FIGI
FINANCIAL INCLUSION
GLOBAL INITIATIVE

Digital ID to Enhance Financial Inclusion

A Toolkit for Regulatory Authorities

DECEMBER 2021

WORLD BANK GROUP

ACKNOWLEDGMENTS
This report has been prepared by Fredesvinda Montes and Sharmista Appaya (World Bank) and co-chairs of Financial Inclusion Global Initiative (FIGI) Digital ID Working Group. The authors are grateful to Minita Varghese for her extensive support during the research and drafting and in reaching out to selected study countries. In addition, the authors are also thankful to Marc Hollanders (Bank for International Settlements), Vijay Venkatesen (International Telecommunication Union) Jamie Zimmerman, Christopher Calabia (Bill & Melinda Gates Foundation), Vyjayanti Desai (ID4D World Bank) and Harish Natarajan (World Bank) for their guidance in developing the project concept. The authors are also thankful to Patrick Armstrong (Financial Stability Board), Lauren Night (US Treasury), Shana Krishnan (Financial Action Task Force FATF), Emile Van der Does, James Newman, Minita Varghese and Anna Metz (World Bank) for their review and improvement of the report. The authors also thank colleagues from World Bank's ID4D, Financial Inclusion and Infrastructure and Financial Stability and Integrity teams, for their contributions to this report. Experts from Omidyar Network and Open Identity Exchange, IDnow, GSMA and FIDO Alliance, iSpirit, have also provided valuable comments and inputs in various stages of the project. Finally, we want to thank all the members of the FIGI Digital ID Working group for their participation in the project workshops and bilateral interviews. This Toolkit was funded by the Bill & Melinda Gates Foundation under the FIGI program.

The interpretations, and conclusions expressed in this work belong to the authors and do not necessarily reflect the views or positions of either the World Bank Group, its Board of Executive Directors, and the governments they represent, or the Bill & Melinda Gates Foundation.

FINANCE, COMPETITIVENESS & INNOVATION GLOBAL PRACTICE

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

DISCLAIMER
The Financial Inclusion Global Initiative led in partnership by the World Bank Group (WBG), International Telecommunication Union (ITU), and the Committee on Payments and Market Infrastructures (CPMI), with the support of Bill & Melinda Gates Foundation (BMGF). The FIGI program is a three-year investment funding national implementations in three countries (China, Egypt, and Mexico), supporting topical working groups to tackle 3 sets of outstanding challenges in closing the global financial inclusion gap, and hosting 3 annual symposia to gather the engaged public on topics relevant to the grant and share intermediary learnings from its efforts.

This work has been prepared for the Financial Inclusion Global Initiative by the Digital ID Working Group. The work is a product of the staff of the World Bank with external contributions prepared for the Financial Inclusion Global Initiative. The findings, interpretations, and conclusions expressed in this work do not necessarily reflect the views of the Financial Inclusion Global Initiative partners partners including The World Bank, its Board of Executive Directors, or the governments they represent, or the views of the Committee for Market Payments Infrastructure, International Telecommunications Union, or the Bill & Melinda Gates Foundation.

The World Bank does not guarantee the accuracy of the data included in this work. The boundaries, colors, denominations, and other information shown on any map in this work do not imply any judgment on the part of The World Bank concerning the legal status of any territory or the endorsement or acceptance of such boundaries.

RIGHTS AND PERMISSIONS

Table of Contents

Figures

Tables

Boxes

Digital ID to Enhance Financial Inclusion

A Toolkit for Regulatory Authorities

NOVEMBER 2019[1]

ABSTRACT

The Financial Inclusion Global Initiative was launched by the World Bank Group, the International Telecommunication Union, and the Committee on Payments and Market Infrastructures, with support from the Bill and Melinda Gates Foundation, to advance financial inclusion in developing countries. The Financial Inclusion Global Initiative comprises the Digital ID Working Group; Electronic Payments Acceptance Working Group; and Security, Infrastructure, and Trust Working Group.

