border exposures to over-the-counter (OTC) derivatives.

Digital: When an individual's attributes can be captured and stored electronically and issued on digital credentials that can uniquely identify a person, the identity is referred to as digital ID. A digital identity provides a potentially transformative solution the global challenge of inclusion by offering countries the ability to leapfrog the development of paper-based systems and rapidly establish robust identification infrastructure. As described, in the section on authentication of the technologies, extensive use of mobile devices in developing countries can be leveraged for this purpose. Moreover, digital IDs can have benefits beyond the financial sector, such as in enhancing gender equality as noted previously.

These three characteristics highlight varying levels of quality and sophistication, and have important implications on access to financial services, customer oversight, and the efficiency of financial service provision. As policymakers consider how they approach identification systems within their jurisdictions, it is useful to have a sense of the trade-offs and cost/benefit implications of the options being considered.

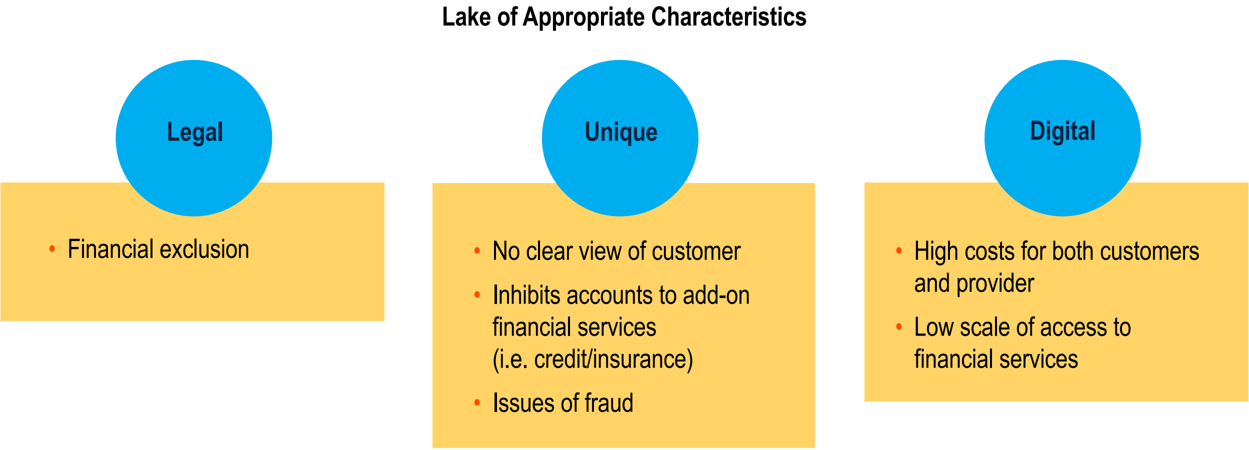
Each of these characteristics impacts the sustainability, affordability and reach of financial services affecting financial inclusion objectives. The lack of legal, unique ID captured consistently across institutions impedes efforts to gain a complete view of the customer hence limiting the services available to the individual. From the perspective of the regulators, the lack of a unique, digital ID, limits the ability to gauge household credit exposure. This lack can add inefficiencies and costs as all verifications must be done manually along with maintaining paper trails. It is important that policymakers keep these characteristics and the utility they offer in mind during the design phase of planning their own identity programs.

Box 5: Case Studies Highlighting the Benefits of Digital ID to Governments

In 2015, Nigeria began a biometric verification pilot for all civil servants in an effort to get an accurate record of the personnel and ensure that 'ghost' salaries were not paid out. The Central Bank of Nigeria, required that all customers enroll with their banks to get their unique Bank Verification Numbers (BVN), operated by the Nigeria Inter-Bank Settlement System (NIBSS). In early 2016, they announced the removal of 24,000 (ghost) workers,[42] and that number has since doubled – saving the tax payer equivalent of USD $74million.

The Sistema de Identificación Nacional Tributario y Social (SINTyS) system in Argentina enabled individual records to be linked across 13 databases covering employment, pensions, electoral roll, social beneficiaries, as well as registries for the deceased, real estate and auto ownership. This resulted in savings of USD $187 million in reduced leakage and tax evasion.[43]

Figure 6: Lack of Appropriate Identity Characteristics and Its Impact on the Financial System


Lake of Appropriate Characteristics
Legal
Financial exclusion
Unique
No clear view of customer
Inhibits accounts to add-on financial services (i.e. credit/insurance)
Issues of fraud
Digital
High costs for both customers and provider
Low scale of access to financial services

Risks and Challenges in Implementing Digital ID

Despite the numerous benefits of an inclusive, robust, and responsible digital ID system, governments are faced with challenges, such as those mentioned below. To ensure that trust is maintained in the system, governments should consider and work to mitigate these risks.

Exclusion Risks

Demographics, culture and ethical considerations all require attention when defining a digital Identity. 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.

Such populations might include vulnerable populations (including tribal and ethnic populations or those with unclear migration status) as well as those with low digital literacy or lack of connectivity. Infants or those affected by skin or eye diseases might have unformed or disfigured features which might make fingerprint and iris capture of sufficient detail and quality, problematic. Advances are being made using a mixture of anatomical studies, artificial intelligence (AI) and deep learning algorithms to overcome these hurdles.[44] Other considerations are religious beliefs or conflicts with one' values against capturing of biometrics leading to self-exclusion. Such reasons need to be carefully measured when designing a digital ID for an entire population sample especially in the context of personal freedom and democratic rights.

Privacy and Data Protection

A key consideration are the privacy and data protection issues, including ethical concerns, that are inherent in the collection of personal and biometric information. The (most likely) centralized nature of sensitive data storage also exacerbates the cybersecurity concerns and privacy risks associated with digital IDs. It is vital that governments set out a robust governance procedure including for data management systems, and that this be maintained and consistently updated. It will be the responsibility of the government to define data protection policies, including rules around the collection, use, management and disclosure of the data. Governments may also think about mechanisms to minimize the amount of personal data which is collected and how data systems will be maintained, especially to safeguard against data leakages and (cyber) attacks.

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. There should be appropriate mechanisms to ensure that consent from individuals is obtained which covers the basis on which the data will be collected, maintained, used and disclosed. Individuals should be aware of who holds and has access to their personal data and have an opportunity to inspect the data held about them and to ask for corrections for any errors or out of date (or incomplete) data. Regimes should also provide for expungement or deletion of specific data if the original purpose for the data collection has expired. Moreover, suitable independent oversight and enforcement mechanisms should be available to individuals who have complaints regarding misuse or other non-compliance with rights guaranteed under the privacy and data protection regime.

The EU has recently introduced the General Data Protection Regulation (GDPR) to deal with this challenge and harmonize data privacy laws across Europe. GDPR requires companies that collect data on EU citizens to comply with strict rules on consumer data and rights regarding their data. The implementation of the law has had to address a number of contentious issues from data portability – the ability to transfer data across interoperable applications – as well as how to define data controllers and the associated designation of a dedicated Data Protection Officer.[45]

Misuse of data and breaches in security can result in identity theft, physical harm, discrimination, and emotional distress to individuals causing them to lose trust in the system. Organizations also suffer considerably, causing both financial and reputational damage.

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.

It is vital that economic feasibility, and infrastructure constraints are adequately evaluated and that systems are future proofed to keep up with the changes so the resilience of the system is not compromised.

Governments should:

- Design digital infrastructure appropriate for the context, including strategies to reach remote areas and ensure 'last mile connectivity'. Off-line solutions can complement the absence or loss of on-line connectivity.[46]
- Develop robust procurement guidelines and contemplate open design standards to promote innovation and allow for greater flexibility, efficiency and functionality of the system both within and across borders.
- Ensure the technical capacity of government agencies, private sector and other stakeholders in the digital identity ecosystem (including end-users) to operate and maintain new systems and devices.
- Consider opportunities for savings and revenue generation for both the public and private sector that may offset some of the costs of implementing a robust digital ID system.
- Ensure that the ID system meets the needs of a wide variety of users, including both public and private entities, in order to drive demand for the system.

APPROACHES TO INTEGRATE ID INTO THE FINANCIAL SECTOR

Using Existing Legal IDs

In many countries, as a matter of general practice, all FSPs collect a specific ID which is in generally considered reliable and universal. In general, the financial sector relies on existing legal IDs, traditionally based on physical interactions and physical exchange of documents,- between the user and the relying party, to allow access to services (public or private) such as healthcare, education, financial services. With the rapid development in technology, FSPs in many countries have access to identification systems to help validate credentials. In the case of digital IDs, the validation and subsequent verification can be conducted in real-time at the time of account opening, either in-person or even remotely. (*Please refer to Annex 2 for details of the validation and verification process*)

The box below highlights examples that show the potential of using legal ID's to integrate with the financial sector and the significant benefits that are accrued from this integration.

Box 6: Legal IDs: NADRA, Peru ID, Aadhaar, SPID

Peru ID

The National Registry of Identification and Civil Status (Registro Nacional de Identificación y Estado Civil, or RENIEC) is the premier national digital ID system in Peru. RENEIC has been used as a form of identification for a wide range of public and private services. For example, RENIEC serves as the core verification database for e-money platform called 'Modelo Peru' serving millions of customers across Peru for e-money transactions. In addition, a new service using RENIEC known as Billetera Movil (BiM), was launched in February 2016, which provides services such as cash in/cash out at agents, the ability to check balances, conduct P2P payments and top-up airtime credit.[47]

Aadhaar

In the case of India, its universal digital ID named Aadhar (a 12-digit number issued by Unique Identification Authority of India (UIDAI)), provides biometric verification for a variety of services through CDD/e-KYC authentication platforms. The Central KYC Records Registry (CKYCR) is envisaged as a repository of the CDD records obtained and uploaded by the Regulated Entities (REs) across the financial sector. CKYCR has been set up through an amendment in the relevant Prevention of Money Laundering (PML) Rules: specifically, those regarding the maintenance of records which mandate financial sector entities to upload the customer information onto a common database of the proposed registry. This database aims to facilitate inter-usability of the CDD records across the sector(s), with one of the objectives to reduce the burden for both individuals and the RE of obtaining and verifying CDD documents each time a customer creates a new relationship with a financial entity.[48]

NADRA

Pakistan's CNIC (Computerized National Identity Card), a core product of NADRA (National Database and Regulation Authority), is the legal digital ID card for Pakistani citizens. CNIC provides legal ID verification services across a number of platforms and sectors. For example, the

Box 6: Legal IDs: NADRA, Peru ID, Aadhaar, SPID (continued)

PTA (Pakistan Telecom Authority) and MoIT (Ministry of Information Technology) collaborated to introduce a SIM registration system called Biometric Verification Systems (BVS) program. The program made it mandatory for all cellphone owners to register each new SIM and have their identity biometrically verified against the NADRA digital ID database. As part of this process, PTA developed a SIM registration information system, which links a customer's CNIC with several SIMs. SIMs can only be activated after the purchaser's biometrics (finger impressions) have been verified against NADRA. In addition to the verification requirement, a limit was placed on each person obtaining SIMs, and a cap enforced. The SIM verification program has been a success due to the lower operations costs enabled by the digital ID integration.[49]

SPID

The Italian Public System of Digital Identity (SPID) is the Italian solution developed under the EU eIDAS Regulation. It is a public open system allowing public and private entities (Identity Providers), accredited by the Agency for Digital Italy (AGID), to offer registration services and the digital ID verification for access to services for citizens and businesses.

The acceptance of SPID is mandatory for the public sector and is optional for private and financial sectors. SPID envisages different levels of authentication, consistent with standard ISO-IEC 29115, according to the level of security of the services required by the users. Launched in 2016, SPID reached about 2.5 million digital identities by March 2018.[50]

Private Sector Initiatives

In a few countries with reliable and universal coverage of legal ID, banking and other industry consortiums have developed digital capabilities that are built on top of these legal IDs and leverage the value of them. Moreover, in the recent past, dedicated general-purpose digital features and solutions have been developed as an overlay on legal ID. These services seek to offer an open and general-purpose authentication which can be used to avoid the need for dedicated passwords and security credentials. These general-purpose services are now also being targeted at the financial sector. Examples of this include FIDO alliance and Mobile Connect and other services based on federated architectures that are being developed. In this model, a diverse set of underlying legal ID and information held with private sector institutions could be used and the individual choses which underlying legal ID or private sector information source is used to assert one's identity in a given context.

Some examples of these initiatives are highlighted in the boxes next page.

Social Data for Identity Proofing

The increasing use of online social and professional networks, e-commerce platforms, and use of connected devices (IoT) that can track location and service usage data, generates a vast amount of data points about an individual. These data points can be aggregated to determine, with some degree of confidence, information such as: where the person lives (based on, for example, shipment of e-commerce purchases and taxi rides); where the person works (based on geolocation co-ordinates during typical business hours); the social life of the individual; professional connections (via channels such as LinkedIn) which can be used to also judge general reputation in the industry; the marketing of tailored products and services (such as insurance); and also the general demographic characteristics based on what the person reads, buys and listens to. It is possible to glean all this information without even knowing the person's name, age or date of birth from any registered website or official database.

While potentially useful, this has several cons, such as breach of privacy and data protection as well as the exclusion of those who need services (such as insurance) most, by eroding the principle of risk pooling. Moreover, not all the above information is usually available from one institution. There are emerging signs of institutions collating and sharing information through APIs to potentially commercialize this along the lines of a credit reporting system, causing further concerns about the data privacy standards being adhered to.

Several firms have started to use big data as either a complement to traditional sources of information or rely solely on it to conduct identity checks before the provision of services. Notable examples include peer-to-peer (P2P) lending platforms, which use captured social media data to assess credit worthiness of individuals who do not have a credit history.

Box 7: Private Sector Initiatives: FIDO, BVN, GOV.UK Verify, BankID

Fast Identity Online (FIDO) Alliance

The FIDO Alliance is a non-profit, industry alliance nominally formed in July 2012 to address both the lack of interoperability among strong authentication devices, as well as the problems users face when creating and remembering multiple usernames and passwords. Headquartered in California, the members have developed technical specifications that define an open, scalable, interoperable set of mechanisms that supplant reliance on passwords to securely authenticate users of online services. The FIDO Alliance currently has over 260 members.[51]

BankID

BankID is an electronic identification for Swedish citizens issued by a consortium of Swedish banks with an estimated 7.5 million active users currently. First issued in 2003, it can be used by members of the public, authorities and companies. Citizens can use their BankID for identification as well as a means of digital signature for signing transactions and documents remotely. It has been adopted by the government, municipality, banks and companies to validate identity. In accordance with Swedish law as well as within the European Union, a signature via BankID is legally binding.[52]

Bank Verification Number (BVN)

The Central Bank of Nigeria (CBN) in conjunction with the Bankers Committee launched a project in 2014 to develop a single biometric database for all banks' customers nationwide. The features captured include fingerprints and facial images providing customers with a 11-digit number. Customers were required to enroll with their bank to get a unique BVN which would then be valid across the entirety of the Nigerian banking sector. Each customer is only allowed to have one BVN and the adoption of this ID was made a mandatory requirement for access to all banking services.[53]

GOV.UK Verify

GOV.UK Verify is an identity assurance system being developed by the UK Government Digital Service (GDS) that facilitates a marketplace of trusted third parties to identify and authenticate users of online services. The system works by behaving like a platform so that those companies who are registered on the platform (currently seven[54]) such as the post-office and Barclaycard can 'verify' the information submitted by individuals.

Once verified, the registered company lets the government know the identity of the individual and the verified individual can access up to 15 government services such as benefits, driving license, the ability to file tax returns or check your state pension. The GDS set a target to reach 25 million registered users by 2020 and wants it to become the default system for all those accessing public services.

Verify was first launched in 2014 but had some trouble gaining traction finally going live in only 2016. To register, a valid UK address is required and by late 2017 1.5 million Verify accounts had been set up.[55] The system remains in its beta phase and is hence not open to all users.

Aggregation services and P2P lenders in some markets ask users to share their access credentials with various websites, primarily financial, and then aggregate the data from the user's various financial services relationships. In the process of aggregating the information, predictably, a lot of underlying information like the address of the individual, phone number(s), periodic incoming payments (like salary and expenses), could become visible to the aggregation service. The use of social data thus aggregated is increasingly being considered as part of the identity validation and is used as a basis for decisions on creditworthiness. A few firms are now moving one step further to offer so-called 'social identity' verification services. This type of data could have potential in addressing the challenges of identity validation for individuals with limited traditional biographical footprints in official records.

Despite the potential opportunities that arise in using social media data for identity proofing there are several challenges that emerge, particularly around privacy and consent. Under the terms of the forthcoming GDPR directive, user consent must be freely given in the form of either a statement or a clear affirmative action that signifies agreement to personal data being processed. It is highly likely that its approach will influence the development of data protection laws globally.[56]

Blockchain and Digital ID Identity

Federated authentication could potentially provide the solution to be able to trust unknown identities across organizations or even borders. This is illustrated by blockchain – a distributed ledger technology which is essentially a shared ledger between network participants and the use of 'tokens' as a way to incentivize participants for running the network in the absence of a central authority. This allows exchange of information among multiple parties in what essentially is trust-less system.

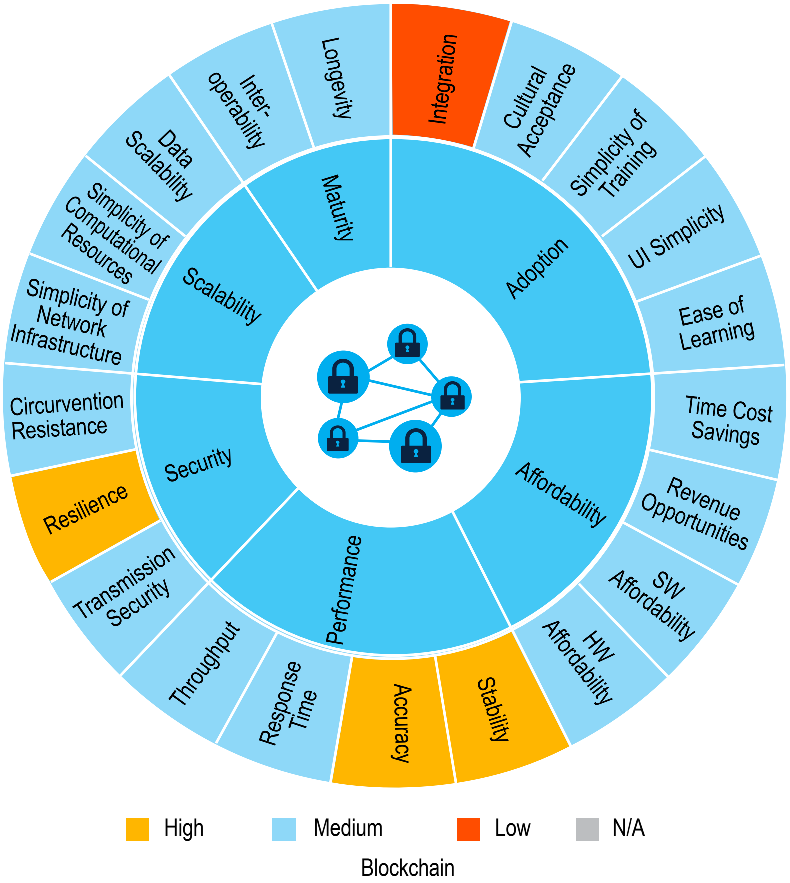
This technology is being trialed for various financial sector applications including funds transfers, payment settlement and regulatory oversight, and due to its decentralized and transparent nature[57] also increasingly in identity management as well. The immutable nature of the ledger ensures that dispute resolution is embedded and enforced by computer protocol. Moreover, the transparency, resilience and replication at each node offered by the shared ledger is a useful tool for tracking and maintaining the integrity of the information.

It should be noted that although blockchain and distributed ledger technologies were not built with identity in mind, there are use cases identified in supporting the development of self-sovereign identity (SSID) – (i.e.) a mechanism for an individual / entity to assert its own identity without having to rely on any third party. This term (SSID) is increasingly being contested, as the basis for the identity is often some form of underlying legal ID which is first validated by the issuing authority before being managed by an individual / entity on their own. Hence, in that sense, it more of a 'self-managed' rather than 'self-sovereign' ID. For example, the Government of Dubai recently announced a plan to use blockchain technology to verify all information on an Emirates ID card. Details related to a resident would be stored on the card, including insurance documents, passport information, and health data, and by 2020 it is expected to be stored in blockchains, secured, and encrypted.[58] In actuality, what will be stored in the distributed ledger is not identity itself but an identity 'transaction' or attestation of an identity.

Some argue that blockchain could be used to empower an individual to have complete control over their identity including where, when and what parts of their identity they wish to share. Essentially, when a person presents their digital identity to a third party, they will do so by proving that they have control over the private key that corresponds to the relevant linked identity transactions allowing the individual to divulge only that information that needs to be shared with authenticating body and not the entirety of the digital ID. Moreover, this is possible without data storage. For example, if a user wanted to access a service that was only available to people who lived in a specific region, the attestation could provide proof that the user's home address is within the required region, but does not need to provide the actual address itself.

There have been recent developments on blockchain based digital identity and associated CDD. However, many of these developments are still in early stages and have not yet produced results at scale, making it difficult to evaluate their feasibility. It's also important to note that despite the progress, concerns remain around the legal standing of blockchain-based applications, the standards used, and the interoperability of shared ledger systems as evident from the assessment in the figure below along the dimensions of Maturity, Ease of Adoption, Affordability, Performance, Security and Scalability.[59]

Figure 7: Assessment of Authentication Robustness of Blockchain[60]



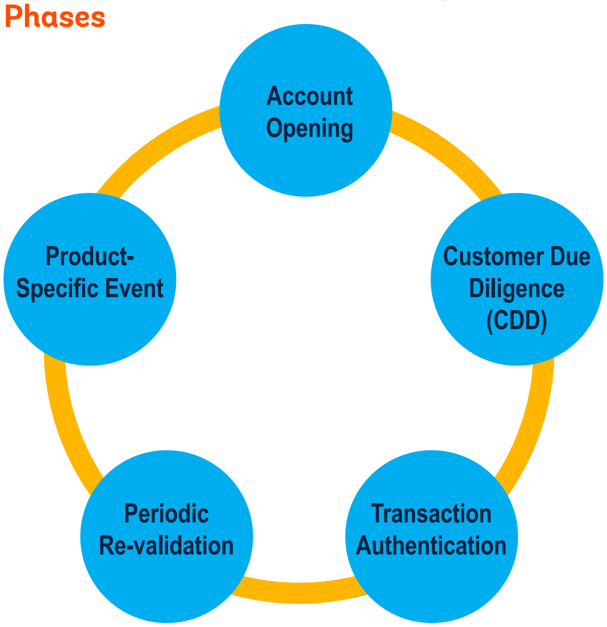
ICA
INTERNET
PASSWORD
CODE
DATA
INTERNET
SECURE
BD55U
6E78BC9

APPLICATIONS OF IDENTITY IN FINANCIAL SERVICES

Identity is integral to providing and obtaining financial services, and is needed at various transaction points when using financial services. The role ID plays at each of these transaction points and for different services will vary (see Figure 6 below). These distinctions are subtle but have important implications for policymakers, regulators, service providers and consumers alike. Identity is also vital for ensuring the safety and integrity of the financial system.

During account opening, a customer is required to provide credentials to establish identity so that the FSP can carry out CDD procedures. These credentials then need to be validated and allows the FSP to link and match information gathered from other sources of information such as credit bureaus to validate the information provided and assess the suitability of the product to the individual. Once complete, a transaction identifier maybe issued (for example a debit card and PIN), to be used for **authentication** in future transactions or access to other services.

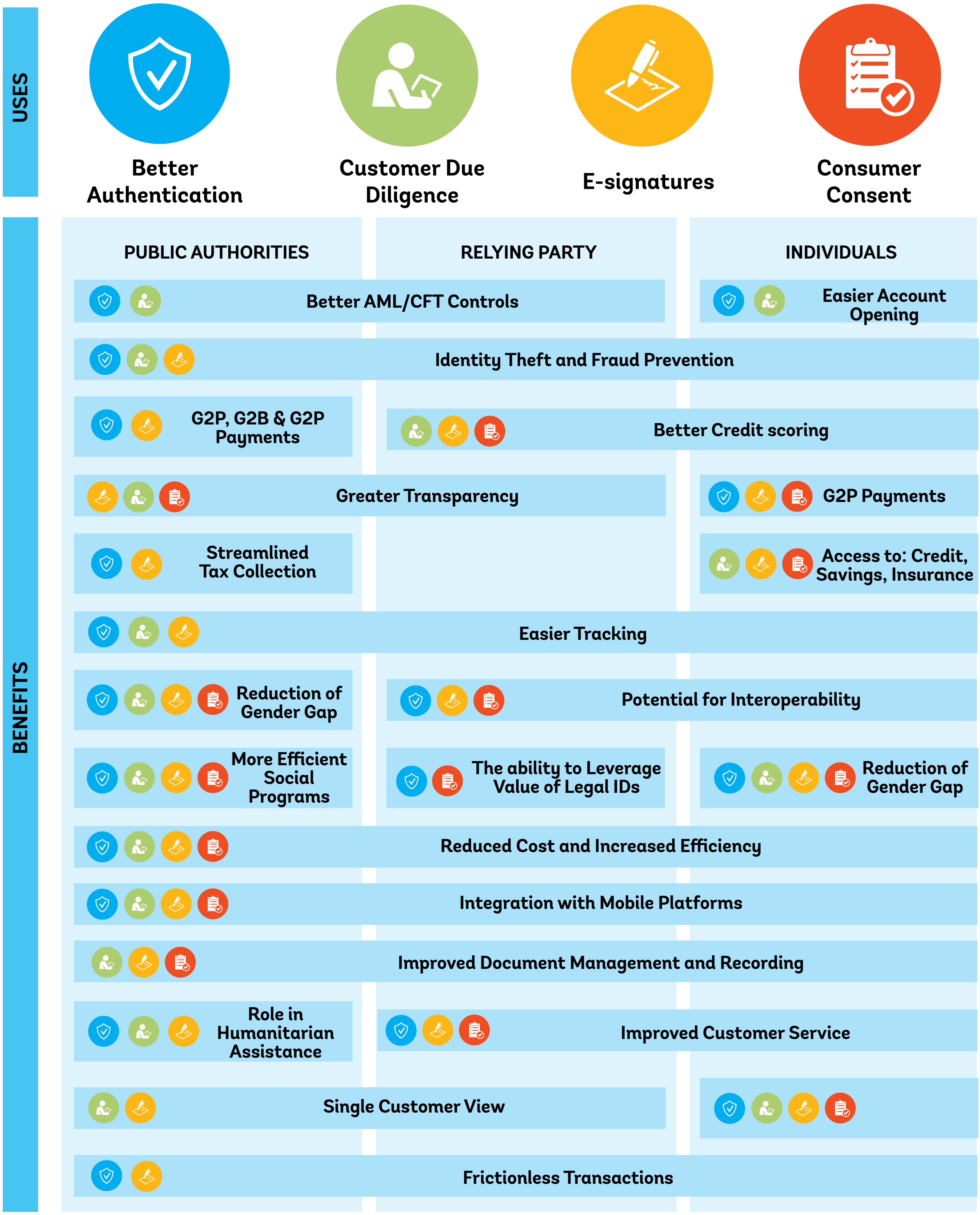
Figure 8: Financial Service Stages and Phases



The information collected during account opening—for example, address, other contact details, and employment status—can change over the customer lifecycle. Hence, **periodic re-validation** is required to ensure that key data underpinning CDD continues to be valid. The frequency of this varies according to local regulatory requirements, which are often at least once every 3 to 5 years, depending on risk profile of the customer. Finally, there are occasional **product-specific events**, such as the re-issuance of an internet banking password and returning mortgage documents, which require the re-validation of identity documents to ensure that the information is being provided to the rightful owner of the account relationship. The specifics will depend on local regulatory requirements and industry standards and codes.

The subsequent sub-sections below describe the applications and utility of ID within specific financial sector services and processes associated with provision of services and products. The different processes described in Figure 6 can be broadly grouped into three: account opening; ongoing authentication and customer consent; and back-office processes. Digital ID has applications in each of these three areas and are described in the sections below. This includes a focus on (1) **account opening**, (2) **customer due diligence**, (3) **authentication**. In addition, digital IDs have the potential to (4) **transform payment**

Figure 9: Benefits of Digital ID



USES

🔵 Better Authentication

🟢 Customer Due Diligence

🟡 E-signatures

🔴 Consumer Consent

BENEFITS

PUBLIC AUTHORITIES | RELYING PARTY | INDIVIDUALS

🔵 🟢 Better AML/CFT Controls

🔵 🟢 Easier Account Opening

🔵 🟢 🟡 Identity Theft and Fraud Prevention

🔵 🟡 G2P, G2B & G2P Payments

🟢 🟡 🔴 Better Credit scoring

🟡 🟢 🔴 Greater Transparency

🔵 🟡 🔴 G2P Payments

🔵 🟡 Streamlined Tax Collection

🟢 🟡 🔴 Access to: Credit, Savings, Insurance

🔵 🟢 🟡 Easier Tracking

🔵 🟢 🟡 🔴 Reduction of Gender Gap

🔵 🟡 🔴 Potential for Interoperability

🔵 🟢 🟡 🔴 More Efficient Social Programs

🔵 🔴 The ability to Leverage Value of Legal IDs

🔵 🟢 🟡 🔴 Reduction of Gender Gap

🔵 🟢 🟡 🔴 Reduced Cost and Increased Efficiency

🔵 🟢 🟡 🔴 Integration with Mobile Platforms

🟢 🟡 🔴 Improved Document Management and Recording

🔵 🟢 🟡 Role in Humanitarian Assistance

🔵 🟡 🔴 Improved Customer Service

🟢 🟡 Single Customer View

🔵 🟢 🟡 🔴

🔵 🟡 Frictionless Transactions

services for FSPs and also government-to-person (G2P) and humanitarian assistance. Further, digital IDs have a critical impact of effectiveness of (5) **credit reporting systems** and facilitates (6) **digital signatures** and (7) **insurance schemes**. Finally, a strong digital ID system can also help (8) **small business** development by improving identification of firms and employees. The list is not exhaustive but is aimed at those elements of financial services that are most pertinent to financial inclusion. The role of digital ID on each of these areas is described below and illustrated through relevant case studies.

Account Opening

One of the important applications of digital ID in the financial sector is that of account opening. According to the Global Findex Survey recently released by the World Bank Group, 515 million adults worldwide opened an account at a financial institution or through a mobile money provider between 2014 and 2017. This means that 69 percent of adults now have an account, up from 62 percent in 2014 and 51 percent in 2011. However, only 63 percent of adults have an account in developing countries, compared with 94 percent in high-income countries. The survey also finds that the digitization of government payments, which is supported by digital ID, could help to reduce the number of unbanked people by 100 million globally.

Countries such as Peru and India have already used digital ID to rapidly increase account opening in recent years. Specifically, India has pioneered the JAM (Jan Dhan Aadhar Mobile) approach has enabled more than 80 percent of the population to have bank accounts[61] (see Box 8 below). In Peru, the digital ID system enabled rollout of an interoperable mobile money service and platform.

Customer Authentication

After account opening and customer due diligence, FSPs need the ability to authenticate customer identities for a variety of services and transactions. Secure, digital authentication mechanisms based on attributes and credentials established during account setup are necessary to ensure that only legitimate customers to access services and to prevent identity theft and fraud. Furthermore, digital ID technology can help FSPs implement automated methods of authentication that do not require the costs and manpower needs of face-to-face interaction. This section highlights some of common authentication mechanisms and draws attention to developments in this area.

Currently, the provision of credentials for use in authentication are often tied to a specific financial product they service, such as a user ID and password for online transactions and/or a payment card and PIN. There is however, a trend towards de-coupling authentication credentials from a specific financial product and making it available as a service on its own. One example is the growing use of token-based authentication to access one's accounts at an institution. The general concept behind a token-based authentication system is simple: they allow users to enter their username and password

Box 8: Case Study: India *'JAM Trinity'*

In India, the foundation of financial inclusion strategy has been based on the Jan-Dhan, Aadhaar, and Mobile (JAM) trinity. The JAM trinity integrates the ID system and payment applications with a view to becoming more cost effective and efficient to open an account and for accessing them.

The Aadhaar ID system includes an electronic KYC (e-KYC) service to expedite the verification of a client's identity. The e-KYC enables an individual with an Aadhaar number to allow Unique Identification Authority of India (UIDAI) to disclose his/her personal information to service providers who wish to instantly activate services such as mobile connections and bank accounts.

e-KYC is paperless, consent-based, private and instantaneous. As a result, reliable[62] CDD data is shared with the reporting entity in real time. Furthermore, as the KYC data is released directly to service providers only upon the consent of the customer, his/her privacy remains protected provided robust data protection measures are in place. So far, a total of 4.9 billion e-KYC transactions have been conducted through Aadhaar.

Banks and payment network operators have embedded Aadhaar authentication into micro-ATMs to provide branch-less banking anywhere in the country in a real-time, scalable and interoperable manner. From the FSP's view point, it offers tremendous benefits in terms of near elimination of paperwork and the consequential burden of keeping records and facilitating audit and forensics through the electronic storage of information.[63]

Box 9: Case Study: Peru *'Modelo Pero'*

The Peruvian Bankers' Association (ASBANC) announced an initiative to develop a shared e-money platform in 2014 called 'Modelo Peru'. This quickly grew into a collaboration between the country's financial institutions, government, telecommunications companies, large payers (salaries) and payees (billers), leading to the establishment of a dedicated entity in July 2015 the Peruvian Digital Payments (PDP) to develop and offer a new payment service. This new service is known as Billetera Movil (BiM), and was launched in February 2016, reaching around 80,000 subscribers in its first three months of operation.

Through the successful integration of Peru's national Digital ID system (RENIEC) and payment applications via a mobile phone, a successful ID backed payment system was developed. The digital ID is linked to all accounts, enabling enforcement of various transaction and account balance limits. According to the GSMA, 95 percent of the population of Peru lives in an area with mobile broadband coverage and at least 70 percent of the population have a mobile phone connection.[64] This enabled provision of services such as cash in / cash out at agents, balance check, P2P payments and airtime top-up across large sections of the population, whilst being able to enforce the specific transaction and account balance requirements across all the accounts an individual held.

It is expected that other services such as ATM integration, utility bill payments and merchant payments would be enabled by end-2018. Important characteristics of this system include: being able to sign up without a bank account; ability to send or receive money without the use of mobile data or a pre-paid plan; and withdrawal/transaction limits up to USD $300 a day and USD $1200 per month. If this payments system is scaled up, it has the capacity to bring more than 60 million people into the formal economy.

to obtain a token which allows them to fetch a specific resource. Users can then use this token to access the specific resource for a specific time period.[65]

There can be several approaches for authentication, depending on the assessment of risks associated with unauthorized access. As policymakers push the sector to expand financial services into underserved and often rural areas, a key consideration should be to identify methods that offer secure and reliable authentication for FSPs, while also being convenient for users. The concept of Levels of Assurance (LOA), for example, takes a graduated approach to security and matches the LOA needed to the specific class of service to be provided. While the purpose of this report is not to go into a detailed analysis of the LOA levels, it is important to note that service providers always face a cost-benefit tradeoff in seeking to achieve higher LOAs. Specifically, a tradeoff between the perceived risk of a transaction versus the cost of authenticating that transaction. For example, a face-to-face manual authentication process will incur a relatively high cost but will likely result in lower risk and thus higher LOA. Conversely, a username and password type of authentication system will incur much lower costs to service providers but entails much higher risk of fraud.[66] More detail on the LOA provided in Annex 1.

Personal Identification Number (PIN)

The Personal Identification Number, or PIN, is the authentication technology used by almost all payment card services worldwide particularly for ATM cash transactions. A PIN differs from a password in that it is transformed into a reference value using encryption keys which is then stored on the authorization systems of the FSP while the PIN itself is transient in nature. The security relies in having a robust transformation process that provides a high degree of confidence that the PIN cannot be derived from the reference value. A PIN is intended to be remembered by the user and when used safely and as required by prevalent standards,[67] provides a good degree of protection and certainty.

However, there is a commonly held view that some customer segments cannot use PINs reliably, due to illiteracy, innumeracy or lack of familiarity with the technology and other issues. The security of the PIN lies in being able to commit it to memory. However, low frequency of use forms a tenuous link with memory, since many of these customers access financial services infrequently, perhaps as little as once every 3 months or even less. Further, the infrequency of use leads people to write their PINs down, often on the back of the card or mobile phone they are using, leading to PIN compromise.

In addition, PINs can and often are easily be shared with others, which can presents a security risk. For example, national and global fears around terrorism are beginning to influence PIN use. The 2015 terrorist attacks in Paris were reported to have been financed using prepaid cards. This reflects a broader issue with payment cards in that one person, who passes the necessary CDD checks can acquire the card and top it up, whilst another person uses the funds. The PIN is forwarded by post or text message or even word of mouth making it increasingly difficult to track.

Regulatory authorities in several countries have concerns that a PIN is not secure enough, for at least some financial transactions. For example, in India, online biometric authentication for bank transactions is becoming available. The diminishing reliance on solely PIN use for security, is further evidenced by the announcement that the Payments Association of South Africa (PASA), in partnership with Visa and MasterCard, is seeking to introduce biometric authentication of payment cards in South Africa.[68]

Smartcards

A Smartcard is a card that has embedded integrated circuit or chip. Smartcards can be used to store attributes and credentials such as PINs or biometric data (see next section) and with the appropriate application, can enable interaction with recorded data. For example, a smartcard can be used to verify that a fingerprint sample collected by a connected device is the same as a template stored in the Smartcard. Smartcards can either be "contact" cards that are read when in direct physical contact with a reader, or "contactless" card that uses Near Field Communication (NFC) or radio frequency identification (RFID) technology (see Box 10). In general, "contact" smartcards also have capability of requiring a pin for identification.

Smartcards are most commonly used for payments, public transport, or access to office buildings. Many countries also issue national ID cards and other credentials that use smartcards. Digital ID cards in global circulation are expected to increase from 1.75 billion in 2013 to 3.3 billion in 2021. Of this, a total of 3.2 billion national ID smart cards will be issued by 103 countries.[69] As of early 2017, 82 percent of all countries issuing official ID cards have implemented programs that depend on smart cards or plastic cards and biometrics. These are typically contact cards, although some including Germany's ID card (Personalausweis) and Malaysia's MyKad use contactless technology.

In addition to using smartcards as standard IDs, some emerging cases have attempted to combine identity and payment capabilities on one smartcard potentially offering great convenience to users and service providers alike.

For example, the Government of Maldives, in collaboration with Mastercard, has recently launched a biometric smartcard-based national ID called the 'Passport Card' for its citizens. The card contains 10 fingerprints for secure verification and a unique combination of dual-interface chip for contactless and contact card reading. This card functions as the passport, driving license, and national ID of the cardholder, and can be used to provide health and e-services by the government. It also functions as a payment card to make payments.[70]

However, like most innovative technologies, integrating identification and payments also introduces a layer of complications and risks, such as: data privacy; dilution of data ownership; liability between state identity authorities, payment service providers and banks; and general risk and fraud management. In addition, while smartcards are more secure than non-chip-based cards, they are only as secure as the features installed onto them at the time of production. Estonia, for example, had to re-issue 750,000 national e-ID cards because of a security risk found in the chips of those cards.[71]

Mobile SIM Authentication

With the ubiquity of mobile phones, there is increasing interest in using the unique identification numbers associated with mobile subscriber identity modules or SIM cards. The algorithms contained in the SIM card allow for encrypted communication between the user and the network. For authentication, the authenticating body generates a random sequence of numbers that is sent to the user's mobile- this is the user's public key.

Box 10: Near Field Communication (NFC) and Radio Frequency Identification (RFID)

Although distinct, NFC and RFID both employ radio signals to tag and track data. Simplistically, NFC is the newer technology and—unlike RFID technology that is only passive — an NFC device can also exchange data with the tag, hence it can be both a reader and a tag.

Tags are based on a number of parameters including the reading distance, speed and amount of data to be transferred, security and cost. They are embedded into retail products to help stores keep tabs on inventory; automatically note the identity of a cars on a toll road and sometimes manage the control of luggage on some airlines. Tags are, also in SMART passports.

Box 11: GSMA's Mobile Connect

Mobile Connect is a secure universal log-in solution that works by matching a user to their mobile phone using a phone number as the identifier and the mobile phone as the authentication device. It is a portfolio of mobile-based secure identity services driven by mobile network operators globally and delivered as a federated identity framework.