The Digital ID Working Group was created to understand and accelerate the use of digital ID to expand access to, and improve the uptake of, financial services. The working group conducted the following tasks: (i) developed guidance to assess and support the quality of ID infrastructure for use in the financial sector; (ii) reviewed existing global digital ID and electronic know-your-customer solutions to understand their potential to bring efficiency, greater usage, and effectiveness to financial products, resulting in a report with findings to support pilots to refine approaches; (iii) studied the emerging regulatory and policy implications that have resulted from the increased capabilities of digital IDs; and (iv) implemented the findings and outputs of working group through the rollout of country pilots. This document builds the knowledge developed and provides a toolkit for regulatory authorities that aims to serve as guidance when evaluating the adoption or current usage of digital ID to identify and verify the credentials of clients of financial services.

Abbreviations

AML/CFT	anti-money-laundering/combating the financing of terrorism
API	application programming interface
CDD	customer due diligence
CPMI	Committee on Payments and Market Infrastructures
FATF	Financial Action Task Force
FSP	financial service provider
IDSP	identity service provider
IOSCO	International Organization of Securities Commissions
KYC	know your customer
MAS	Monetary Authority of Singapore
MNO	mobile network operator

I. Introduction and Background

It is estimated that 1.7 billion adults globally do not have access to formal financial services. While this lack of access is attributed to a wide range of barriers, the ability to prove identity plays a pertinent role. According to the 2017 Global Findex, 26 percent of unbanked people in low-income countries report a lack of ID documentation as one of the primary barriers to accessing services.[1] Identification for Development (ID4D) estimates that one billion people globally do not have an official proof of identity; the largest ID coverage gaps are concentrated in low-income economies and among vulnerable population. Moreover, there are individuals who possess some form of ID documents that are insufficient to access financial services.

Access to financial services enables people to make and receive payments, send money, borrow, save, and invest. Evidence shows that this can help individuals to build resilience against shocks and can create an environment for businesses to thrive. Yet these benefits cannot be realized without a reliable form of customer ID. Digital ID systems use electronic means to assert and prove a person's official identity online (digital) and/or in in-person environments at various assurance levels."[2] The report *Payment Aspects for Financial Inclusion (PAFI)*[3] highlights the importance of achieving long-term and effective adoption of transaction accounts.

Currently, many countries are seeking to increase access to and the usage, efficiency, and affordability of official IDs by leveraging digital technology for the enrollment, verification, and storage of ID information. This is a positive development. However, we cannot automatically assume that digital ID will be used effectively and securely within the financial sector. Financial-sector regulatory authorities will play a relevant role in the adoption of digital ID by financial service providers (FSPs). While seeking broad adoption of digital IDs, authorities should also identify and address arising risks that could affect financial-sector customers, FSPs, and the integrity of the financial sector at large. Therefore, striking the right balance between adopting innovative ID solutions while mitigating risks to financial stability, integrity, and consumer protection is a complex objective that will require research, coordination, and cooperation with private-sector service providers and building trust among the users of digital ID solutions.

1.1 DIGITAL ID AND ELECTRONIC ID VERIFICATION IN THE FINANCIAL SECTOR

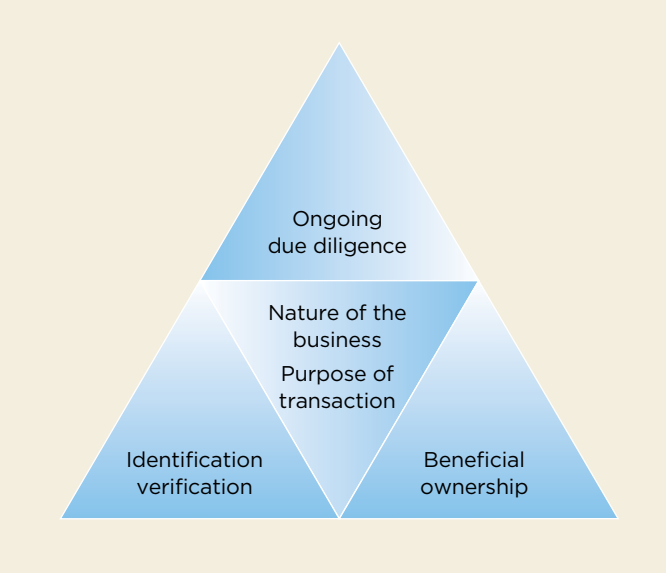
Digital ID plays a role at various stages when using financial services. (1) It makes it easier for the unbanked to open a transaction account that also enables efficient disbursement of social benefits; (2) it enables cost-effective onboarding that can be done remotely by the FSP; and (3) it contributes to the deepening of the financial sector by supporting the take-up of additional products and services.[4] Furthermore, validating a customer's identity using digital IDs allows for a higher degree of assurance than using manual or paper-based processes. In addition, with a digital ID, validating a customer's identity can—in many cases—be completed instantaneously.[5] Some studies have reported digital ID–enabled processes have the potential to reduce customer onboarding costs by up to 90 percent.[6]