It leverages the reach and inherent trust in the mobile network and combined with a unique PIN for more secure use cases, it is used to verify and grant online access where a Mobile Connect logo is displayed. Mobile network operators give users control over their own data and enable end users, businesses, and governments to interact and access online services in a convenient, private, and trusted environment.

While the SIM information itself can act as a form of digital identity, the GSMA is focusing its efforts on using the platform as an add-on element to existing ID programs, to provide additional authentication. Developers can access the ecosystem of operators who have partnered with GSMA for Mobile Connect and their corresponding user base.[72]

The GSMA is also working to align Mobile Connect with other identity standards and regulations, such as Gov.UK Verify in the UK, as well as technical standards produced by bodies such as (International Organization for Standardization) ISO, International Telecommunication Union (ITU) and International Civil Aviation Organization (ICAO).

The public key together with the user's private key and authentication algorithm contained in the SIM, verifies the user.

The Mobile Connect solution created by mobile industry association GSMA (see box below) enables customers to create and manage a digital ID via a single log-on on their mobile phone.

Countries that have adopted cryptographic SIM cards include Estonia, Moldova, and Finland. Norwegian mobile operators offer their subscribers secure mobile authentication through a local BankID solution to provide secure online user identification and user digital signature verification. In 2012, Bank of Mexico issued regulation establishing that banks in Mexico must allow their deposit account holders to associate their cellphone number to their accounts, in order to facilitate electronic transfers of funds across bank accounts.[73] Each cellphone number can be associated to only one account in a given bank, but to multiple accounts, each from a different bank. Once the association is established, a customer can provide her cellphone number as an identifier to receive transfers.

However, it is important to note that mobile authentication is more viable when used in combination with other authentication methods, rather than a standalone technique due to practical challenges such as sharing of mobile phones between individuals.[74,75]

Linked to this and a relevant point to be aware of, is that many countries now require that pre-paid SIM cards only be activated when registered with a proof of identity; those who lack this ID could be denied access to mobile communication, further exacerbating digital, social and financial exclusion.

Biometric Based Authentication

Biometrics are physical and behavioral attributes of a person and are increasingly used as a means of proving one's identity. There is increasing interest around the world in exploring biometrics for authentication, as a response to (amongst other matters) AML and CFT concerns. Authentication services in India and Pakistan are built on biometrics and Bangladesh as well as South Africa (as previously mentioned) is expected to follow suit.[76]

Box 12: Cross Border Systems

Advances in technology are enabling digital identification systems to operate across borders. Individuals holding a valid ID from one country can use their credential to conduct a transaction in another country (such as filing their taxes) or to identify and authenticate themselves at checkpoints or border crossings in other countries.

In the European Union, eIDAS (electronic Identification, Authentication and Trust Services) is a regulation on electronic identification and trust services for electronic transactions in the European Single Market. Under eIDAS, individuals can carry out secure cross-border electronic transactions that require them to authenticate their identity, such as enrolling in a university, opening a bank account and authorizing access to their electronic medical records.

There are three major stakeholders in the eIDAS network: individuals seeking access to a service or establishing their identity in another country, the server providing access to a secure application or service, and the provider of the services an individual is looking for.

Once data to be authenticated are collected at the immigration point, depending on the IT architecture in use, the data are validated through a central database maintained on site or remotely validated if the database is located in a separate location. A secure information exchange channel is achieved using SAML (Security Assertion Markup Language) for single sign on, error handling, and communication. Endpoint security is ensured using TLS (Transport Layer Security) — a cryptographic protocol that provides communication security over a computer network.

The eIDAS regulation also includes rules for trust services providers—companies that handle electronic signatures, time stamps, electronic seals, and other methods for verifying documents—and it governs the use of trust services by consumers, businesses, and agencies to manage electronic transactions or access online services.

Box 13: Biometrics

Biometric recognition uses an individual's unique physiological and behavioral attributes to identify and authenticate his or her identity. The type of attribute collected and matched is called modality.[77]

In biometrics, there are three main types of modalities: hard, soft and hidden. The hard or traditional modality includes iris scans, fingerprints or signatures; the soft -are related to faces, skin color, hair color or measurements and to bodies, like height or weight. It also includes behavioral characteristics and mannerisms such as gait, keystroke patterns, and mouse usage; while the hidden modalities, also referred to as intrinsic, are based on medical data or X-rays.[78] It is only the first two that are generally used in the identity system, with the former being the far more prevalent, while the latter is often used to understand patterns and trends and hence detect anomalies or unauthorized transactions.

When considering which biometric to use for authentication, jurisdictions should consider the accuracy (liability framework for false-positives and false-negatives), universality (presence of the trait universally), stability (permanence over time), the ease of collection as well as acceptability and cost components involved.[79]

Although the use of biometrics is inherently costly, due to the cost of in-person capture and registration when an identity is issued along with authentication costs, there is significant interest from international payment schemes. The Payments Association of South Africa (PASA) is working with Mastercard and Visa to design a solution that is interoperable in South Africa. The specification enables a range of biometric solutions, from fingerprint verification to palm, voice, iris, or facial biometrics. However, there are concerns that the uptake of this by traders will be low due to the high cost of replacing point-of-sale (PoS) devices.

Separately, a private sector initiative led by Zwipe (a company providing biometric solutions) and Mastercard circumvents the issue of high integration costs to merchants by using an integrated fingerprint sensor within the card itself.[80] The solution provides on-card biometric authentication, hence removing the need for the acceptance device to have a built-in biometric reader. While the card is unarguably more expensive than a normal smartcard—and it is likely that the total cost of implementation would be higher than that of deploying a few thousands or tens of thousands of PoS devices, rather than millions or tens of millions of cards—such decisions are often based on several factors, like speed to market, and this could indeed be appropriate in some situations. Furthermore, the fingerprint matching taking place on the card rather than by a device that the card is inserted into adds an extra layer of security to the reference fingerprint data.

Regardless of the format and approach, the adoption of biometrics as the preferred means of customer authentication across the world is attracting lot of attention. Experts expect to see as many as 600 million devices with biometric authentication by 2021.[81] By 2020, 50 billion Internet of Things (IoT)[82] devices are forecasted to be in use, and 500 million biometric sensors will be deployed for IoT by 2018.[83] Indeed, IoT will be a major enabler for combining analytics and continuous assessment to generate an adequate level of assurance, in real time, that an individual is who he or she claims to be.

According to new regulations in some jurisdictions (e.g. China, the EU, Malaysia and Mexico) the initiation of transactions, as well as access to sensitive payment data, should be protected by strong customer authentication (SCA). The general objectives are to improve cybersecurity and reduce the risk of fraud. SCA is the result of a customer authentication process based on three elements: knowledge (e.g. of a customer's own background information), ownership (e.g., of a physical token), and inherence (e.g. a customer's unique biological characteristics). As regards the last of these elements, financial firms are experimenting with the use of biometrics as a technology able to reconcile a simple user experience with adequate security. Technological improvements now allow for cheap and sound solutions embedded by default in a customer's smartphone (e.g. fingerprint, face or voice recognition). Financial firms can develop SCA solutions exploiting these smartphones' native services (e.g., ApplePay, Mastercard Selfie Pay). Biometrics are also an opportunity for customers: the use of modalities such as fingerprint scanning and facial recognition will not only offer a great deal of convenience in general but also a new form of security and identity verification, which may suit some customers better than traditional tools.

Payment Systems and Services

Digital ID is enabling re-structuring payment services and processes, the major developments in this regard are described below:

Combining ID and Payment Applications

ID and payment applications can be combined in one form factor such as a mobile phone and its associated SIM card or even a smartcard or other chip based token. If the basic digital ID credentials are unique and enable individuals to reliably assert their identity without including other data attributes by default, this will spur developments to minimize the disclosure of data.

However, linking a payment application to a digital ID by co-hosting the two applications on the same smartcard – in the way that was done on a limited scale by NIMC and Mastercard in Nigeria – can potentially be problematic. Since Mastercard isn't a bank, in order to function, the application needed to be linked to a bank account not under the control of Mastercard, presenting issues around consumer choice, data protection and simple practicality, beyond the challenge of having a particular commercial brand being tied to a national ID system. It would perhaps have been more straightforward to separate the ID application and the payments service, and develop financial services to be offered to NIMC registrants in a more established manner.

Using the Digital ID Infrastructure for Authentication

Digital ID infrastructure can be used for authentication in place of a dedicated authentication arrangement for a payment instrument.

India's transformational journey in its digital infrastructure in recent years provides a best representation of this application. As mentioned earlier in the case study on account opening, India has spearheaded the financial inclusion exercise using the JAM platform. This serves as an important tool for the central authentication for a variety of transactions, instead of a dedicated authentication arrangement for a single payment instrument. This potentially, increases the level of assurance without adding a corresponding decrease in usability. A total of 4.9 billion e-KYC transactions have been conducted via this platform. Banks and payment network operators have embedded Aadhaar authentication into micro-ATMs to provide branch-less banking anywhere in the country in a real-time, scalable and interoperable manner.

A further innovation in India, was to develop a mapping between the Aadhaar number and payment card/account number while using the fingerprint as an authentication mechanism. This allows an individual to pay, by simply providing a fingerprint at a participating merchant expelling the need to enter an account number or present a payment card. This service is called Aadhaar Pay. A variant of this is used for delivery of rations through the public delivery system and at micro-ATMs for withdrawing cash.

This approach of authentication has its challenges such as not being able to identify certain types of fingerprints and requiring multiple attempts to capture the biometric accurately enough to enable validation. In the current state of development, this could limit the effectiveness for routine transactions and those that need prompt authentication – for example while making a purchase in a high-traffic merchant.

Using the ID Credential as An 'Address'

The ID credential can be used in lieu of a bank account number to direct payments removing the need to reveal the recipient's account number to the payer agencies. This is accomplished by maintaining a mapping between the credential and payment related identifiers.

India's Aadhar payment bridge system (APB) is an example of such a service. It is a unique payment system implemented by National Payments Corporation of India (NPCI), which uses Aadhaar number as a central key for electronically channeling the Government subsidies and benefits in the Aadhaar Enabled Bank Accounts (AEBA) of the intended beneficiaries. The APB system is used by the government departments and Agencies for the direct transfer of benefits and subsidies under Direct Benefit Transfer (DBT) scheme launched by Government of India.[84] This is also an example of the government to person (G2P) benefits brought about by digital ID that supports efficiency and aims to remove the fraud inherent in the benefits system.

Box 14: Case Study: Singapore *'SingPass'*

'Singpass' is a unique national digital ID which is being used by 3.3 million people for speedy access to an array of government and financial services,[85,86] It is recognized and approved by government organizations as a formal credential of the individual and includes access to direct payment systems, insurance and tax reporting systems within the governmental setup.

The unique digital ID has been used as a credential which is used to direct payments without having to know the account number of recipients. With the digital 'MyInfo' platform within Singpass, the need for repetitive form filling is avoided. Launched in 2017, MyInfo pulls personal data such as names and addresses from public agencies. Consent includes only a click of a button and online submissions are made to more than 17 different e-government agencies simultaneously. In addition, the government is working on a pilot project with four private banks to verify customer credentials online using Singapass and it is expected to be open to private financial players as well.[87]

Box 15: Case Study: Pakistan *'NADRA'*

The CNIC has been central to the delivery of G2P payments in Pakistan. G2P payment schemes are organized into three categories: (a) social cash transfers, (b) government salaries and (c) government pensions. In all these categories, the role of CNIC has been integral in enabling the payments to be transferred to the customer.

All citizens are required to register for the CNIC once they reach the age of 18. New CNIC's are machine-readable and carry facial and fingerprint information. One of the important attributes of CNIC is that it ensures the personal presence of the beneficiary at the time of withdrawal of money contrary to the existing system where in most cases the beneficiary themselves is not a recipient of the money. Moreover, the beneficiary does not require a high level of financial literacy to withdraw funds, requiring literacy levels similar to that required for the usage of a debit card.[88] This supports reduction of the gender gap. In addition, the CNIC also makes it less complicated with simpler security tiers for withdrawal; i.e. In order to verify her credentials before making payments, a beneficiary only need present a CNIC.[89] CNIC has helped to promote growth and digitization of G2P payment systems which has triggered the annual 19 percent growth in digital transactions in 2016-17.

Another example of account number-less transaction is as illustrated in the Singapore case study.

Government to Person (G2P) Payments

In many countries Government benefits and subsidies are now increasingly being transitioned to being paid out as cash transfers, i.e., paying the benefit as a monetary value instead of as physical goods or services. This is another key example where digital ID can be utilized to support automatic and hassle-free payouts- as well as to weed out payments made to fraudulent accounts. The same principle has been used for disaster relief and humanitarian relief payments made directly to transaction accounts as described in the next section.

An important and successful example of enabling digital G2P payments is in Pakistan through the NADRA (National Database and Registration Authority) who is responsible for issuing the CNIC (Computerized National identity card) to the citizens of Pakistan.

Importantly, mapping the ID of the individual to their eligibility records in the social benefit transfer systems enables government agencies to reliably ensure that only eligible individuals are receiving the transfers and no individual is able to avail the same services from different locations or different points of time using a different identity. This has substantial implications for the public financial management systems and is also critical for public sector employee salaries and pension payments.

Role in Humanitarian Assistance

The digital ID initiatives have had significant impact on providing humanitarian assistance especially for internally-displaced persons (IDPs) and refugees.[90] This section provides an overview of the sources of ID and the challenges of implementing digital ID in this context.

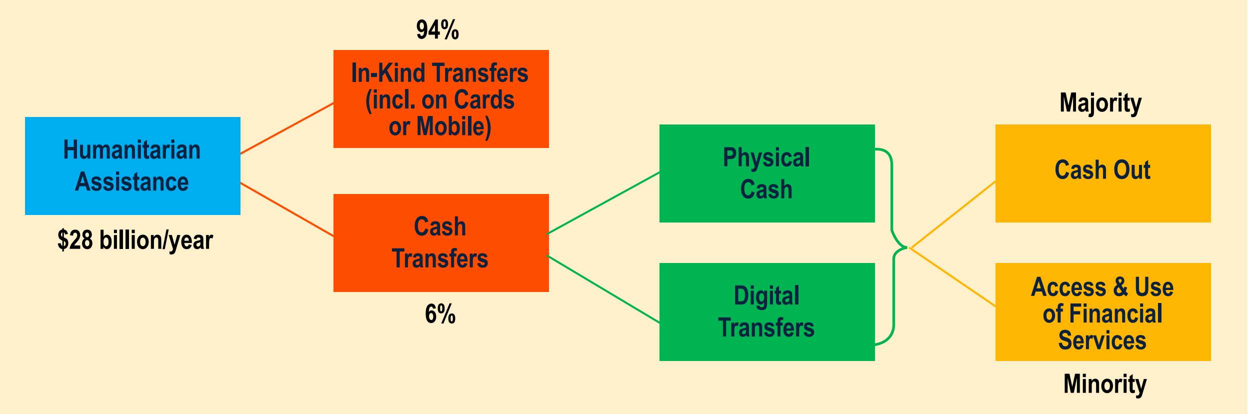
Of the USD $28 billion given out in humanitarian assistance per year, 94 percent are in-kind transfers, while 6 percent are cash. Of this 6 percent, a certain proportion are in the form of electronic transfers. Digital ID will help ensure that the assistance reaches the intended recipient. The authentication[91] of a beneficiary's identity is crucial to cash transfers for two primary reasons: the full potential and advantages of cash transfers over in-kind assistance are only realized if disbursements can be made remotely and digitally and backed by appropriate ID and authentication systems, funds traceability is a key government and donor requirement to scale up cash transfers given the high perceived risk of fund diversion for financing of terrorism.

The table 1 provides an overview of the different sources of ID in the top ten refugee hosting countries. Few governments have issued a formalized national ID system. However, it should be noted that birth registration by the government and provision of a United Nations High Commissioner for Refugees (UNHCR) ID is more persistent in the sample chosen.

There are a number of challenges that hamper the creation of a digital ID for displaced persons:

- *Insufficient evidence of their identity:* Refugees and asylum seekers may arrive in a host state without reliable evidence of their claimed identity, such as a passport, national ID or birth certificate from their country of origin. This may delay their registration by the host state or by UNHCR and could even prevent it entirely. In Norway, Norwegian Refugee Council

Figure 10: Overview of Humanitarian Assistance



Source: 'The Role of Financial Services in Humanitarian Crises', WBG, 2017 estimates that 70 percent of Syrian refugees above the age of 14 do not have their Syrian national ID card.[92]

- *National laws or policies preventing recognition of refugees:* For legal or political reasons, a host state may not formally recognize the status of some refugees, preventing governments from carrying out registration themselves. In some cases, the government may consider the refugees a responsibility of the international community or recognize refugees but refuse to provide an ID for a real or perceived fear that this may prolong their stay.
- *Lack of demand from the refugees:* Refugees and asylum seekers may not register themselves with the host state, UNHCR and/or other agencies, possibly out of fear of extradition or even because they are unaware of the need to do so. Even when refugees register, should they fail to update their information on a regular basis, their ID becomes invalid (notably for use at third-parties).
- *Inadequate capacity:* Some host States may lack the human, financial or technical capacity to carry out effective and timely registration and RSD (Refugee status determination). In many countries, registration and the provision of an ID is linked with a positive RSD. Authorities may have a backlog of RSD applications that could lead to asylum seekers waiting weeks, months or even years for a decision. During this time, they may be provided with a temporary ID, such as a paper certificate, to prove that they have submitted a RSD application. However this temporary ID may not enable them to access certain services, such as purchase of a SIM card.

A digital ID when rolled out effectively can mitigate the impact on host communities by providing an efficient system to help host states and humanitarian partners evaluate the scale and type of assistance needed. It can also support the realization of durable solutions such as voluntary repatriation, resettlement to another country, or integration into host communities.

UNHCR is one of the leading international agencies which is pioneering digital ID in many of the conflict countries, as part of its mandate related to refugees. UNHCR will – on invitation from and in collaboration with, the host state – step in where authorities lack the capacity, resources and/or willingness to carry ID registration for refugees and asylum seekers. In cases where the host state registers refugees and maintains an ID system, UNHCR may also maintain a parallel system for its own operational purposes, from which the data – under appropriate conditions – could be shared with the host State. However, IDs cards issued by UNHCR are not always recognized as evidence of identity or legal status and may not be accepted by service providers outside of UNHCR-administered settlements. UNHCR-issued IDs (refugee cards & asylum-seeker certificates) tend to be widely accepted for authentication among humanitarian organizations.