During account opening, a customer is required to provide credentials to establish identity so that the FSP can carry out one of the customer due diligence (CDD) dimensions. The term CDD is frequently interchanged with the phrase "know your customer" (KYC), although CDD entails more requirements than just identifying the customer—or the one that on a legitimate basis acts on the customer's behalf—and verifying such identification. The burden of compliance with anti-money-laundering/combating the financing of terrorism (AML/CFT) standards remains a financial-inclusion pain point[7] due to the need for formal or officially recognized proof of identification. This is particularly evident when evident in the context of government cash-transfer programs, where electronic disbursement to transaction accounts, as opposed to cash payouts, offers an important tool to increase financial inclusion, as in many cases recipients do not make use of the store-of-value and electronic-payment functions made available to them. Similar behavior is observed with mobile-money solutions, where beneficiaries tend to withdraw the full amount of funds shortly after receiving it.

As shown in figure 2, Recommendation 10 from the Financial Action Task Force (FATF) entails four dimensions: (i) identifying the customer and verifying the customer's identity, (ii) identifying the beneficial owner, (iii) understanding the purpose and nature of the business relationship, and (iv) conducting ongoing due diligence on the business relationship, ensuring consistency of risk profile, source of funds, and knowledge of the customer by the financial institution. (See appendix A for the full recommendation.) However, for the purpose of this document, the focus will be on the identification and verification dimension of CDD, recognizing that all other dimensions are relevant but out of the scope of this toolkit.

FIGURE 1: Digital ID Usage in Financial Services

FIGURE 2: Dimensions of CDD under Recommendation 10



Furthermore, FATF Recommendation 10 establishes that financial institutions should be prohibited from keeping anonymous accounts or accounts in obviously fictitious names. Also, financial institutions should conduct CDD under the following circumstances (see figure 3):

(i) Establishing business relations (that is, onboarding new clients)

(ii) Carrying out occasional transactions above 15,000 US dollars or euros; or

(ii) Electronic transfers based on interpretative note (IN) R16:[8] For cross-border wire transfers, countries may adopt a *de minimis* threshold not higher than 1,000 dollars or euros where information on the name of the originator, the beneficiary, and the account number is required, but there is no need for verification.

(iii) Suspicion of the illegal activity of money laundering or the financing of terrorism; or

(iv) When the financial institution has doubts about the veracity or adequacy of previously obtained customer ID data

FATF standards are applicable to both traditional and digital financial services. The digital financial services cover financial products and services, including payments, transfers, savings, credit, insurance, and securities delivered via digital/electronic technology, such as e-money (initiated either online or via a mobile phone), payment-initiation services, payment cards and online lending.. In many developing countries, the primary pathway to financial inclusion is often via a mobile wallet or e-money account. Therefore, the enrollment process—including identification of customers—by mobile network operators (MNOs) is very relevant to the onboarding process.

Digital ID systems have the potential to improve the reliability, security, privacy, and efficiency of the process of identifying individuals in the financial sector, to the benefit of both customers and regulated entities. However, digital systems also present a variety of technical challenges and risks of failure. Well-design policies, and digital ID system design that fosters both inclusion and trust, are fundamental to mitigating such risks and guarding against challenges.

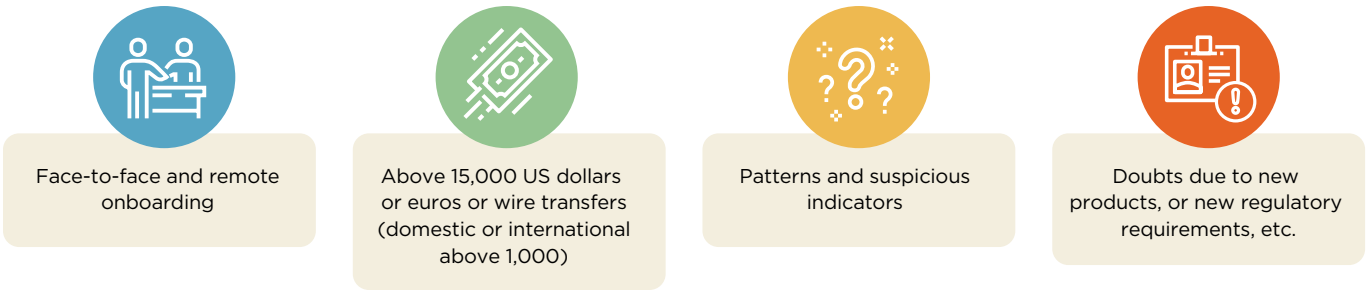
Driven by the rapid growth in digital payments, which requires a better understanding of how individuals are being identified and verified in the world of digital financial services, the FATF released *Digital Identity*, its guidance on digital ID,[9] in 2020.

However, despite the hype surrounding the development of digital ID systems, just a few countries have developed effective, comprehensive approaches to digital ID. Other scenarios also include the electronic ID databases that, to some extent, allow the verification of the ID credentials and/or attributes included in the customer's credentials through online verification services. Finally, in the absence of such measures, FSPs have developed systems that provide a higher level of assurance by adopting electronic KYC (e-KYC) solutions that include supplementary data and external data sources.

1.2 OBJECTIVE OF THIS TOOLKIT

This document will focus on the policy considerations of digital ID and financial inclusion, building on the 2013 ***FATF guidance on financial inclusion,***[10] the 2018 *G20 Digital Identity Onboarding* for the ***G20 Global Partnership on Financial Inclusion,***[11] the 2020 ***digital ID guidance from the FATF,***[12] ***Principles on Identification for Sustainable Development,***[13] ***Enhancing Cross-Border Payments: Building Blocks of a Global Roadmap,***[14] and, finally, practical country experience with ID needs and digital ID implementation, where available. This toolkit aims to provide direction for financial-sector regulators on how to leverage digital ID systems and digital ID solutions to enhance KYC practices.

FIGURE 3: Illustration of Scenarios That Require CDD Measures under FATF Recommendations



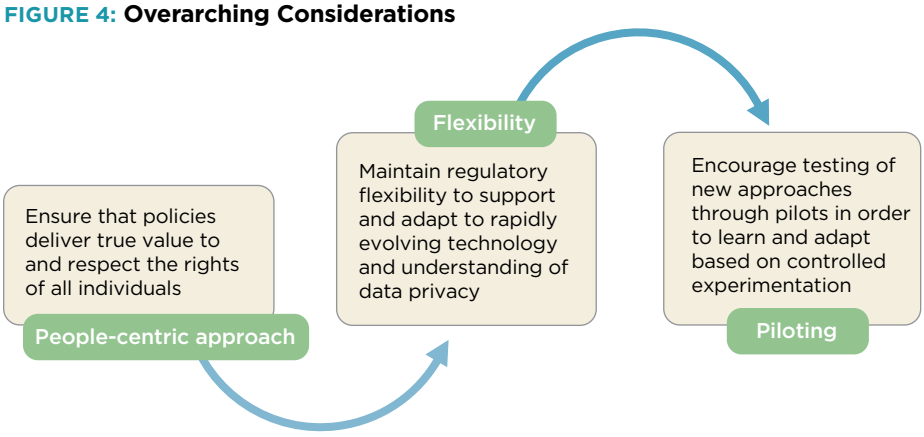
The toolkit comprises (i) an analysis of relevant policy considerations based on overarching objectives and including supporting implementing approaches, (ii) a methodology for using the guide, (iii) guiding questions for regulatory authorities to consider or for external assessors to understand the financial-sector context for the use of digital ID, and (iv) a glossary of terms.

There are three overarching objectives: taking a people-centric approach, maintaining flexibility, and piloting to learn and adapt. These three themes are echoed throughout the following policy considerations and suggested implementing approaches.

This toolkit aims to identify the key policy aspects necessary for the usage of digital ID or other electronic means of verifying the identity of users of financial service and supports their implementation by financial-sector regulators. It focuses on the application of digital ID systems in the financial sector for identification and verification when onboarding new clients for transaction accounts, as well as when additional products and services, including digital financial services, are offered to or requested by customers (as detailed in figure 3). It incorporates the attributes of best practice, including in areas of high assurance and consent-based creation and use, to promote trust and protect personal data.