Table 1: Comparisons of Different ID Systems for Refugees

Country (# of Refugees)	Access to ID/Registration by Source			
	Govt Issued National ID System	Govt Issued Standalone Refugee ID System	Birth Registration by the Govt	UNHCR Issued
Jordan (685,197 under UNHCR; 2.2 million under UNRWA)	Only some Palestinian refugees	Yes	Yes	Yes
Turkey (2.9 million)	Yes (as a Foreigner)	No	Yes	Yes
Pakistan (1.4 million)	No	Only refugees who arrived before 2015	No	Yes
Lebanon (1 million under UNHCR; 463,700 under UNRWA)	No	Only Palestinian refugees	Yes	Yes*
Iran (979,435)	No	Yes	Yes	Yes
Uganda (940,835)	No	Yes	Yes	No
Ethiopia (791,631)	No	No	Yes	Yes
Germany (669,482)	No	Yes	Yes	No
DRC (451,959)	No	No	Yes	Yes
Kenya (451,099)	No	Yes	Yes	Yes

Table 2: Comparison of ID Registration Processes[93]

	Host State-led	UNHCR-led[94]	Decentralized
	Not Mutually Exclusive		
Process	The Government registers refugees and asylum seekers and issues an ID via (i) a standalone refugee ID system; (ii) a refugee category in the national ID system; or (iii) integration into the resident ID system. The government can be supported by UNHCR or other agencies during registration.	With authority from the host State, UNHCR registers refugees and asylum seekers and issues an ID. The registration may be carried out jointly with the host state, but UNHCR manages the data.	A refugee or asylum seeker registers themselves into an online system that stores the data in a distributed ledger (DLT) that does not have a central authority, and may be global in nature and not specifically targeted at refugees. A foundation needs to be present for registration, once done it removes the need to revert back to the original source.
Examples	• Dedicated refugee ID system: Pakistan, Jordan, Uganda, Kenya • Category in the national ID system: Tanzania, Rwanda • Resident ID system: India	• In parallel with the host State: Jordan, Thailand • In lieu of the host State: DRC, Egypt, Ethiopia, South Sudan	• Civic • Sovrin
Advantages	• Likely to be the most widely-recognized and interoperable for authentication, and thus facilitates the greatest access to services and opportunities (e.g. banking and CDD requirements); • Most useful for facilitating durable solutions; • Usually also involves RSD (except if a resident ID model), which is key to facilitating protection and identifying special needs.	• Accessible to anyone making a claim for refugee status; • Very efficient, especially to identify and address special needs of women, children and other vulnerable persons, since UNHCR has high capacity and extensive experience; • Recognized by UNHCR operations across different countries; • UNHCR allows host States to access data after signing a MoU with safeguards; • Trusted by resettlement destinations.	• Not necessarily linked to a jurisdiction; • May—in theory—provide the refugee with the greatest control over their identity data; • Fully digitized and hence most portable; • Could be an effective complement or add-on to host-State led or UNHCR-led IDs
Disadvantages	• Lack of sufficient capacity and burden on host countries; • High identity proofing threshold; • Dedicated refugee ID system may not be interoperable with the national ID system or resident ID system; • Resident ID does not provide proof of refugee status; • Can be revoked or invalidated by the host State at any time.	• May not be widely-recognized; • Carried out at the invitation of the host State and thus could be discontinued anytime; • Not sustainable as dependent on external financing; • Assuming a responsibility that should ideally be the host State's remit.	• Does not address protection issues • As yet unproven method • Heavy reliance on the Internet and mobile devices limiting accessibility, as well as technical literacy and skills; • Lack of universal recognition by governments, international organizations, or service providers; • Trustworthiness based on the reliability of the original identity documents presented to assert identity; • Immutable nature of DLT might mean that a refugee's personal data cannot be removed, even when they cease being a refugee in most cases. • Global, publically-available platform has inherent security risks.

Table 2 draws comparisons on the providers of ID and the pros and cons associated with each.

The use of digital ID in humanitarian causes has been expanding over the years. In countries such as Egypt, India, Uganda, Syria, the impact of digital ID through the UNHCR systems or national ID systems have allowed refugees to secure aid in a more targeted and organized manner. In Jordan, in collaboration with UNHCR, World Food Programme (WFP) and IrisGuard, has allowed 76,000 Syrian refugees to purchase food from camp supermarkets and withdraw subsidies from iris authentication enabled ATMs, replacing cash, vouchers or e-cards.[95] The use of WFP's biometric-based identity and beneficiary management system – SCOPE – for refugees in Kenya enabled WFP to realize monthly savings of $1.5m by removing duplicate and ghost records.[96]

The use of digital IDs in the humanitarian context has demonstrated its potential for efficiency, de-duplication and fraud assessment. However, although the advantages may outweigh the drawbacks, important questions and challenges must still be addressed regarding implementing organizations, data ownership and security, and the ability to implement a solution during the early stages of a crisis within the legal and infrastructure requirements of such solutions.

Credit Reporting

Credit reporting systems (CRS) store data about consumers' repayment behavior of their financial obligations, reliably linking all records collected from different institutions to the relevant consumer and building up a profile of the customer. When it comes to credit products, lenders use risk management and underwriting procedures that traditionally supplement their credit appraisal process with data pulled from this credit reporting system.

The General Principles for Credit Reporting (GPCR) issued in 2011[97] by the International Committee on Credit Reporting (ICCR) recognize the need for data included in the CRS to be unambiguously linked to the customer ('data subject'). The ICCR also recognize that effective credit reporting for disadvantaged individuals remain a challenge. An effective credit reporting, they say, are reliable mechanisms for identifying individuals and firms as well as for linking them unequivocally with their financial obligations.

There is a need to be able to uniquely identify the individual or legal entity and use that unique identifier to organize all the records in the database. This seamless integration or linking of a unique ID with the credit reporting systems is exhibited in the Pakistan case study.

Box 16: Case Study: Pakistan *'NADRA'*

The Electronic Credit Information Bureau (eCIB)[98] has facilitated linkage between a persons CNIC (computerized unique national identity card) to their credit information based on conducting NADRA online verification and authentication process. The eCIB has two types of credit reports which are the consumer and corporate credit reports respectively.

In the consumer credit report, individuals are mapped to their CNIC for their consumer credit and default history over the last 12 months. On the corporate credit reports, each corporate entity (listed and unlisted) is mapped to a unique borrower code derived from the CNIC system. Member financial institutions are required to report all their financial obligations under a unique borrower code assigned to each entity. The corporate credit information report contains details of outstanding liabilities (fund and non- fund based), position of overdues, details of litigation, write-offs, recoveries and rescheduling and restructuring-providing a financial map of the entity.

In addition to the eCIB, (which is a more traditional credit reporting on banked customers), Microfinance Credit Information Bureau (MF-CIB)'s microfinance institutions can access the eCIB data. The country's banks have access to this data and can assess consumer credit status, based on prior consent, for financial and credit reporting purposes. The common link between these organizations (credit reporting systems, banks, microfinance institutions) is that the CNIC provides the unique identity for every individual in terms of their credit histories.

In addition, the Pakistan Credit Bureau Act of 2015 states "credit bureaus would be legally empowered to collect and be answerable for trustworthiness of credit information about debtors of banks, financial institutions, non-banking financial institutions (NBFIs), non-financial companies, leasing companies, and microfinance institutions." The law also provides access into bill payment history (e.g. from utility companies) when it comes to establishing a credit score.[99]

The lack of a unique ID in a credit reporting system could lead to inaccuracies and create serious problems to the integrity of the database such as duplication or the inability to match an individual to a credit score due to differently spelled names or addresses. This fundamentally impacts the effectiveness of credit reporting systems.

The credit reporting systems have developed various approaches to link records with different variations of a name or address to a particular individual. These however, are challenging in context of the financially excluded where an individual is new to the financial system and address details are not structured or do not have a dedicated address (for example using the address of another person - 'care of'). A related point to note is that the architecture of ID systems and credit reporting systems can vary. In contexts where these systems develop in parallel or where credit reporting systems precede the development of ID systems, it is important to compel the recording of the ID details of customers in the credit reporting system. In particular, where there is a unique ID, this can greatly enhance the reliability of the matching process within credit reporting systems. A digital ID system will further enable the credit reporting system to correlate details between the two systems.

As FSPs become more sophisticated, data other than traditionally collected credit reports and scores could potentially inform lending decisions or the provision of investment services. An example is the use of social data for evaluating credit worthiness and to provide a credit rating in China (please refer to the section on social data within authentication techniques). Linking such data also requires some form of mapping between existing identifiers used in the credit reporting systems and the ones used in other non-financial systems.

Credit bureaus also provide fraud prevention services due to the vast amounts of data on consumers from different data providers they collect. They can detect errors and signs of potential fraud including identity theft through monitoring techniques based on data reporting patterns.

Record-Keeping, Document Management And Digital Signature

Once the required ID validation and verification checks have been completed, FSPs need to preserve the records of the validation conducted, as required under the jurisdictional regulations. This involves maintenance of a significant amount of paper records. The use of a digital environment supplemented with a digital ID allows for a more efficient method to record, store and retrieve - by both the FSP and external parties such as auditors and regulators- these validations.

Consumer protection regulations in the financial sector rightly require express consent from customers to provide them with a service or change the terms and conditions of a current service. Complying with this requirement has often required physical interaction with the customer- which can be time-consuming, expensive and not always feasible. Digital signatures have been a solution to these concerns, however it has been a slow and expensive process to extend the service to non-corporate customers. In addition, it involves risks regarding consumer protection and consent which need to be addressed adequately.

Digital IDs however, can offer simpler and more cost-effective means to provision digital signatures, in an easy to use user interface. They have opened up opportunities for supporting remote account opening as is depicted in the Norway BankID framework.

Box 17: Case Study: Norway *'BankID'*

In 2004, through a collaboration between the Norwegian government and a group of cooperative banks, BankID was created as a unique digital ID primarily for financial transactions.[100] More than 7.5 million Norwegians (75 percent of the adult population) now use BankID to prove their identity and complete transactions online. Access to internet banking and the digital signing of financial documents are services most commonly used by customers.

The system is simple to use, requiring users to enter their personal identification number, their chosen personal password and a one-time password (OTP) from their physical code token. An electronic signature using BankID is just as binding as a handwritten signature on paper. By the end of 2014, the long-awaited Java-free BankID 2.0 project was complete and implemented by most banks. Also, more than 600,000 Norwegians now use Mobile Bank ID,[101] which uses the same secure technology but generates and stores the security elements on a mobile phone's SIM card instead of a physical token.

Access to digital signature infrastructure and allowing customers to authenticate themselves digitally enables financial institutions to interact remotely with customers, exchange agreements as well as terms and conditions and other confidential documents digitally. This can bring about significant cost savings for both individuals and the FSP by reducing the cost of paper based processing, transmission and associated staff time; enabling faster turn-around times and automation with the internal systems of a FSP. Digital IDs can help businesses streamline onboarding of new customers and allow legally-binding contracts to be signed online. For example, Netherlands-based Rabobank has partnered with Norwegian digital ID provider Signicat to offer their customers a range of services like online login, identity, signature and data archiving services under the banner of Rabo eBusiness.

Customer consent is gaining more prominence given the strong focus on digitization being a core component of fintech developments, notably to provide consent for collecting data from external sources and also the ability to initiate transactions on behalf of the customer.

Small Businesses

While this report focuses on identity verification for individuals, it is as important for MSMEs to establish the identities of staff and directors authorized to setup, operate and instruct changes for the business. Obtaining business bank accounts or payment services often requires formal business registration documentation, which can be costly and cumbersome to obtain. Without such formal business identification, FSPs find it difficult if not impossible to provide appropriate financial services to businesses and the businesses in turn continue to operate in cash, with no recourse to a line of credit due to a limited credit history and continue to be caught in a vicious cycle. A pertinent example that deals with the challenges of small and medium businesses is Canada's Digital ID for businesses as showcased in Box 18.

Some other relevant country examples include: Aadhaar in India is being used to assert and confirm the identity of participants in transactions, from opening a bank account, fund transfers, to trading in securities, and the ownership of businesses (through the Udyog Aadhaar registration process for MSMEs, where an Aadhaar number is associated with a company registration).[102]

Bangladesh[103] is following a similar path. For larger businesses, they are recording the digital IDs of the board of directors and management team, which when combined with information on transaction patterns, could have implications for validating beneficial ownership of the business.[104] Broader monitoring of this nature is likely to significantly ease the task of the regulatory and enforcement authorities, though it is also likely to raise demands for the appropriate tools to trace the changing ownership of assets and funds, which could potentially be a significant opportunity for the developers of 'regtech' services. Other examples can be found in the *'GPFI report on alternative data transforming SME's'*[105] besides the Serbia example Box 19.

Where the ownership of an asset is with a company, rather than a private individual, then such controls are limited to the availability of a corporate digital identity. The issuance and usage of corporate digital identities

Box 18: Case Study: Canada *'BN9'*

A 9 digit BN (BN9) number, administered by the Canadian revenue agency, is used to identify businesses at the national level. While the role of BN number is multifold, it has helped to substantially reduce the amount of time required to get registered and moreover is more cost effective than traditional registration processes. The initiative has adopted more than 100 program areas across Canada to enable registration and business approvals.

Box 19: Case Study: Serbia *'UBI Digital ID'*

Serbia[106] has a unique 12 digit UBI digital ID which is mandatory for all businessmen as a form of identification within the country. One of the key objectives of the ID was to reduce the number of days required to set-up a business and improve the ease of business ranking. A robust unique ID which was connected to all government divisions enabled Serbia to reduce time to register a business from 52 weeks to 5 weeks and then to 1-3 days. There was a significant improvement on risk based tax compliance due to accurate data, less administrative burden on entrepreneurs and overall improvement in business functioning.

is well established, particularly in the financial sector, though there have been issues around recognition and acceptance by regulatory authorities. An issue that was recently addressed in Singapore, when the government introduced the 'CorpPass'- improving the ease of doing business for corporates and the government.

A corporate digital identity is only useful if it can be reliably and securely asserted, which requires access by a 'natural person', who must assert and authenticate his/her own identity attributes, before being allowed to access and assert the corporate identity and associate it with a transaction. One example of this is Nigeria, where the Bank Verification Number (BVN) of a Director or an authorized signatory of the company must be provided.

Insurance

A unique digital ID is an important asset in the insurance industry as well. A vital facet of this is the ability to provide digital consent- which comes into play in a number of service offerings. A digital ID offers the ability to establish remote ownership of an asset; for example, it can link a driver's license to a unique ID establishing a unique link that has implications for insurance.

For uses such as universal health care coverage which require large scale and integration, the importance of valid authentication and accurate records are being considered by governments globally. The ability of digital ID systems to aggregate data and provide valid authentication and maintain accurate records is extremely important and is more relevant in countries which are scaling up for universal health coverage. In Thailand,[107] for example, the national population registry serves as the baseline list of beneficiaries for the universal healthcare scheme, allowing for rapid coverage and eliminating the need for a duplicative enrollment campaign.

Importantly, health financing and insurance schemes also need complete and accurate records on service usage and data on system performance to correctly bill patients and care providers and to inform budgeting and management decisions. In a country like Republic of Korea, where more than 97 percent of the population are part of a single insurance scheme, this becomes all the more relevant.

Box 20: Legal Entity Identifier (LEI)

A LEI is a unique code made up of a series of letters and numbers that can be requested by a legal entity. It was adopted by the G20 in 2012 and is intended for parties of primarily cross-border financial transactions with a global governance framework to represent the public interest and is related in the main to over the counter (OTC) derivative products. While there is no prohibition for legal entities in other sectors to request an LEI, there is a substantial cost attached and needs to be renewed on an annual basis. LEIs also record group structures – i.e. a subsidiary -parent relationship. Although LEI is intended to track counterparties of OTC derivatives, these could be used in other sectors. For example, LEI could be used to ease the efforts of supervisors and regulated entities when identifying legal entities in compliance with CDD and similar regulatory requirements.

Box 21: Case Studies: Estonia

In Estonia,[105] the linkage between the country's health information system and population register— underpinned by its unique eID and integration layer—has enabled every child to be automatically listed as a beneficiary in the health insurance fund from birth (World Bank 2015).[105] Furthermore, Estonia's e-Services infrastructure allows patients and providers to instantly check insurance coverage online using their national eID.

Furthermore, the EHIF (compulsory national insurance program) uses the eID to facilitate e-Services related to insurance and benefits coverage, such as allowing patients and doctors to conveniently check insurance information through online digital ID authentication. In addition, the EHIF also relies on the integration layer to update its health insurance registry of beneficiaries. The registry is updated daily with information on new births, deaths, and other changes. Newborns that enter the register through birth registration are linked to their mothers' eIDs and automatically entered as new beneficiaries. All children are thus guaranteed coverage from birth, regardless of their parents' work status or social contributions.

Korea’s NHI (National Health Insurance) system makes extensive use of administrative information sharing with the CRVS system (the registration system) to identify eligible beneficiaries and determine and collect insurance premiums. For example, determinations of health insurance premiums rely on the national ID number to verify subscriber’s personal income, tax, and pension information. After birth, parents register their newborns at a local office, and the infant receives a unique number (referred to as RR) which is entered into the CRVS system. Parents must then apply for NHI coverage of the newborn within 14 days, including the infant’s RR number and the parent’s ID numbers.

Besides the direct benefits to the insurance industry, the implication on insurance through the ownership of an asset via a digital ID is significant. For example, when a driver’s license is linked to a digital ID (as in countries like India, Peru, Estonia etc.), there is an indirect link to the insurance bought by that the concerned person (e.g. car insurance). Digital consent, mentioned earlier in the digital signatures sub-section, plays an important role in linking various services through the digital ID ecosystem. It is crucial that the digital consent infrastructure is secure for the digital ID to be successful in insurance-based applications.

KEY FINDINGS

Our review and analysis of ID requirements and its role in facilitating customer identification have led us to the following key findings.

Digital IDs Are Important to Public Policy and Service Delivery and Require Significant Support and Investment

A nation-wide digital identity system is critically important to support public policy programs and should be a key priority of policymakers, especially in the financial sector. In designing such systems authorities should consider the following:

- Any such digital ID system must not be limited to citizens, but it should be aimed at registering all residents (as well as citizens abroad). This can be problematic, however, if registration is based on documents that are only available to citizens or if non-citizens are required to prove legal status, which can be a challenge in some countries with porous borders, irregular migrants, displacement, and/or stateless populations.
- Excluding non-citizen residents can have implications that make it more expensive for banks to service non-citizens and could lead to their financial exclusion. This is particularly relevant to vulnerable populations like refugees and temporary work migrants.
- The use of a digital identity system for verification and/or authentication must be made available to all authorized service providers, from health and education through to the financial sector. The digital ID information should also be linked to the reference systems relied on by the financial sector like credit reporting systems, tax systems, business registries and other forms of legal ID.
- There are however political sensitivities around mandating the use of such a service for the receipt of social benefits and for financial services generally. This suggests that transitional arrangements must be put in place, to ensure that eligible individuals are not denied service due to the lack of a new ID. Likewise, there needs to be exception handling mechanisms to deal with situations where the digital ID system might be down or if someone cannot authenticate themselves for reasons beyond their control (e.g. worn fingerprints).
- It is important to carry out single robust identity proofing for each individual as part of the registration exercise, and rely on it repeatedly and across sectors, rather than do it inadequately many times over. Registration and the issuance of a digital identity is an expensive process. Investment in a high quality national foundational biometric digital identity service will derive the most benefit for the cost.
- National authorities must give careful consideration to charging fees and determining the pricing of identity verification services. While there is a natural desire to ensure that legal identity agencies are self-financing, this can serve as a disincentive financial and other service providers to link to these systems beyond the on-boarding process, resulting in duplicated systems and additional costs.

Digital Identity Can Be A Critical Enabler for Financial Inclusion

It is clear that where a national identity platform or service functions well, the financial sector is an active adopter of identity services. However, in cases where ID systems are non-digital (traditional plastic or paper card), even though useful, it does not allow for the full scale of benefits to be realized. This is particularly important for reaching previously underserved populations who may have trouble accessing or using existing identity systems.

The availability of a reliable, digitally authenticated identity system can strongly support financial inclusion initiatives in several ways:

- Digital IDs, especially those linked with biometrics, should make it easier for the unbanked to obtain financial accounts by simplifying the documentation requirements required at account opening. A digital ID is also easier and safer to replace if lost or stolen as credentials can be centrally verified and updated.
- Digital IDs can help financial institutions comply with the customer identification and verification components of CDD. It also provides more cost-effective ways of onboarding new customers, which could potentially be conducted by agents. Agents can use digital ID authentication to reliably record customer's identity and proof of validation which can be verified and used to feed the information from the digital ID system for the required CDD checks. When coupled with simplified CDD norms for basic transaction accounts, a significant portion of the customer onboarding process can be completed at the agent end itself, without the customer having to present themselves physically at the service provider offices or for a personnel of the service provider to travel to and meet the customer in person. However, this is dependent to a large extent on the agents having biometric compatible technology linked to the main registry.
- The development of an identity infrastructure, and the potential of basic transaction accounts linked to that infrastructure, are a necessary element of financial inclusion. However this alone is not sufficient. Digital IDs can contribute to financial sector deepening by supporting the adoption and delivery or more complex services, such as credit and insurance with minimal additional verification. The ability of digital ID databases to support the creation of credit histories for previously unserved customers will help service providers to extend credit and better monitor customer behavior and liabilities across multiple service providers.

Digital IDs Help Financial Service Providers Streamline Their Business Operations

Digital IDs help service providers streamline many of their business processes, from customer registration and transaction monitoring to credit risk assessment, compliance and reporting. Importantly for financial inclusion, such streamlining reduces the overall costs of providing service which should in turn help lower fees.

Digital IDs Can Help Bring More MSMEs Into the Formal Financial Sector

Many of the unbanked are small entrepreneurs who face the same financial exclusion challenges for their businesses as do individuals, namely, valid identity documentation. Digital IDs not only help these individuals access personal financial services, but also help them validate and register their businesses which in turn gains them access to business services such as credit, working capital and payment services. Digital ID for individuals has implications for larger businesses, as well, by connecting the digital ID of the board members, management team and authorized signatories to the ID of the businesses.