The guidance is not intended to replace but to complement the tool *Guidelines for ID4D Diagnostics,* as well as the *ID Enabling Environment Assessment (IDEEA)*[15] developed through the ID4D initiative at the World Bank.[16]

FIGURE 4: Overarching Considerations



2. Policy Considerations

The G20 digital ID onboarding paper highlights seven policy considerations. In brief, they include (i) ensuring an integrated identity framework, (ii) the appropriateness of the regulatory framework; (iii) establishing a reliable oversight model to include stakeholders beyond the traditionally regulated financial institutions; (iv) building authentication and service-delivery systems that protect user privacy; (v) establishing clear and well-publicized procedures for citizen redress; (vi) supporting and empowering the development of services led by the private sector to leverage the legal ID infrastructure for building out digital layers; and (vii) closely monitoring emerging developments and technologies.

Here, we present five policy considerations that are specifically relevant to financial-sector regulators looking to accelerate the use of digital ID for expanding access to and the uptake of financial services. Each policy consideration includes several suggested implementing approaches and highlights relevant case studies. These approaches are intended to help countries assess and implement key policies necessary to access and use digital ID in the financial sector, with the understanding that these approaches will need to be adapted to fit the needs of each country.

2.1 POLICY CONSIDERATION 1: *Ensure that the legal and regulatory framework is supportive of the ue of digital ID by financial service providers*

Financial-sector regulations have long-standing requirements related to customer ID, validation, authentication of customer identity, and retention of customer records, to ensure the safety and integrity of the financial system, based primarily on FATF recommendations. (See appendix A.) The FATF recommendations encourage countries to incorporate the recommendations into the laws of the country. FATF recommendations (R10) require financial institutions to identify their customers and, when verification is needed, to use "reliable and independent source documents, data or information" (identification data) to verify identity. Therefore, as presented in table 2, the use of digital ID by FSPs for CDD and authentication, requires updating or establishing legal/regulatory frameworks to establish legal certainty of its usage as well as to protect customers. In addition, other general rules also apply to financial institutions, such as those related to perfection of contracts and consumer protection, including data protection and fraud prevention (for example, e-signatures and consumer consent).

TABLE 1: Summary of Policy Considerations and Implementing Measures

Policy Considerations	Implementing Measures
1. The legal and regulatory framework supports the use of digital ID by FSPs	Foster dialogue between different agencies and actors
	Develop clear guidelines or regulations allowing the appropriate, risk-based use of digital ID systems
	Consider if a simplified CDD framework would be appropriate based on a risk-based analysis
	Assess if the existing legal and regulatory framework covers the use of digital ID and electronic verification of customer identity
	Harmonize CDD requirements
	Adopt technical standards to the use of digital ID
	Support the use of e-KYC solutions
	Guidelines on nonface-to-face account opening
	Guidelines on the role that electronic signatures (e-signatures)
	Mitigate exclusion risks for those who do not have a digital ID
2. Identify the full range of risks related to the use of digital ID by FSPs	Data governance
	Privacy by design
	Conduct a data protection impact assessment
	Encourage data minimization, whereby FSPs collect only the minimal amount of data required for the intended purpose
	Mitigate fraud-related threats
	Establish guidelines on legal and technical requirements for cyber resilience and cyber incidents.
	Establish protocols for incident responses when there is a data breach
3. Adopt consent mechanisms for customers	Build easy-to-understand consent mechanisms
	Data controllers to be able to prove the capture of consent and expiry of consent
	Handle disputes for errors in consent management
4. Support collaboration with the private sector	Establish a platform (such as a working group) for collaboration and dialogue
	Consider the supportive role that MNOs can play in ID enrollment and verification
	Ability for the private sector to build on top of, or supplement, foundational infrastructure and resources
	Encourage the use of collaborative platforms and application programming interfaces to support identity management, including interoperability, efficient data exchange, and data portability
	Develop robust procurement guidelines and support open design standards
	View emerging technologies and applications as an opportunity, but recognize the potential risks they pose to regulatory objectives
	Consider the use of regulatory "sandboxes"
5. Oversight framework for digital ID	Establish clear institutional mandates
	Transparent, proportionate, and equitable framework
	Establish an independent oversight body