Digital IDs Can Support the Establishment of KYC Registries

The use of a digital ID system to build a centralized KYC registry increases CDD onboarding and verification efficiency for both the customer and FSP. For example, India has a centralized repository of capital market investor's CDD records, known as the Know Your Client Registration Agency (KRA). Aadhaar is one of the documents that can be submitted as proof of identity before the investor's details are uploaded to the KRA. The uploaded information is then made accessible to all capital market intermediaries registered with the Securities and Exchange Board of India (SEBI). The main purpose of a KRA was to eliminate duplication of CDD efforts that a customer must undergo while dealing with multiple market intermediaries like Mutual Funds, Private Equity Funds, Brokers, and Depository Participants. There is now an effort in India to expand this effort to the whole of the financial sector. Similar initiatives are proposed in several countries – for example Russia and Mexico.

There May Be Gains from Decoupling Identity Authentication from Other Functions

Digital identity systems, specifically those that provide online verification of identity credentials to third parties, allow identification, authentication and authorization capabilities to be combined, which can simplify operations for service providers, but can also inject privacy concerns around having so much valuable data in one place. Balancing the tradeoffs between convenience and privacy is an ongoing concern in the financial services space, and one for which there are no defined answers as yet. From the perspective of the government, uncoupling the provision of foundational identification from the

Box 22: Mexico *'CURP'*

The Clave Única de Registro Nacional de Población (CURP) is a key uniquely associated to each individual in the country, including non-citizens. It is issued by the National Population Registry (RENAPO). State-level Civil Registries provide RENAPO with birth-related information needed to generate each individual's CURP. However, one individual can have more than one CURP issued by the system. Birth certificates and the CURP serve as foundational IDs that enable individuals to obtain functional IDs that are used to vote and to access social security programs and public health care services.

Low-income individuals may lack the standard documents to satisfy KYC and AML/CFT requirements to open an account or to obtain a loan. In order to address this concern, risk-tiered accounts were created in 2009 with related tiered CDD requirements. Regardless of the ID presented to open an account or to obtain a loan, financial institutions need to validate that the information they collect, including the CURP individuals report, match RENAPO's records. This helps to reduce fraud.

Additionally, in 2017, regulatory adjustments to the identification process were introduced. These included requiring financial institutions to collect and verify biometrics for opening higher-risk accounts and for obtaining loans, or for performing high-value transactions at bank branches. These regulatory adjustments aid to reduce identity theft and further mitigate fraud.

responsibility for conducting a separate authentication by an FSP has the potential to support the relatively rapid roll out of basic digital identity credentials, with a wide uptake but based on low assurance identity data. The quality of the digital identity can be enhanced over time, in part simply through a history of ownership and use or by incorporating additional data points.

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

Private sector solutions built on top of the legal identity credential or system can greatly enhance authentication processes without jeopardizing the foundational identity role of the government system. Programs such as Gov. UK Verify[108] and Canada's Digital Authentication and Identification Council of Canada (DIACC)[109] provide solutions and frameworks that offer users and service providers authentication services without having to revert back to the original source of the identity. Services like the GSMA's Mobile Connect,[110] which adds an additional layer of security via the SIM card, can augment authentication efforts and strengthen security. And the FIDO Alliance's[111] work on identification protocols enable its member companies to produce products and services that adhere to common standards and technologies around authentication, again without necessarily having to establish direct linkages to official identity databases. These also illustrate the potential and the ability to integrate such initiatives with a government provided ID. Using FIDO alliance in combination with a one time validation using Government ID could be an example of such a collaboration, another example is Canada's Mobile Connect. It should be noted however that all these services rely on the individual's ability to present a foundational or functional ID to complete the initial registration in the process.

Other private sector initiatives like BankID in Sweden[112] and Norway[113] are examples of a secure solution to verify and authenticate an individual's identity that other service providers, including government, can utilize. Multiple service providers, including those outside the financial sector, use this solution to successfully identify a beneficiary/ customer without having to burden both parties with multiple document submissions or requests.

The Principles on Identification for Sustainable Development

As policymakers pay increasing attention to upgrading or establishing ID systems, they are realizing that the issue of identity is a complex, multi-faceted topic that is being asked to meet many varying national and social needs. Furthermore, as these needs evolve over time, the design of digital ID systems needs to be future-proofed[114] to reduce potential (and costly) failure or weaknesses in its functionality, as well as to facilitate interoperability with existing and new hardware and software technology.

With that in mind, the common Principles fundamental to maximizing the benefits of identification systems for sustainable development were developed facilitated by the World Bank Group and the Center for Global Development.

The management of personal identity can be seen as part of a continuum or lifecycle that includes five fundamental stages: (a) Registration, including enrollment and identity proofing, (b) Issuance of documents or credentials, (c) Identity authentication & verification for service delivery or financial transactions, (d) Authorization and (e) Identity management. Please refer to Annex 2 for a description of the various steps in the identity lifecycle.

Table 3: Principle on Identification for Sustainable Development: Towards the Digital Age[115]

Inclusion: Universal coverage and accessibility	Ensuring universal coverage for individuals from birth to death, free from discrimination.
	Removing barriers to access and usage and disparities in the availability of information and technology.
Design: Robust, Secure, Responsible and Sustainable	Establishing a robust-unique, secure, and accurate-identity.
	Creating a platform that is interoperable and responsive to the needs of various users.
	Using open standards and ensuring vendor and technology neutrality.
	Protecting user privacy and control through system design.
	Planning for financial and operational sustainability without compromising accessibility.
Governance: Building Trust by Protecting Privacy and User Rights	Safeguarding data privacy, security, and user rights through a comprehensive legal and regulatory framework.
	Establishing clear institutional mandates and accountability.
	Enforcing legal and trust frameworks through independent oversight and adjudication of grievances.

POLICY CONSIDERATIONS

Based on current experiences and the lessons learned from both national identity programs and private sector initiatives, the following policy considerations are presented as a basis for national policymakers, especially in the financial sector. The field of digital identity is rapidly evolving, so it is imperative that central authorities and public bodies consistently incorporate new technologies and business models while protecting the financial sector and its customers.

Ensure an Integrated Identity Framework

A legal or foundational identity system is critical to reliably assign an identity recognized across Government and the private sector. It forms the legal basis for identity validation for critical services and critically, governments should update existing privacy frameworks in the context of planned and potential future uses of digital ID services. In the financial sector once the identity validation is done, the subsequent interactions of the customer with the financial service provider can use other approaches for authentication and authorization in the process of service delivery.

Policymakers should:

- Design digital infrastructure appropriate for the context, including strategies to reach remote areas and ensure 'last mile connectivity'. Off-line solutions can complement the absence or loss of on-line connectivity.[116]
- Develop robust procurement guidelines and should contemplate open design standards to promote innovation and allow for greater flexibility, efficiency and functionality of the system both within and across borders.
- Ensure the technical capacity of government agencies, private sector and other stakeholders in the digital identity ecosystem (including end-users) to operate and maintain new systems and devices.

A biometric-based legal identity system can potentially support both compliance with authentication services and AML/CFT customer identification and verification requirements, upon which the service provider can further develop authentication and authorization processes. However, wide-spread use of legal identity infrastructure for multiple phases of financial services provision (e.g., onboarding and authorizing access to established accounts) has implications at several levels, including the cost of replacing existing infrastructure established for these processes; the pricing of these services; a liability framework for false-positives and false-negatives for biometric credentials; and the impossibility of replacing authentication credentials in a centralized legal identity database if there is a compromise of biometric information.

There therefore needs to be careful consideration of these and other potential issues relating to using national foundational identity infrastructure for on-going transactional authentication and authorization. This includes whether to reserve the use of the national foundational identity infrastructure for providing proof of verified legal identity for customer identification/verification at on-boarding or if other well-established reliable, efficient and safe processes exist for authentication/authorization functions.

Consider the Appropriateness of the Regulatory Framework to Capture the Challenges Related to Digital ID, and Risks to Its Appropriate Implementation; Deliberation on Updates to the Regulatory Framework Including the Issuance of New Regulations Where Necessary

The introduction of digital identity services can enable faster, more cost-effective means of meeting identity validation, authentication and authorization requirements, as well as improve monitoring and oversight for both service providers and regulators. In some cases, however, regulations need to be introduced or updated to reflect the capabilities and risks of such new technologies. Of the ten Principles on Identification for Sustainable Development,[117] three specifically focus on the issue of governance, including the regulatory framework.

Financial services sector regulations have longstanding requirements related to identity validation, authentication and retention of records, to ensure the safety and integrity of the financial system, based primarily on the FATF recommendations. It is important that each country's financial services regulatory framework recognizes the potential of digital identity services to support both trustworthy identification/verification for AML/CFT compliance and financial inclusion. The regulatory framework should recognise that requirements for the use of digital identity services in the financial sector, including for account opening, are risk-based and reflect both the potential benefits of digital identity technologies and the risks associated with a particular customer, financial services, or whether the account opening and customer identification/verification is remote or in-person. Among other things, the regulatory framework should authorize remote digital identification/verification and account opening at certain risk levels and levels of trustworthiness provided by the identity service, particularly for financial inclusion purposes where other risk mitigants, such as tiered account or transaction thresholds, are available. Any such regulatory reform must be done in a way that is aligned with FATF recommendations.

The specific areas which may need to be addressed in a regulatory framework include, but are not limited to, whether or not:

- digital identity validation using digital means constitutes completion of identity verification under prevailing AML/CFT requirements;
- legal certainty and equivalence between digital signatures and physical signatures;
- the private sector managed third party authentication services are recognized as legally equivalent to a bank doing identity identification and verification itself and if so, where regulatory liability lies with respect to any failures regarding customer identification/verification and authentication/access processes;
- when there is universal coverage of a particular identity credential all bank customers should be required to provide that. Preferably this identity credential should have the characteristics of being legal, unique and digital;
- consumer interests are protected when new digital ID services are made mainstream, in particular ensuring that no segment of customers are placed at a disadvantage; and
- privacy considerations in the financial sector are protected when using third party services and alternative sources of data.

Establish a Reliable Oversight Model to Include Stakeholders Beyond the Traditionally Regulated Financial Institutions Who Can Introduce Risks to Digital Identity Systems

Financial institutions are subject to often rigorous supervision and must adhere to a number to measures as dictated by governments. This is due to the significant financial stability and consumer protection implications they have. This policy recommendation aims to specifically highlight that oversight needs to be maintained not only financial sector players but others within the ecosystem that contribute, collect, store or disseminate information related to digital ID.

Oversight frameworks need to consider risks of

- data security and no compromise on protection of privacy;
- robustness of the underlying technology, systems and processes used for digital ID;
- ensuring that the technology and business model is updated in keeping with the rapidly changing landscape; and
- ensuring effective governance arrangements for the use of digital ID infrastructure in the financial sector, particularly as it applies to non-regulated entities.

Many of these aspects may be covered in a general legal and regulatory framework for digital IDs, though there might be a need for some specific regulations related to their use for the financial sector. The prevailing FATF recommendations, in particular, Recommendation 10 and 17 relating to CDD and 'reliance on third parties,' respectively have a bearing on outsourced identity services and the ability to perform parts of the CDD process. But it also makes clear that where such reliance is permitted, the ultimate responsibility for CDD measures remain with the financial institution relying on the third party.

Build Authentication and Service Delivery Systems That Protect User Privacy, and Provide Individuals with the Right to Access Their Data and Oversight Over How Their Data Is Shared

The adoption of Privacy by Design approach to ID systems could be considered: This process envisages building privacy into all stages of the design and architecture of information systems, business processes, and networked infrastructure. The focus is on taking a proactive, preventive approach to the protection of privacy and the avoidance of privacy harms. The concept rests on the following seven principles: 1. Proactive, not reactive; preventive, not remedial 2. Privacy as the default setting 3. Privacy embedded into design 4. Full functionality—positive-sum, not zero-sum 5. End-to-end security—full life-cycle protection 6. Visibility and transparency—keep it open 7. Respect for user privacy—keep it user-centric. This approach together with data minimization could mitigate privacy concerns. Even if the ID system stores a considerable amount of data items, the systems should enable users to verify and validate identity accessing the minimum possible data items.

Further, ID systems should be vested with security measures to protect the data. Given the nature of the data stored in the systems, the security should follow a tridimensional approach (logical, physical and organizational) and should include not only the system where the data is stored but also the network enabling its access, the back-up systems and any others linked to the personal data of the individual including those third parties that perform any task related to the personal data included in the ID system.

Establish Clear and Well-publicized Procedures for Citizen Redress Including Where the Onus of Responsibility lies, in the Case of Errors or in the Event That the Security of a Person's Identity is Compromised

To maintain the integrity of the system and ensure that there is trust in the system policymakers should consider the need for resolution and regulatory redress systems. There is a suggestion that if policy makers see themselves as having a democratic responsibility to build an identity infrastructure that allows users to control their identity information- aiming towards a self-managed identity- it will promote accountability and trust. The identity infrastructure should be built in such a way as to allow audits enabling records for local redress if needed. There is arguably an ombudsman role for accountable officials to play in verifying that individual data, if shared without consent, receives proper treatment and is safeguarded from subsequent misuse by downstream actors.[118]

Support and Empower Development of Private SectorLed 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

National legal identity infrastructures can provide the fundamental platform on which the private sector can build solutions to meet the needs of the financial sector and beyond. Authorizing private sector providers to leverage the national digital identity platform could potentially provide better digital identity products and services and faster roll out than the state alone can achieve. Two of the Principles on Identification, in fact, specifically call for creating interoperable platforms using open standards for this very reason. However, enabling an effective private sector role imposes requirements on the identity platform, particularly in relation to requirements establishing interoperability, open-source access, such as through areas of open interfaces, and requirements for sustainable charging models.

Countries with existing established foundational systems, but with some weaknesses could potentially exploit private sector led services to address the gaps, instead of building additional new infrastructures. For example, a country with a well-functioning, reliable and efficient paper based legal ID system with universal coverage could leverage private sector services under a 'broker' model to offer digital ID services. These private sector players conduct authentications based on the original legal ID, which various private sector players are already doing as part of their ongoing activities.

Even countries with comprehensive government led digital ID systems can allow third parties including the private sector to build out additional services that rely on the state's digital ID. In some countries, there is a noticeable effort by Government agencies responsible for the ID systems to develop ancillary services. For example, in India, services such as e-Sign and Digital Locker (DigiLocker) both rely on Aadhaar to offer additional services such as electronic signature and an on-line document storage service respectively. If unsuited to their needs, FSPs may aim to conduct their own authentication for transactions after initial account opening. This illustrates the need to carefully balance the role of the Government agency to provide the foundational services in a sustainable manner on the one hand and the impact of cost structure of using ID by the FSPs and other uses. There are opportunities for private sector to develop solutions on top of the foundational services. This removes the operational burden of operating ancillary services from the government agencies.

A conglomeration of global entities, private and public entities, have collaborated into international alliances to foster legal ID infrastructure among other services. An example is the FIDO alliance. The alliance hopes to provide a myriad of benefits to customers including stronger account/transaction security, improved user experience, improved return of investment on authentication and reduction in fraud services. It also aims to enhance leveraging legal ID infrastructure in the ecosystem.

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

There are a number of emerging technologies and new combinations of existing technologies that have the potential to leapfrog the need for a unique national identity platform, digital or traditional. These methods include using distributed ledger technologies and social data. However, these are currently in very early stages of development and do not represent a viable alternative for a comprehensive build out of a foundational legal ID infrastructure.

As with any innovation the capabilities can dramatically increase and hence authorities need to closely monitor developments, use prevalent best practices and think in terms of open interfaces and modular approaches in the build out of legal ID platforms.

ANNEX 1: LEVELS OF ASSURANCE[119]

Identity Assurance Level (IAL)

- IAL1 – Self-asserted; no requirement to link the applicant to a specific real-life identity.
- IAL2 – Evidence supports the real-world existence of the claimed identity; either remote or physically-present identity proofing.
- IAL3 – Physical presence is required for identity proofing. Identifying attributes must be verified by an authorized and trained representative.

Authentication Assurance Level (AAL)

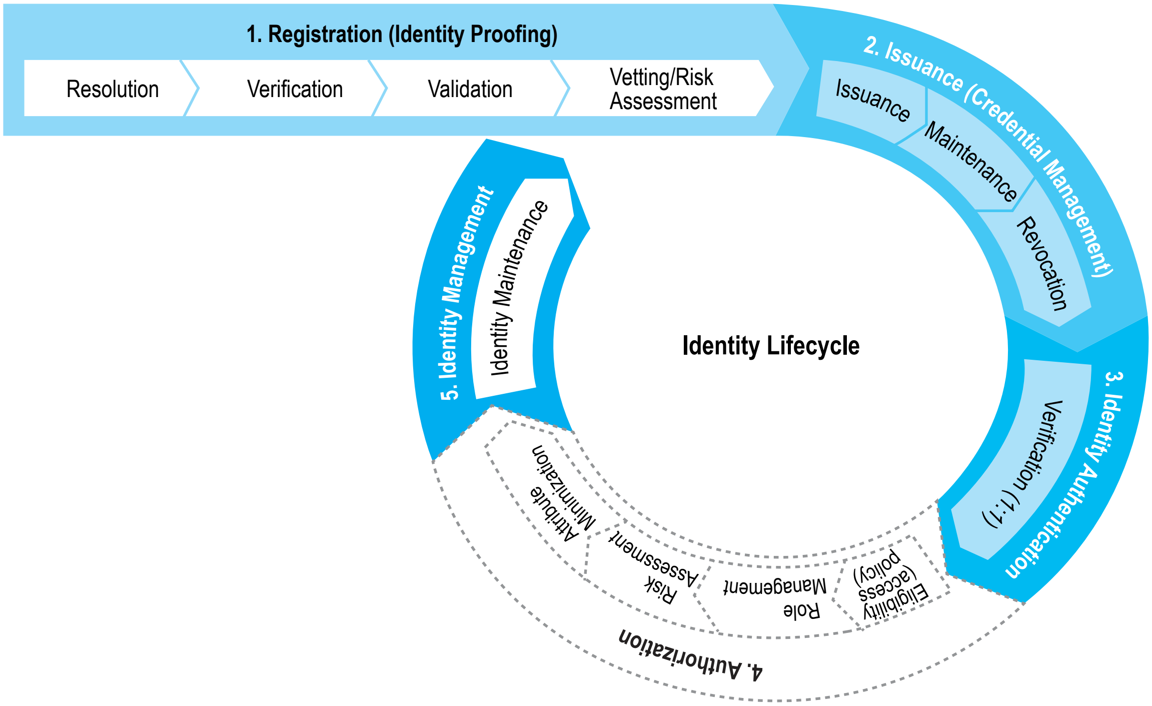
- AAL1 – Provides some assurance that the claimant controls the authenticator; requires at least single-factor authentication.
- AAL2 – Provides high confidence that the claimant controls authenticators; two different authentication factors are required; approved cryptographic techniques are required.
- AAL3 – Provides very high confidence that the claimant controls the authenticator; authentication based on proof of possession of a key through a cryptographic protocol; requires a ‘hard’ cryptographic authenticator.

Federation Assurance Level (FAL)

- FAL1 – Allows for the subscriber to enable the RP to receive a bearer assertion.
- FAL2 – Adds the requirement that the assertion be encrypted such that the RP is the only party that can decrypt it.
- FAL3 – Requires the subscriber to present proof of possession of a cryptographic key referenced in the assertion in addition to the assertion artifact itself.

ANNEX 2: THE IDENTITY LIFECYCLE

Figure 11: Digital Identity Lifecycle and Key Roles[120]


1. Registration (Identity Proofing)
Resolution
Verification
Validation
Vetting/Risk Assessment
2. Issuance (Credential Management)
Issuance
Maintenance
Revocation
3. Identity Authentication
Verification (1:1)
4. Authorization
Eligibility (access policy)
Role Management
Risk Assessment
Attribute Minimization
5. Identity Management
Identity Maintenance
Identity Lifecycle

Registration (Identity Proofing)

The registration process involves an applicant providing evidence of his or her identity to the issuing authority. The identity credential here can take a variety of forms and its acceptance will be based on the specific regulations within the jurisdiction. The accuracy and reliability of each credential can vary based on variables such as the information recorded and the validation it was subject to. Ideally, a digital identification system should be integrated with civil registration, which is the official recording of births, deaths, and other vital events including marriages, divorces and annulments.[121]

If an individual reliably identifies himself or herself, the authority can assert that identity with a certain level of assurance. In developing countries, and in cases like those of displaced persons or refugees (*discussed in more detail later in the document)*, it is not uncommon for applicants to lack fundamental documents (birth certificate, passport, utility bill, driving license). In such situations, identification systems may use an individual[122] who is tasked with verifying the applicant's identity and address. Once verification is completed, biometric registration and de-duplication will bind the applicant to his or her identity claim, which will then be used during subsequent identity interactions.

Once individuals have an identification document, the process of registration may start with ***Resolution***,[123] the process of uniquely distinguishing an individual in a given population or context. The applicant presents biographic information, or documents such as birth certificates, marriage certificates, and social security documents, as well as photographs which are then validated and augmented by the registration authority as needed. A growing trend in recent years has been to use biometrics to ensure that an identity is unique.

The next step is ***Validation***, where the authority determines the authenticity, validity, and accuracy of the identity information the applicant has provided, and relates it to a living person. An ID with a digital characteristic could be provisioned digitally through a digital certificate or a smart card, it could also be provisioned in paper form, but with associated service infrastructure built around it to enable a digital authentication approach. When the ID validation process can be done digitally and the proof of validation recorded digitally, there can be a true seamless process for ID validation.

This is followed by ***Verification***, the establishing of a link between a claimed identity and the real-life subject presenting the evidence. The final step is ***Vetting/Risk Assessment***, assessing the user's profile against a watch-list or a risk-based model.

In advanced economies, information needed for registration is typically universally available. In other countries, even if such identity credentials are available, they might not be universal or easily obtained. Members of marginalized groups such as the poor, the elderly, women, and infants have a higher propensity of not being captured. Some individuals may have poor biometric features (like poor fingerprint ridge structure) that make accurate enrolment difficult. Moreover, there are issues of the affordability and accessibility of the hardware and software used for registration.

When considering the implementation of an ID system, policymakers should ensure that the scope of the process must be clearly defined, including the population whose data will be collected, the attributes that will be collected, and the corresponding performance of the registration system. For instance, will registration be for residents of that country only, or for visitors as well? Will the information required for registration include name, birth details, or fingerprints? What are the accuracy and confidence levels of the registration process? Clearly defining the scope of the population whose data will be collected and the attributes that will be collected will mitigate any future issues related to privacy and consent.

Issuance (Credential Management)

Issuance is the process of creating and distributing virtual or physical credentials like e-passports, digital ID cards and driver's licenses and a unique identifier (with central biometric authentication), such as the Aadhaar system in India. The other steps are **Maintenance** (the retrieval, update, and deletion of credentials) and **Revocation** (the removal of the privileges assigned to credentials).

In some countries, primary legal identity credentials also imply citizenship rights, in the sense that it legally accords proof of residency or nationality. Examples of this include Pakistan's NADRA CNIC card and Peru's DNI card. There are also examples of countries where primary legal identity systems do not accord citizenship rights (e.g., Aadhaar in India).

Interoperability of these credentials for authentication is becoming increasingly important for intra-country and inter-country service delivery, as can be seen in the European Union (EU), East African Community (EAC), and West Africa regions. In the EU, for example, electronic identification (eID) and electronic Trust Services (eTS) provide the interoperability framework for secure cross-border electronic transactions of the Digital Single Market under the electronic Identification, Authentication and Trust Services (eIDAS)[124] *(see key terms and definitions)* regulation.

Identity Authentication

Authentication is the process of verifying an identity claim against the registered identity information. Such information could be a personal identification number (PIN), a password, biometric data such as a fingerprint, a photo—or a combination of these. Challenges in this phase include how to reduce processing time, improve accuracy of matching for authentication, ensure a seamless experience for applicants, mitigate challenges with network connectivity, counter fraudulent behavior, and find affordable hardware and software solutions.

An important criterion around authentication in financial services is a concept known as a 'Level of Assurance', or LOA. A Level of Assurance, as defined by the by ISO/IEC

Box 23: eiDAS

There has been rapid progress across the world in adoption of statutory legal measures to give legal certainty and equivalence to digital signatures and physical signatures. Regulation (EU) N°910/2014[125] eIDAS is an EU regulation on electronic identification and trust services for electronic transactions in the internal market that was adopted in July 2014. It is a set of standards for electronic identification and trust services for electronic transactions in the European Single Market and is an example of providing explicit legal basis for identity services. It seeks to establish a single legal framework for recognizing electronic signatures and identities throughout the EU.

The Directive does not make digital identity (eID) mandatory, but does aim to greatly increase the mutual recognition of eID between countries, in order to facilitate cross-border business as well as international administrative tasks for citizens. To this end it aims to ensure that both people and businesses can use their own national electronic identification schemes (eIDs) to access public services in those other EU countries where eIDs are available, and creates a new EU market for 'electronic Trust Services' (eTS) – namely electronic signatures, electronic seals, time stamps, electronic delivery services and website authentication – by ensuring that they will work across borders and have the same legal status as traditional paper based processes.

29115 Standard,[126] describes the degree of confidence in the processes leading up to and including authentication. NIST describes varying levels of assurance[127] (LOA) which have further been broken down into its component parts of identity proofing, authentication and the ability to communicate authentication and attribute information. Please see Annex 1 for the levels of assurance by component.

It should be noted that different LOAs might be required as based on why the ID is being authenticated. For example, for the financial sector the additional registrations and validations required might require that a higher LOA is achieved to allow access. It provides assurance that the entity claiming a particular identity is the entity to which that identity was assigned.

Authorization

Authorization takes place after an individual's claim of identity is authenticated and access rights of a 'relying party' are defined. These rights of a 'relying party' needs to be associated with the identity aligned to the relationship between the individual and the relying party independent of the identity provider (eg: National Identification Authority). Authorization typically takes place after an individual's claim of identity is authenticated and defines access rights (or grants) that a Relying Party has associated with the identity aligned to the relationship between the individual and the Relying Party (e.g., a financial institution)—independent of the Identity Provider (e.g., the National Identification Authority). In more advanced authorization schemes the access rights are granted in a dynamic fashion.

Identity Management and Maintenance

Identity management or maintenance is the ongoing process of retrieving, updating, and deleting identity attributes or data fields and policies governing users' access to information and services. Identity retrieval involves fetching a user's identity attributes from the specific database in which it is contained. Security policies should be used to enforce access privileges to ensure that only authorized individuals can access, alter, or delete identity information, and to ensure that the actions are audited and cannot be repudiated.

Credentials may be deactivated, revoked, or made dormant as a result of certain events, and identity information may be updated or deleted. Identity Management challenges include how to make system maintenance cost-effective, use data analysis to improve the system's performance (including its efficiency), ensure that databases are updated to reflect major life events (such as birth and death), and maintain privacy and security controls.[128]

While the specific terminology can vary across different organizations and reports, the fundamental processes are important to understand as they apply to different aspects of financial service provision and how identity is used at each step along the way.

ANNEX 3: UNHCR ID SYSTEM

When UNHCR maintains a registration and ID system in a country, this will typically involve issuing refugees and asylum seekers with ID cards and other credentials, such as family or individual certificates, certifying their status and their eligibility to receive certain goods and services. UNHCR seeks to keep entitlement documents (e.g. ration cards) and its refugee ID cards separate in order to distinguish itself from other agencies providing assistance.

UNHCR's registration and case management software (proGres) was introduced in 2003. ProGres was initially designed provide and manage identification services on a national or sub-national basis. Cloud storage for proGres was introduced in 2015. In addition, the Refugee Assistance Information System (RAIS) was established in 2009.[129] RAIS is an Inter-Agency tool for tracking assistance, referrals, and assessment information. It enables UNHCR and partners to share assistance records, cross-check beneficiaries lists, and host different types of data. RAIS is synchronized with proGres, from which refugee data from all UNHCR field offices is updated daily. A data sharing agreement with UNHCR is a prerequisite for accessing RAIS. RAIS assists in enabling reach, creating better coordination mechanisms (since many other organizations are doing the same relief work in similar geographical areas) and ensuring better protection of beneficiaries' personal data. Since June 2014, 150,000 home visits have been recorded on RAIS, and there are over 7 million assistance records corresponding to 1.5 million beneficiaries.[130]

Also in 2015, following successful pilots in Malawi and Thailand, UNHCR introduced its Biometric Identity Management System (BIMS) through which country operations can capture fingerprints, irises and facial photo during registration. UNHCR today maintains a central and searchable database of unique records for all refugees and asylum seekers registered through BIMS around the world (4.4 million across 48 country operations as of February 2018), which allows persons of concern to re-establish or continuously their identity as they travel across borders and encounter different UNHCR country operations.

UNHCR follows standardized registration processes across all its country operations. These processes were designed with recognition that refugees and asylum seekers may not have official identity documents that would enable the verification of their identity claim or that could support an initial needs assessment. Each refugee registered with UNHCR is provided with a unique registration record and is issued with an ID confirming their asylum seeker status. Once refugee status is confirmed, UNHCR may issue a second, updated ID. These UNHCR-issued IDs may be the only that refugees will have access to.

If certain conditions for refugee data protection and identity management are met, UNHCR may give access to the relevant portion of its database to the host state. The data may then be integrated with the host State's national ID or standalone refugee ID system. Such data sharing arrangements can save host states the time and cost associated with repeated data collection and registration and facilitate the provision of government-issued identity documents to refugees and asylum seekers. These are often more widely accepted and allow for greater access to host country services and opportunities.

ANNEX 4: REFUGEE DIGITAL ID CASE STUDIES

Uganda – A Standalone Refugee Registration and ID System

Uganda hosts over 1 million refugees who live in settlements and in and around the community, primarily from South Sudan and DRC. Uganda is a party to the 1951 Refugee Convention and is widely-recognized as one of the most generous host States for refugees in the world. The Government provides freedom of movement, access to services and allocates plots of land for shelter and agricultural production.

In terms of RSD and registration, UNHCR and the Government's Office of the Prime Minister (OPM) carried this out jointly, leveraging UNHCR's proGres software, until 2014 when the OPM introduced its own system, the Refugee Information Management System (RIMS). RIMS is a web-based platform that includes registration, biometric capture, case management and card production modules. Although RIMS captures two fingerprints, it does not operate a biometric deduplication or authentication and is not linked or interoperable with the national ID system- maintained by the National Identification and Registration Agency (NIRA) and covers all nationals and foreign residents. NIRA provides civil registration services to refugees and asylum seekers.

Since assuming responsibility for refugee registration, the Government is in the process of registering[131] over 1 million refugees with RIMS. The refugee ID card and certificates that are issued is widely-recognized and allows access to all services that a non-national is entitled to. In 2017, when the Government made it mandatory for all SIM cards to be linked to a national ID number, the refugee ID number was accepted. Likewise, the refugee ID card is accepted to open a bank account. The refugee ID card enables refugees to access a range of special entitlements for refugees, including discounted education and healthcare. While there have been some challenges with the implementation of RIMS, Uganda's progressive policy and practices with regards to providing IDs to refugees and asylum seekers, and ensuring that these IDs are widely-recognized should be applauded.

Lebanon, Jordan & Egypt

These countries use extensively the RAIS system (articulated in the previous Annex) to monitor and coordinate humanitarian aid. Today, UNHCR and WFP (World Food Program) provide both direct assistance to beneficiaries as well as managing other NGOs operating as direct/indirect system users.

The largest implementation is in Lebanon, where more than one million refugees now use either WFP's smartcard to buy goods at participating retailers, and/or UNHCR-backed ATM cards to withdraw money instead of receiving physical goods. However, there is currently no clear legal and regulatory framework for e-money transactions.

In Egypt, WFP has adopted the store card of the supermarket Carrefour as a delivery mechanism. In Jordan, branches of Cairo Amman Bank, refugees are able to withdraw their cash entitlement from UNHCR by placing their eye against an IrisGuard scanner – no card required. The success of this program has encouraged WFP to pilot use of iris recognition technology to allow refugees to purchase food in participating supermarkets.

ANNEX 5: COUNTRY CASE STUDIES

(adapted from country submissions)

Canada

Introduction

Digital ID and financial inclusion has progressed through a variety of Digital ID programs based on a national framework that had evolved over the years. In 2014, the Digital ID & Authentication Council of Canada was launched as a public-private effort, and in 2016, the Pan-Canadian Trust Framework (PCTF) Overview was published enabling the public and private sector to work collaboratively to safeguard digital identities by standardizing processes and procedures. In 2017, as part of the Pan-Canadian Trust Framework Components, the DIACC (The Digital ID & Authentication Council of Canada) and IMSC (Identity Management Steering Committee) collaborated to develop conformance standards criteria for trust framework components.

Based on the national framework, a set of Digital ID programs were created as pilot projects. These include British Columbians (B.C) ‘Service cards’ which is used for connecting provincial services and Alberta’s ‘My Alberta Digital ID program which is used for digital identity purposes in the state of Alberta. In the latter half of 2018, SecureKey’s‘Verified.me’ will be launched to provide secure and privacy respecting authentication and attribute validations across Canada. In addition, the Government of Canada’s own cyber authentication solution and immigration frameworks mapping trust frameworks has been developed to assist users of these Digital ID’s. There is an attempt being made to unify all the pilot projects into a unified Canadian Digital ID ecosystem and this would enable greater integration of the various Digital ID projects that have been created.

Applications

B.C. Services Card

The B.C. Services Card is a security-enhanced photo ID developed by three provincial government organizations — the Ministry of Technology, Innovation, and Citizens’ Services (MTIC), the Ministry of Health, and the Insurance Corporation of British Columbia (ICBC). It replaces the aging CareCard (an unique ID card used for health care services), can be combined into a single card with a driver’s license, and, like many new credit cards, is a ‘chip card’ — meaning it is embedded with an encrypted chip that can connect to secure and inexpensive chip card readers. These card readers can be set up at government service counters and also connected to a personal computer at home. This chip and the digital identity management system open up the possibility of reliable and secure online access to more government services.

My Alberta Digital ID

The My Alberta Digital ID program provides an Alberta resident with a personal online identity that securely accesses multiple Government of Alberta online products and services. My Alberta Digital ID uniquely identifies an individual online, much like a driver’s license or identity card works in person-to-person interactions. The Government of Alberta ensures that sufficient information is obtained to properly identify an individual to differentiate from others that have the same or similar names. This ensures the correct services are provided to the correct person.

Government of Canada Cyber Authentication Solution

The Government of Canada Cyber Authentication Solution provides end-users. A mandatory cyber authentication service that enables Canadians and the general public to securely sign-on to Government of Canada online services. The solution is a standards-based, anonymous user sign-in solution, available through GCKey, a government-branded service, and a '*Credential Broker Service*'[132] that enables users to authenticate with their online banking credential.

Verified.me

In the latter half of 2018, SecureKey's Verified.me, a competitive and interoperable ecosystem for financial inclusion, is expected to launch. Verified.me leverages capabilities of Canada's financial institutions and participating provinces to provide secure and privacy respecting authentication and attribute validation. Furthermore Canada's payments network, Interac indicates their intent to launch an interoperable digital identity service in the near future. The Interac model will issue and leverage a secured record of identity with a tokenized credential.

Immigration Services

There is work underway between countries US, Canada and the UK to map their respective trust frameworks, and develop a cross-border mutual recognition process. This also extends to other services including security and transparency mechanisms for the Digital ID setup.

India

The Indian government has undertaken reforms to increase financial inclusion through the JAM Trinity, an enabling ecosystem integrating Unique Digital IDs (Aadhaar), Bank Accounts (Jan Dhan) and Mobile through various cost effective digital payments systems such as United Payment Interface (UPI), Bharat Interface for Money (BHIM), and Aadhaar Enabled Payment Systems (AEPS).

'Aadhaar', a free 12-digit number issued by the Indian government to all residents of India, was issued by the UIDAI (Unique Identification Authority of India) with the objective of being (a) robust enough to eliminate duplicate and fake identities and (b) able to be verified and authenticated in a simple cost-effective way.

The technology uses demographic information (i.e. name, address, date of birth, gender, telephone number and email address) along with biometric data collected through the use of fingerprint scanners, iris scanners, and cameras – for face recognition, allowing for instantaneous identity authentication. So far, almost 1.20 billion Aadhaar Numbers have been generated, 339 million Aadhaar have been linked with bank accounts, and over 1.7 billion authentications have been done through Aadhaar in last 3 years. Total digital transactions have reached 17.57 billion in FY 2017-18, which is nearly 70 percent more than the digital transactions in FY 2016-17 (10.76 billion).[133]

Applications

Integration of Digital ID with e-KYC (Electronic KYC) Service

Digital onboarding through JAM is fast, reduces transaction costs for the customer and facilitates a near instant opening of account. The Aadhaar system has been integrated with an electronic KYC (e-KYC) service to expedite the verification of a client's identity. The e-KYC enables an individual with an Aadhaar number to allow UIDAI to disclose his/her personal information to service providers who wish to instantly activate services such as mobile connections, bank accounts, etc. The e-KYC is paperless, consent-based and private, non-repudiable and instantaneous. As a result, accurate and reliable CDD data is shared with the reporting entity in real time. As the CDD data is released directly to service providers only upon the consent of the customer, his/her privacy remains protected. So far, a total of 4.9 billion e-KYC transactions have been done through Aadhaar. Banks and payment network operators have embedded Aadhaar authentication into micro-ATMs to provide branch-less banking anywhere in the country in a real-time, scalable and interoperable manner.

Seamless Integration with Other Financial Services

The Central KYC Records Registry (CKYCR) is envisaged as a repository of the KYC records obtained by the Regulated Entities (REs) across the financial sector. This database enables inter-usability of the KYC records with a goal of reducing KYC documents and its subsequent verification processes for a new financial entity.[134]

Mobile Payments

One of the building blocks of the payments ecosystem in India, Unified Payments Interface (UPI) powers multiple bank accounts into a single mobile application (of any participating bank), merging several banking features, seamless fund routing and merchant payments under one umbrella. Based on UPI, the

Government of India has introduced Bharat Interface for Money (BHIM) application which allows users to directly perform payment transfers to other users or merchants with an easy to use interface. BHIM has been downloaded 23.8 million times since its launch in December 2016. Till 31st January 2018, the number of transactions on BHIM-UPI platform (BHIM and BHIM UPI family Apps) has reached USD 1.12 Billion (by Value) and 580 Million (By Volume).

Facilitating Government-to-Person Transfers

The introduction of Aadhaar Enabled Payment System (AEPS) has facilitated disbursements of entitlements (like wages under Mahatma Gandhi National Rural Employment Guarantee Scheme, Social Security Pension, Old Age Pension etc) of Central or State Government bodies using Aadhaar based authentication. During FY 2017-18, a total of around 1.62 billion transactions amounting to INR 1612.05 billion have been carried out through the Direct Benefit Transfer (DBT) scheme.

Mexico

Introduction

Recent regulatory adjustments in Mexico are contributing to address important challenges to financial inclusion such as limited availability of points of access to financial services, lack of required documents, lack of trust in the financial system. These regulatory adjustments have exploited the country's existing identification infrastructure to ease the onboarding and identification process for the provision of financial services and improve fraud detection.

In Mexico, when individuals are born, they are registered in State Civil Registries, and the National Population Registry (RENAPO, for its acronym in Spanish) generates a unique key[135] (CURP) which serves as a foundational ID used for essential functions such as voting, social security programs, and public healthcare services. Although this information is digitized, it lacks biometric information. As part of the registration process to perform such activities, several government agencies offer functional IDs based on the above mentioned foundational IDs, which are legal, unique, mostly digital, and biometric.[136] The most commonly used is the *Voting Card*, available to Mexicans 18 years old and above, which requires a birth certificate, proof of address, and a picture ID.[137] INE (Insituto National Electoral—the agency for conducting elections) contacts RENAPO to get individuals' CURP, adds it to its database. It then collects applicants' biometric information, such as fingerprints and picture, and issues the Voting Card.[138] By mid-2017 (biometric registration started in 2001), the electoral registry had data on about 95 percent of the voting-age population.

Low-income individuals may lack all the standard required documents to satisfy CDD and AML/CFT requirements to open an account or to obtain a loan. In order to address this concern, a proportional regulatory approach for deposits accounts was developed. Risk-tiered accounts were created in 2009 and were divided into four levels in 2011. Higher-level accounts allow higher levels of monthly deposits and higher balances,[139] more access devices, and more operations that are available.[140] In turn, these prescribe increasing opening requirements. Level 1 accounts are anonymous and need no documentation or interview to be opened. Level 2 accounts require applicants to provide personal data[141] and show a valid ID.[142] The opening process for level 2 accounts may be carried out face-to-face at a bank branch, face-to-face through an agent authorized by the bank, or remotely, through a digital device.[143] Relative to level 2 accounts, level 3 and level 4 accounts require additional data[144] and, for level 4 accounts, photocopies of some documents.[145]

Applications

Worried about fraud and identity theft, some banks have begun collecting biometric information. In 2017, with the goal of curbing identity theft by taking advantage of technology, regulatory adjustments to the identification process undertaken by banks were introduced.[146] These consider two moments when clients must be identified: when signing on products (see Table 1), and when performing transactions at a bank's branch (see Table 2).[147] In both cases, the main innovation is to require financial institutions to collect and verify biometrics in some cases (without the need to store them), improving access by using remote channels,[148] and enhancing security. Regardless of the ID presented, the institution needs to validate that the information they collect, including the CURP, matches RENAPO's records.

Instead of verifying identity with INE, banks may create a database with their customers' fingerprints and use these to identify them in the future. To do so, banks previously need to register the fingerprints of all their employees and their managers and, when registering the fingerprints of each customer, they need to validate the client's identity with INE (fingerprint matching).

The regulatory adjustments expand onboarding access, since some higher-level accounts and some loans can now be obtained remotely. The adjustments reduce the risk

Table 4: Identification When Signing on Products (Accounts, Loans and Transactions)

Signing on Method			
		Face-to-Face	**Remote**
Accounts	**Level 1**	No biometrics.	Not allowed.
	Level 2		No biometrics. No video-call interview. CURP verified against RENAPO's records.
	Level 3	Biometrics (**fingerprint**) are verified with INE's registries only when the ID presented is the Voting Card.[149] CURP verified against RENAPO's records.	Biometrics (**face-recognition**) are verified through video call. The only accepted ID is the Voting Card.
	Level 4		
Loans	**0 – 60,000 UDIS**		
	60,000 UDIS or more		Not allowed.
Transactions (Cash withdrawals &Transfers[150])	**<1,500 UDIS**	No biometrics, a valid picture is required.	Not allowed.
	1,500 – 2,800 UDIS	Biometrics (fingerprint) are verified with INE when the ID presented is the Voting Card.[151] If clients present a debit/credit card that includes a chip and enter their Personal Identification Number[152] and any valid ID, there is no need to verify biometrics.	Not allowed.
	>2,800 UDIS	Biometrics (fingerprint) are verified with INE when the ID presented is the Voting Card. If clients do not present their Voting Card, they can show other 2 IDs and banks need to verify that their underlying data matches. The bank's branch manager needs to authorize the transaction.	Not allowed.

that a fake customer's ID is accepted, preventing fraud, since institutions are required to verify that the provided data is consistent with RENAPO's registries and that the Voting Card's underlying data matches INE's.[153] The risk of identity theft is also reduced, because when individuals present Voting Cards as a means of identification, it is checked that their biometric information matches INE's records. Mitigating fraud and identity theft risks has the potential to enhance population's trust in financial institutions and lower provision costs, thereby increasing demand and supply of financial services.

Despite these benefits, there are important areas of opportunity. First, biometric verification is not carried out when individuals present IDs other than the Voting Card at bank branches. Extending biometric identification mechanisms to other functional IDs has the potential to further curb identity theft and fraud. Moreover, if biometric data were linked to the foundational IDs, it would be possible to substitute current ID requirements linked to functional IDs and, more importantly, individuals lacking functional IDs would be able to apply for financial products.

A related challenge concerns the collection of the underlying biometric information. Currently, some public and private institutions, including banks, are engaged in gathering different types of biometric information. In August 2018, when the discussed regulatory changes become effective, all financial institutions will be forced to verify biometric information. In doing so, they may wish to store it. One possible course of action is to integrate biometric information collected and stored by public and private institutions into a centralized database, and that this database is used to validate individuals' identity and to grant them with a recognized digital ID.

Nigeria

Introduction

The cornerstone of the digital identification initiative in Nigeria, a country with a population of nearly 187 million people,[154] is the National Identity Management Commission (NIMS), the parent organization of the National Identification Number (NIN): The NIN is a set of numbers assigned to an individual upon successful enrolment. Every citizen or legal resident above the age of 16 is eligible to enroll for the National Identification Number (NIN). Enrolment consists of the recording of an individual's demographic data and capture of ten (10) fingerprints, head-to-shoulder facial picture and a digital signature, which are all used to cross-check existing data in the National Identity Database to confirm that there is no previous entry of the same data. Uses of the NIN number include obtaining a National e-ID (electronic ID) card, obtaining a passport, opening personal bank accounts, obtaining a driver's license, obtaining a Permanent Voters' Card, participating in the National Health Insurance Scheme and paying taxes.

Applications

National e-ID Card

The biometric general multi-purpose e-ID card can be used to authenticate an individual's identity across several public and private services. The card was developed in liaison with MasterCard, with Prepaid MasterCard functionality included in the e-ID. The primary ID number and infrastructure used for the national e-ID card is the NIN. Following the launch of the NIN registration in 2014, about 15 percent of the adult population (14,491,000) has been registered for a NIN; however, only 3-4 percent of the population has been issued an e-ID card. Challenges pertaining to lack of enrollment include lack of rural identification centers and an inequitable regulatory system.

BVN: The BVN (Bank Verification Number) service, operated by the Nigeria Inter-Bank Settlement System (NIBSS), provides a unique identifier for each citizen that allows them to be identified, authenticated, and linked to existing accounts and financial products by any Nigerian bank. Besides serving as the national ID authenticator,[155] the NIN platform provides foundationalsupport enabling the development of BVN numbers across Nigeria. The stated objective of BVN is to provide a uniform industrially accepted unique identity for bank customers, enabling customer identification and transaction authentication without the use of cards, using only biometric features and PIN.

Harmonization & Integration Using NIN

There are initiatives to integrate the NIN, e-ID and BVN to achieve the harmonization objective and facilitate e-government and public-sector applications. The NIN presents the core infrastructure and framework upon which harmonization would operate, as most common factor to all stakeholders in the harmonization platform is the requirement of a 'proven identity'. The NIN infrastructure serves as the platform in which identity management sub-systems and applications as components are coordinated.

The NIMS, which is designed to provide a unique identity for all individuals as well as a national identity database and authentication/verification infrastructure, will be central to the harmonization process. In the future, there could be a universal ID (like SSN in the USA) integration which could facilitate opportunities for data exchange and efficiencies by re-using existing data in each system.

Regulatory and Legal Framework

Data Protection

Nigeria has no comprehensive data protection law and no independent data protection authority. Two separate Bills have been pending since 2008 and 2010. In 2013, The National Information Technology Development Agency Draft Guidelines on Data Protection, known as "the Guidelines". Additionally, while there has been integration of the NIN with other services including transit, immigration, and police, there appears to be insufficient separation between services to ensure privacy.

Norway

Introduction

Digital ID in Norway is based on the National Population Register's identification system, managed by the Norwegian Tax Administration. All Norwegian residents are issued with a personal identification number which becomes their personal identifier for life. This personal identification number can be linked to e-ID to provide individuals with access to numerous digital services such as online banking and public services.

In 2004, the BankID solution was developed through cooperation by Norwegian banks. The BankID solution fulfills the highest level of security requirements and can be used for accessing both private and public sector services. eID was established through private and public sector cooperation; eID solutions used within the Norwegian public sector are mainly supplied by private developers. These privately developed eID solutions are integrated within the public sectors' ID-portal (ID-porten), and the use of such solutions has been secured through a national public procurement agreement.

Applications

The Norwegian ID-portal

In 2017, the Norwegian ID-portal was used more than 11,415 million times and provided access to more than 1500 public services. The portal can be used by anyone with a national identifier issued by the Norwegian Tax Administration, including citizens, foreign residents and persons working temporarily in Norway.

The ID-portal can be used by central, regional and local government agencies to provide access to public services online. It simplifies public agencies' use of eID by providing technical solutions and a common procurement agreement. It provides a single sign-on universe which simplifies the development of digital services that span different agencies and sectors. In terms of security, the ID-portal protects and prevents the user's public service log-in history from being transferred to private eID developers. Only the ID-portal and user know which public service a user has chosen to access.

The ID-portal supports public services from all sectors, including health, inland revenue, government to business, education and municipal sectors. Since the portal supports the recognition of eID at the highest level of security, access to all services can be provided and protected.

eID in the Financial Sector

BankID, supported by eID, is used on average by each Norwegian 160 times per year and scores well (80-90 percent) when it comes to user satisfaction, user-friendliness, safety and ease of use among its 3.8 million users. BankID provides access to a large range of services relating to the financial sector. Access to internet banking and the digital signing of financial documents are services most commonly used by customers. A customer can open a new bank account online without having to go to the bank in person or provide paper documentation. BankID supports Norwegian anti-money laundering regulation and is an important tool for the digitisation of the Norwegian banking sector.

Public Sector eID Solutions

In addition to the ID-portal, other eID alliances operate within the Norwegian public sector. *Feide* is an eID solution used by the Norwegian education sector. This eID solution provides access to educational resources that require a lower level of security than those protected by the ID-portal. The Feide solution allows access to services across primary and secondary schools, as well as higher education institutions. Within the health sector, an eID solution provided by private developers is used by health personnel for authentication and authorization purposes.

Pakistan

Introduction

NADRA (National Database and Regulation Authority) is one of the earliest developing country ID agencies to use biometrics to ensure unique ID numbers for its citizens. With estimated coverage of the adult population at 207 million people,[156] almost 99 percent, the National ID Card has become the dominant form of identification for most transactions. NADRA has worked closely with the Benazir Income Support Program (BISP) [157] to ensure robust identification of the beneficiaries of the country's largest cash transfer program and has implemented an e-payments system linked to this robust form of identification.

The Computerized National Identity Card (CNIC), a unique 13-digit number applicable to every Pakistani citizen above 13 years of age, is the core product of NADRA.[158] The CNIC, with its enhanced security features, is specifically used for opening accounts and receiving remittances, in different government programs such as voting and social welfare and in the private sector for verification purpose.

While digital ID services have become widespread, there is concern about the ID services offered, specifically for the private sector. While the account opening costs are estimated to vary from PKR 15 to PKR 45,[159] the transaction based costs are estimated to range from Rs 2 to Rs 6 per transaction depending on the number of total transaction. These are subsidized for government entities with large discreet discounts. While the concept of 'value pricing' is known in the private sector, the lack of transparency and fairness in pricing across the public and private sectors remains an issue.

Applications

Branchless Banking

Digital ID has played an integral role in the growth of branchless banking by enabling banks to offer specialized types of accounts that can be accessed through mobile phones using mobile technologies for initiating Person-to-Person (P2P) remittances, bill payments and payments for retail purchases, as well as cash withdrawal and cash deposit through mobile banking agents.[160] A total of 8 banks, including micro-finance banks, offer mobile money accounts and collectively operate 402,710 agents (as of January 2018[161]). NADRAs can also be used to open level 0 accounts, accounts with the lowest transaction limits, through validation of basic biometric information linked to a CNIC through branchless banking systems.[162]

SIM Verification

Based on NADRA's Digital ID, the PTA (Pakistan Telecom Authority) and MoIT (Ministry of Information Technology) collaborated to introduce a SIM registration system called Biometric Verification Systems (BVS) program, which made it mandatory for all cell phone owners to register each new SIM and have their identity biometrically verified against the NADRA database before activation of SIMs.[163] The customer's CNIC is linked with several SIMs (up to 5),[164] and a limit placed on each person obtaining SIMs. An important factor that has led to the success of the BVS rollout is the extensive and dense agent network throughout the country, which was originally developed for the branchless banking system.[165] The unique 'Over the counter' (OTC) methodology allowed agents to connect with customers at low cost.[166]

Accelerating G2P Payments

The CNIC has been central to promoting the growth and digitization of G2P payments, organized into three categories: (a) social cash transfers, (b) government salaries and (c) government pensions. One of the important attributes of CNIC is that it ensures personal presence of the beneficiary at the time of withdrawal of money contrary to the existing system where the beneficiary himself/herself is not self- recipient of money in majority of cases. The beneficiary does not require high level of financial literacy for withdrawal of money as required for usage of debit card, and the CNIC simplifies security tiers of withdrawal.[167,168]

Credit Reporting Systems Development

In the credit information space, the Electronic Credit Information Bureau (eCIB)[169] has facilitated each CNIC having credit information linked using the NADRA online verification and authentication process. For corporate credit reports, each corporate entity (listed and unlisted) is mapped to a unique borrower code derived from the CNIC system, and financial institutions are required to report all financial obligations under this unique borrower code. In addition to the ECIB, more traditional credit reporting on banked customers, Microfinance Credit Information Bureau (MF-CIB)'s microfinance institutions can access the ECIB data. The common link between all credit reporting systems, banks, and MFIs is the CNIC.

NADRA E-Sahulat and International Remittances

E-Sahulat, launched in 2008 as part of NADRA's electronic commerce platform drive in 2005[170] is a CNIC enabled low-cost e-services collection and disbursement platform consisting of over 12 thousand active franchisees and a switch connecting with telecoms and banks processing an average of 7.5 million transactions a month. All the three stages of the E-Sahulat process (site survey, verification and enrollment) involves mapping with the CNIC Digital ID system. The E-Sahulat interface plays a significant role in expanding domestic and international remittances, especially due to its more than 8000 plus touch points serving low socioeconomic status customers.[171]

Regulatory and Legal Framework

Legal Measures to Enable Data Protection

Pakistan has no independent data protection authority or data protection law, although a draft Electronic Data Protection Act was introduced in parliament in 2005 focusing on personal and sensitive data. There has been a sustained effort by policymakers and social think tanks to enact a new law, and it is expected that new legislation will be passed soon.[172]

Branchless Banking Regulations Incorporating Digital ID

'Branchless banking' regulations which were introduced in 2007 and updated in 2016[173] and are applicable to all banks including Islamic and microfinance banks, lay out regulations for the technology architecture of the CNIC/NADRA Digital ID ecosystem and minimum standards for data and network security along with consumer protection and risk management. There is an emphasis on risk based CDD processes. In addition, a risk management program to FIs shall put in place risk based information/data security requirements as well as channels like mobile phones, SMS, USSD, mobile applications (3G or 4G) etc.

Peru

Introduction

The National Registry of Identification and Civil Status (*Registro Nacional de Identificación y Estado Civil*, or RENIEC in Spanish) is the premier national ID system in Peru, a country with a population that is in excess of 31 million[174] with the fifth largest economy in GDP.[175] The RENIEC is an autonomous constitutional body of the State of Peru that is charged with maintaining records of major events such as births, marriages, divorces and deaths in the country in addition to information regarding voter eligibility and registration along with the issuance of the national identity card.

The national identity card comes in two types: the traditional non-smart DNI (Documento Nacional de Identidad card), and the relatively new smartcard-based electronic ID (DNIe) with biometric identification. To date, 99.9 percent of citizens have DNI and there are plans to aggressively scale up the DNIe in the years ahead RENIEC has a budget of US $130 million, and it is estimated that about 45 percent of this comes through revenues generated through fees generated through the ID program. Currently the DNIe card is a standard contact smart card, and citizens must pay US$10 for it. Banks, mobile operators and other service providers/relying parties pay a transaction fee for online verification to RENIEC – between US$0.30 and US$1 depending on the service requested.

Applications

Mobile Connect

The RENIEC Digital ID serves as the foundation for enabling authentication in the Mobile Connect platform, the customer authentication mechanism for the mobile environment including access to websites and apps. The international telecom trade body GSMA launched Mobile Connect in Peru with Movistar, who went live with the service in June 2016. Movistar is reported[176] to have a 54 percent share of the telecom market; estimated at around 8.5 million subscribers. Mobile Connect's service is currently being absorbed by the participating mobile operator (Movistar), with the support of the GSMA. It is expected that this will change once usage of the service becomes more commonplace.

Modelo Peru (e-money Platform), PDP & BIM

The Peruvian Bankers' Association (ASBANC) announced an initiative to develop and offer a shared e-money platform in 2014 with RENEIC Digital ID as its core database. Named *Modelo Peru*, the initiative quickly grew into a collaboration between the country's government, financial institutions, telecommunications companies, large payers (salaries) and payees (billers) as part of Peruvian Digital Payments (PDP). PDP is co-owned by the Association of Banks of Peru (ASBANC) as well as many of its member banks and electronic money issuers and developed the shared infrastructure for the mobile money service.[177] Known as Billetera Movil (BiM), the new service, which provides services such as cash in/cash out at agent points, balance check, P2P payments, and airtime top-up, was launched in February 2016, and reached around 80,000 subscribers in its first three months of operation. According to the GSMA,[178] 95 percent of the population of Peru lives in an area with mobile broadband coverage, and around 70 percent of the population has a mobile phone connection.

Some key challenges of Modelo Peru include expanding the potential of the agent network and mobile money in inaccessible areas. Issues of training and knowledge transfer can be reduced through hybrid and technological approaches. Reaching remote rural communities through mobile networks is a challenge which cannot always be left to mobile operators; government investment may play a critical role in expansion in areas with difficult geography.

Regulatory Protection

Peru has both comprehensive data protection legislation[179] and an independent data protection authority.[180] Under this legislation:

- Personal data includes any information on an individual which identifies or makes him identifiable through means that may be reasonably used.
- Sensitive data includes biometric data, data concerning the racial and ethnic origin, political, religion, philosophical or moral opinions or convictions, personal habits, union membership and information related to health or sexual life.

The inclusion of biometric data in 'sensitive data' has implications for ID systems by requiring consent given through a handwritten signature, digital signature or other authentication mechanism that guarantees unequivocal consent by the owner.[181] It is unclear how these restrictions would apply to biometrics delivered via a mobile device such as Apple's TouchID.

United Kingdom

Introduction

The UK national eID scheme, GOV.UK Verify, has been live since May 2016 and currently has over 2.2 million users with a verified identity. There are currently 17 public sector services that are utilizing these identities to allow citizens to access digital services ranging from taxation and pension transactions to benefits, driver licensing, and redundancy claims. The program is currently being expanded to various health and social services as well as the private sector.

GOV.UK Verify is a federated identity system managed by the UK Government Cabinet Office. The trust framework within which providers and services operate follows rules defined by the UK Government such as its well known identity proofing, verification and authentication standards,[182] all of which are openly available. Identity proofing, verification and authentication are all provided by a group of commercial organisations certified to operate against UK standards and subject to commercial contracts derived from a Cabinet Office procurement framework for identity assurance. Currently 7 providers are certified to operate under this framework and provide identity accounts to citizens.

Applications

Interoperability with the Private Sector

The UK government is engaging with the financial sector, where changes to legislation and disruptive technologies are driving the need to better understand the identity of online users, to expand digital ID. The government is currently removing commercial and policy barriers to interoperabilitywhere they exist whilst continuing to publish standards for digital identity that support the needs of users and services alike.

International Interoperability

The UK government views international interoperability of eID as a key driver for the growth of digital economies around the world. The key is to provide interoperability frameworks to enable the recognition and reuse of identity from multiple trusted sources based on international standards. To ensure interoperability and trust frameworks, the UK has engaged (at various levels) with international organisations such as the UN (UNCITRAL), the World Bank, and the European Union, where these frameworks are being considered.

Trusted Attribute Services

Trusted Attribute Services provide data about individuals or entities (Attributes) where a link can be established between the identity and the data at some level of assurance, Attribute data combined with verified identity satisfies many of the needs of digital services and citizens accessing services by providing much needed trust when determining eligibility, and also enables the creation of efficient digital services. GOV.UK Verify currently only utilises attribute data to satisfy the need for identity matching at a relying party. In this case, attributes are provided as part of an identity assertion from the Identity Provider as MDS (Minimum Data Set). The UK government intends to widen this capability enabling verified identity to release further attribute provision.

ENDNOTES

1. Adapted from NIST (2013a)
2. Adapted from OWI (2017), NIST (2013a), World Bank 2016.
3. Adapted from NIST (2013b)
4. Adapted from World Bank (2018a)
5. Adapted from Distributed Ledger Technology (DLT) and Blockchain, Fintech Note 1, WBG 2018.
6. Adapted from World Bank (2016, 2018b)
7. Adapted from World Bank (2018b)
8. Adapted from World Bank (2018b), EC (2017), IDB (2013)
9. Adapted from World Bank (2018a, 2018b), Gelb & Clark (2013)].
10. World Bank (2017, 2018b)
11. NIST Glossary: Identifiers
12. As defined by ISO 17442 here: https://www.leiroc.org/
13. World Bank 2017 (Pending HLAC/UN discussions)
14. Richard Kissel (May 2013). Glossary of Key Information Security Terms. NIST Retrieved from: http://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf
15. NIST Glossary: Relying Party
16. NIST Glossary: Revocation
17. Sovrin: A Protocol and Token for Self-Sovereign Identity and Decentralized Trust
18. NIST Glossary: Verification
19. Transaction account refers to any type of account maintained with a bank or licensed non-banking entity that enables making and receiving payments and saving balances – (i.e.) serve as a store of value. References to account in this document should be read as transaction account.
20. World Bank (2017). Identification for Development.
21. G20 High-Level Principles for Digital Financial Inclusion
22. Principles on Identification for Sustainable Development
23. http://pubdocs.worldbank.org/en/205641443451046211/ID4D-IntegrationAproachStudyComplete.pdf
24. http://www.fatf-gafi.org/
25. Ten Principles on Identification for Sustainable development
26. 2017 Global FinDex Report
27. A transaction account is defined as a basic bank account with a financial institution which allows for the efficient transfer of funds by the account holder to third parties as well as receiving electronic payments into this account.
28. UFA2020 Overview: Universal Financial Access by 2020
29. http://globalfindex.worldbank.org/
30. World Bank (2017). Identification for Development.
31. Digital Identity: Towards Shared Principles for Public and Private Sector Cooperation
32. Digital Identity: Towards Shared Principles for Public and Private Sector Cooperation

33. UN-WB working paper: DISCUSSION PAPER: Working Definition of Proof of Legal Identity, May 2018
34. 'Are Biometric ID Systems Good for Women?', Alan Gleb, 2016
35. Digital Financial Inclusion: Emerging Policy Approaches
36. ID4D is a multi-sectoral and cross-practice initiative that unites teams from around the WBG. To enable access to services and rights the initiative supports progress towards identification systems using 21st century solutions.
37. Landscape Technology for Digital Identification
38. World Bank ID4D Dataset, 2017
39. Digital Identity: Towards Shared Principles for Public and Private Sector Cooperation
40. Jan Dhan Yojana (JDY) scheme, was launched by the Indian government in August 2014, with the goal to ensure that every household in the country has an account. Everyone with a JDY account is eligible for a RuPay debit card, accident insurance of Rs.100,000 (~USD $150) and life insurance coverage of Rs.30,000 (~USD $45) and is eligible for an overdraft facility upon satisfactory performance of the account.
41. http://www.pmjdy.gov.in/home
42. News Article: Nigeria announces removal of 23,846 ghost workers from government payroll
43. Public sector savings & revenue from identification systems: Opportunities & Constraints', WBG ID4D report, 2018
44. http://www.intellectualventures.com/news/press-releases/global-good-fund-and-element-inc.-to-develop-biometric-identification-techn
45. GDPR Regulation
46. Digital Identity: Towards Shared Principles for Public and Private Sector Cooperation
47. https://cfi-blog.org/2016/02/17/bim-the-first-fully-interoperable-mobile-money-platform-now-live-in-peru/
48. Excerpt provided by the G20 representatives from the Government of India as a case study (attached in the annexures)
49. Consult Hyperion Pakistan Note', 2017
50. Numbers supplied by country
51. https://fidoalliance.org/
52. https://www.bankid.com/en/om-bankid/detta-ar-bankid
53. Regulatory Framework for Bank Verification Number (BVN)
54. https://www.gov.uk/government/publications/introducing-govuk-verify/introducing-govuk-verify
55. http://www.bbc.com/news/uk-politics-41642044
56. Graham Greenleaf, "Global Tables of Data Privacy Laws and Bills (4rd Ed, January 2015)," SSRN Scholarly Paper (Rochester, NY: Social Science Research Network, January 30, 2015), https://papers.ssrn.com/abstract=2603502; Graham Greenleaf, "Global Data Privacy Laws 2015: 109 Countries, with European Laws Now a Minority," SSRN Scholarly Paper (Rochester, NY: Social Science Research Network, January 30, 2015), https://papers.ssrn.com/abstract=2603529.
57. It should be noted there that transparent is used to indicated that the records are public, however, the algorithms behind it are most often opaque.
58. Tobias Young (14 March 2017). Blockchain technology cuts through the hurdles to simplify everyone's lives.
59. Technology Landscape for Digital Identification
60. Technology Landscape for Digital Identification
61. 'Global Findex Survey 2018', WBG, 2018, (http://globalfindex.worldbank.org/)
62. Providers are legally permitted to "rely" on an Aadhaar check to discharge their ID and ID verification obligations
63. Adapted from the case study provided by India membership.
64. Closing the coverage gap: Digital Inclusion in Latin America, 2015, GSMA
65. http://www.w3.org/2001/sw/Europe/events/foaf-galway/papers/fp/token_based_authentication/
66. For further reading on LOAs, see: http://securekey.com/wp-content/uploads/2016/06/ECONOMICS-OF-IDENTITY.pdf
67. One critical element of the standards are that the PIN is encrypted from the time it is entered to the time it is transformed into the reference value of verification. The full standards are available at https://www.pcisecuritystandards.org/

68. http://www.fin24.com/Tech/Companies/fingerprint-authentication-coming-to-sa-bank-cards-20160726?isapp=true
69. The Global National eID Industry Report: 2017 Edition by Acuity Market Intelligence.
70. Mastercard (26 October 2017). Mastercard and Bank of Maldives Introduce Passport Card in Partnership with Maldives Immigration.
71. https://www.zdnet.com/article/estonias-id-card-scrisis-how-e-states-poster-child-got-into-and-out-of-trouble/
72. Introducing Mobile Connect – the new standard in digital authentication.
73. Circular 3/2012, article 17
74. Technology Landscape for Digital Identification
75. World Bank (2016). Digital Identity: Towards shared principles for public and private sector cooperation
76. https://www.techdirt.com/articles/20161011/10075735774/bangladesh-brings-nationwide-digital-identity-cards-linking-biometrics-to-mobile-phone-numbers.shtml
77. Technology Landscape for Digital Identification
78. Soft and Hard Biometrics for the Authentication of Remote People in Front and Side Views: Ghalleb A, Amara N
79. As above
80. https://newsroom.mastercard.com/press-releases/mastercard-zwipe-announce-launch-worlds-first-biometric-contactless-payment-card-integrated-fingerprint-sensor/
81. Smith, S. (29 November 2016). Voice and Facial Recognition to Be Used in Over 600 Million Mobile Devices by 2021.
82. refers to billions of physical devices around the world that are now connected to the internet, collecting and sharing data
83. Badugu, N. (17 May 2017). Biometrics in Internet of Things (IoT) Security. IoT ONE.
84. ‘NPCI FAQ on Aadhar Payment Bridge System’ (APB),2017, (https://www.ucobank.com/pdf/faq-apb.pdf)
85. Singpass,2018, Government of Singapore (https://www.singpass.gov.sg/spauth/login/loginpage?URL=%2F&TAM_OP=login)
86. ‘It’s important no one gets left behind’, The Guardian, 2017, (https://www.theguardian.com/public-leaders-network/2017/may/02/singapore-government-data-strategy-jacqueline-poh)
87. ‘MyInfo access extended to local businesses’, Nov 2017 (http://www.straitstimes.com/singapore/myinfo-access-extended-to-local-businesses)
88. BISP’s innovation in G2P payment systems’, BISP, Government of Pakistan, 2018
89. https://www.nadra.gov.pk/about-us/
90. Financial Inclusion of forcibly displaced Persons (GPFI)

    *These cards were issued initially by UNHCR but Government of Lebanon told UNHCR to stop registering refugees from 2015 onwards.
91. ‘The Role of Financial Services in Humanitarian Crisis’, WBG, Nov 2017, (http://documents.worldbank.org/curated/en/687701493270597254/The-role-of-financial-services-in-humanitarian-crises)
92. Norwegian Refugee Council (2017). Syrian refugees’ right to legal identity: implications for return. https://www.nrc.no/globalassets/pdf/briefing-notes/icla/final-syrian-refugees-civil-documentation-briefing-note-21-12-2016.pdf
93. ‘Approaches to Providing Identification to Refugees and Asylum Seekers’, WBG ID4D Working Paper, 2018-9
94. Other humanitarian agencies, such as WFP and NGOs, may also register refugees and asylum seekers, as beneficiaries of the assistance they provide.
95. ‘Iris scan helps Syrian refugees in Jordan receive UN supplies in ‘blink of eye’, UN news, 2016 (https://news.un.org/en/story/2016/10/542032-iris-scan-helps-syrian-refugees-jordan-receive-un-supplies-blink-eye)
96. https://documents.wfp.org/stellent/groups/public/documents/communications/wfp287655.pdf
97. ‘General Principles of Credit Reporting’, 2011, Financial Stability Board, (http://www.fsb.org/2011/09/cos_110907/)
98. ‘ECIB Website’, State Bank of Pakistan (http://www.sbp.org.pk/ecib/index.htm)
99. WBG Digital ID note on Pakistan 2017

100. Bank-ID website, 2018, (https://www.bankid.no/en/about-us/)
101. ‘Changing ID trends power banking in Norway’, 2015, (https://www.computerweekly.com/news/4500244960/Changing-IT-trends-power-banking-in-Norway)
102. ‘UID Aadhar’ http://udyogaadhaar.gov.in/UA/UAMRegistration.aspx
103. ‘Bangladesh brings nationwide digital identity cards linking biometrics’ https://www.techdirt.com/articles/20161011/10075735774/bangladesh-brings-nationwide-digital-identity-cards-linking-biometrics-to-mobile-phone-numbers.shtml
104. http://siteresources.worldbank.org/EXTFINANCIALSECTOR/Resources/Good_Practices_for_Financial_CP.pdf
105. ‘GPFI report on alternative data transforming SME’s’, GPFI, 2017, (https://www.gpfi.org/publications/gpfi-report-alternative-data-transforming-sme-finance)
106. ‘Digital ID for businesses’, WBG Report, 2017
107. The Role of Digital Identification for Healthcare: The Emerging Use Cases’, Case Studies, 2018
108. https://www.gov.uk/government/publications/introducing-govuk-verify/introducing-govuk-verify
109. http://diacc.ca
110. https://www.gsma.com/identity/mobile-connect
111. https://fidoalliance.org/
112. https://www.bankid.com/en/
113. https://www.bankid.no/en/about-us/
114. Def: to design a framework so that it can still be used in the future, even when technology changes.
115. Principles on Identification for sustainable development: toward the Digital Age
116. Digital Identity: Towards Shared Principles for Public and Private Sector Cooperation
117. http://documents.worldbank.org/curated/en/213581486378184357/Principles-on-identification-for-sustainable-development-toward-the-digital-age
118. At a Crossroads: PersonHood and digital identity in the information society. OECD working paper, 2008.
119. https://pages.nist.gov/800-63-3/sp800-63-3.html
120. Dig and Text below Adapted from the World Bank Report: Technology Landscape for Digital Identification 2018
121. United Nations Department of Social and Economic Affairs (2014). *Principles and Recommendations for a Vital Statistics System, Revision 3*. Retrieved from: https://unstats.un.org/unsd/demographic/standmeth/principles/M19Rev3en.pdf
122. Aadhaarcard.net.in (07 November 2016). *Apply for Aadhaar Card without any Documents*. Retrieved from: https://uidai.gov.in/component/fsf/?view-faq&catid=36
123. National Institute of Standards and Technology, U.S. Department of Commerce (June 2017). *Digital Identity Guidelines: Enrollment and Identity Proofing*. Retrieved from NIST: https://pages.nist.gov/800-63-3/sp800-63a.html
124. European Commission (25 February 2015). *Trust Services and eID*. Retrieved from European Commission: https://ec.europa.eu/ digital-single-market/en/policies/trust-services-and-eidentification
125. http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2014.257.01.0073.01.ENG
126. https://www.iso.org/standard/45138.html
127. https://pages.nist.gov/800-63-3/sp800-63-3.html
128. Technology Landscape for Digital Identification
129. https://reliefweb.int/report/jordan/rais-jordan-mission-assistance-coordination-bulk-upload-trainer-trainer-guide
130. https://reliefweb.int/report/jordan/rais-jordan-mission-assistance-coordination-bulk-upload-trainer-trainer-guide
131. ‘Uganda launches major refugee verification operation’, UNCR, 2018 (http://www.unhcr.org/en-us/news/latest/2018/3/5a9959444/uganda-launches-major-refugee-verification-operation.html)
132. ‘Credential Broker Service’, 2018, Government of Canada
133. ‘India: Case Study on Digital ID’, G20 Digital ID Onboarding paper, Government of India, 2018
134. More details can be obtained in Box 7 in the main text of ‘G20 Digital ID Onboarding Paper’
135. It is composed by a codification derived from an individual’s name, gender, place and date of birth, plus a random number.

136. These functional IDs include Voting Card, Passport, Certificate of Higher Education Studies (college and graduate degrees), Military Service Card, Consular ID (offered by Mexican Consulates as a mean of identification), Senior Citizen's ID, IDs issued by Mexican Social Security Agencies (which mainly provide health care services), driver's license and taxpayer identification number.

137. Individuals without a picture ID need to present two witnesses with valid Voting Cards. Accepted IDs are those currently valid which include a picture of the individual. Such IDs may be not be linked to foundational IDs and thus be more easily falsified.

138. Currently, INE has 100 percent of the 2 index fingerprints and 80 percent of the 10 fingerprints of individuals in the electoral registry. INE started collecting only 2 index fingerprints. It now collects all 10 when individuals obtain their Voting Card, and when they renew it or replace it.

139. Level 1-3 accounts' maximum monthly deposits are, respectively, 750, 3,000, and 10,000 "UDIS" (1 UDI = 0.33 USD). Level 4 accounts have no maximum monthly deposits. Level 1 accounts' maximum balance is 1,000 UDIS.

140. Level 1 accounts cannot be set up for electronic banking. Levels 2-4 accounts may use electronic banking including through mobile devices.

141. Full name, date of birth and address, at a bank or by authorized agent. If the account is opened remotely, the data to register are: full name, gender, place and date of birth, address, CURP, and cellphone number if the account has a linked cellphone.

142. The ID needs to include a picture and signature. No photocopies are collected.

143. If the process is carried out face-to-face, the data is collected through an interview. If it is carried out remotely, the corresponding individual's information needs to be verified against RENAPO's records.

144. Country of birth, nationality, occupation, taxpayer ID number, telephone number, e-mail and serial number of the electronic signature (if the client has it).

145. Level 3 accounts require the client showing a valid ID with picture and signature. Level 4 accounts require photocopies of a valid ID with picture and signature, CURP, and proof of address.

146. Since 2008, Mexican regulation has foreseen that banks may use biometric data to identify their clients when performing some transactions through banking agents and through electronic banking. Banks were then allowed to use identification mechanisms such as PINs, passwords, tokens or the use of debit or credit cards with a chip. In addition, biometric information from the Voting Card did not need to be verified with INE.

147. The main regulatory changes are included in articles 51 Bis to 51 Bis 12 and Annex 71 of the "Circular Única de Bancos".

148. Only levels 3 and 4 accounts (level 4 with maximum monthly deposits of 30,000 UDIs) and loans under 60,000 UDIs can be obtained remotely through a video-call interview, in which biometric information is collected.

149. If the client does not have a Voting Card, she can show her passport and any of the IDs that allow complying with AML rules and the bank needs to verify that the data is consistent across these two. These IDs include consular registration card, professional identification card, the national military service record, the military ID, the National Institute of Senior Citizens' ID, the Mexican Social Security Institute's ID, driving license, and any ID issued by a Federal, State or Municipal Authority. If INE cannot issue Voting Cards, due to restrictions derived from the electoral calendar, the client has to show any 2 of the above-mentioned IDs, and the operation requires authorization from the bank's branch manager.

150. Money transfers to other accounts owned by the client in the same bank are exempted from identification actions.

151. If the client does not have a Voting Card, she can show 2 IDs that allow to comply with AML Rules and the bank has to verify that the underlying data across these matches. These include the IDs mentioned above and passport.

152. The bank must validate a client's identity with INE (fingerprint match) when the client is given her card and when the client sets the Personal Identification Number for the first time.

153. In the case of immigration documents showed by foreigners and passports, banks have to identify their security elements.

154. United Nations, World Population Prospects (2016) https://esa.un.org/unpd/wpp/DataQuery/

155. ‘BVN Biometric’, https://www.firstbanknigeria.com/biometric/, 2017
156. Pakistan Population Census, 2017 (http://www.pbs.gov.pk/content/population-census)
157. ‘5.2 million families receive a monthly transfer of USD15 through BISP’ World Bank Group ID4D 2 Pager, December 2015
158. ‘National Identity Card’, NADRA, 2017, https://www.nadra.gov.pk/identity/identity-CNIC/
159. Rs 15= 0.129 USD and Rs 45= 0.389 USD as per XE conversions (Conversion rate: 1 USD = 115.601 PKR)
160. ‘Technical Note: Payment systems aspects of financial inclusion’, Pakistan, 2014
161. ‘State Bank of Pakistan agents numbers”, December 2017, (https://propakistani.pk/2017/12/05/number-branchless-banking-agents-crosses-400000-pakistan/)
162. ‘State Bank of Pakistan removes barriers to branchless banking’,CGAP, July 2011
163. ‘Biometric Verification Services’, PTA. 2017, (https://www.pta.gov.pk/en/biometric-verification)
164. The biometric linking process is not done for post-paid accounts but these comprise less than 1% of the market (which is almost entirely pre-paid) and other checks are done to prevent fraud and other issues with corporate accounts
165. For example, agents are located so close together that it takes a median of 5 minutes to reach the nearest agent serving the same provider, with Telenor providing one of the broadest reaching networks of over 200K points of service, selling airtime for its GSM business, unlike bank branches, which had limited geographical reach.
166. ‘Agent Network Accelerator—Pakistan Country Report’, Helix Institute of Digital Finance, 2014
167. BISP’s innovation in G2P payment systems’, BISP, Government of Pakistan, 2018
168. ‘BISP’s innovation in G2P payment systems’, BISP, Government of Pakistan, 2018
169. ‘ECIB Website’, State Bank of Pakistan (http://www.sbp.org.pk/ecib/index.htm)
170. ‘NADRA E-Sahulat’, Government of Pakistan, 2018 (https://e-sahulat.nadra.gov.pk/)
171. “HBL Express and NADRA launch branchless banking services’, January 2015, (https://goo.gl/3Nhdv7)
172. ‘Data Protection Law in Pakistan: Policy Recommendations by DRF’, Digital Rights Foundation, October 2017 (https://goo.gl/KaR4st)
173. ‘State Bank of Pakistan Branchless Banking Regulations’, June 2016, (http://www.sbp.org.pk/bprd/2016/C9-Annx-A.pdf)
174. https://esa.un.org/unpd/wpp/Download/Standard/Population/
175. https://www.cia.gov/library/publications/the-world-factbook/geos/pe.html
176. https://www.budde.com.au/Research/Peru-Telecoms-Mobile-Broadband-and-Digital-Media-Statistics-and-Analyses
177. https://cfi-blog.org/2016/02/17/bim-the-first-fully-interoperable-mobile-money-platform-now-live-in-peru/
178. “Connected Society: Digital inclusion in Latin America and the Caribbean”, GSMA, 2016
179. Data Protection law (Ley N° 29733)
180. National Authority for Personal Data Protection
181. Article 14 of Law 29733
182. https://www.gov.uk/government/collections/identity-assurance-enabling-trusted-transactions

G20
ARGENTINA 2018
BUILDING CONSENSUS FOR FAIR
AND SUSTAINABLE DEVELOPMENT

0110100101110011001000000011101000110
0010000000110001001100000101100011010110
0010000000110010101110110011001010111
0110000010110001101101011011001110111
0111001100100000001110100011010000110
0110001001100101011000010111010010111
1100110010000010000000111000000110111110
0000110000010110111001100100000100000000
0000110000010110111001100100000100000000
1010110001101101000000100000001101010010
1110110111101110010011011000110010000

WORLD BANK GROUP

GPFI
Global Partnership
for Financial Inclusion