TABLE 2: Credentials and Their Use in the Financial Sector

Application	How Digital ID Helps Address Barriers	Risks Mitigated
CDD	Allows FSPs to prove the identity of a customer and verify if the ID belongs to the customer in real time, resulting in better AML/CFT controls. For low-risk scenarios, simplified CDD can be used, and there is no need to verify the customer's identity at that moment. Ongoing monitoring is supported by digital ID.	Financial fraud, ID theft
Authentication to access services	Allows FSPs to conduct real-time authentication of customer identity based on information submitted at onboarding.	Cyber risk, fraud, data breaches
E-signatures	Enables remote access to financial services by ensuring that the message is adequately attributed to its original sender.	Fraud
Customer consent to access data	Allows FSPs to prove that the consent has been provided by the customer itself.	Financial fraud, ID theft

While digital ID systems enable accessibility and provide a robust means of verifying customer identity, they also bring several risks in terms of data protection, fraud, and cybersecurity issues. Hence, a robust regulatory framework on AML/CFT and data protection and privacy that strengthens CDD while mitigating the risks associated with digital ID forms the first-order consideration for policy implementation.

When deploying financial services and particularly digital financial services, multiple scenarios require a clear legal and regulatory framework with regards to CDD, authentication, remote transactions acceptance, and authorization to access customer's data. Each of these scenarios responds to different needs and different FSPs and may involve fraud risks and risks of money laundering and the financing of terrorism that affect the regulatory approach adopted in a certain jurisdiction.

The financial-sector regulator will need to assess whether the existing regulations and guidance on CDD, financial inclusion, and fraud prevention accommodate digital ID systems and revise as appropriate in light of the jurisdictional context and the identity ecosystem. To assess if the existing legal and regulatory framework supports the adoption of digital ID, it would be necessary to evaluate the following features:

i. Is the legal framework flexible enough to allow for new financial customers to use digital ID for remote onboarding?

ii. Does the legal framework establish sufficient and adequate authentication factors for existing customers?

iii. Does the legal framework allow the use of documents, data, and information from different authoritative sources to prove a customer's identity?

iv. Does the legal and regulatory framework establish adequate and proportionate requirements for customer identification and verification based on the risks of money laundering and the financing of terrorism?

v. Does the legal framework recognize e-signatures for remote perfection of contracts?

vi. Does the legal framework sufficiently cover risks associated with fraud, ID theft, and cybersecurity, and does the legal and regulatory framework apply equally to all potential providers of digital financial services in a given jurisdiction?

2.1.1 Implementation Approaches for Policy Consideration 1

a. Conduct extensive interagency dialogue across relevant agencies in line with FATF Recommendation 10 to understand opportunities and risks in sharing data across agencies pertaining to money laundering and the financing of terrorism, data protection, fraud, and cybersecurity.

The financial regulator should consider facilitating dialogue through a working group or similar structure while establishing the legal and regulatory framework for digital ID systems in the financial sector. The key players could be the foundational identity authority, financial-sector regulatory authorities, including the financial intelligence unit, the financial authority with a financial-inclusion mandate, data-protection authorities, cybersecurity-enforcement agencies, the telecom regulator and other entities that might be relevant to the context that pertains to a specific jurisdiction. A formal or informal consultative group that enables open discussions and fosters collaboration could be a useful instrument for such dialogue. Authorities could also consider involving the private sector in the dialogue through either a consultative mechanism or by inviting them to participate in the working group.

b. Develop clear guidelines or regulations allowing the appropriate, risk-based use of digital ID systems by regulated FSPs for AML/CFT purposes, including across borders.

A flexible approach to documents and data attributes for customer ID as well as for authentication factors enables broader financial services coverage of individuals. Many countries require customers to provide specific attributes or documents that are not available for all population groups. Other countries require additional information beyond a basic ID document to open an account with a FSP. The graph in figure 5 depicts the different documentation required to open a transaction account based on data collected from 124 separate jurisdictions (**Global Financial Inclusion Consumer Protection Survey, 2017**)

The use of digital ID systems for customer ID verification by FSPs might also require an assessment of the digital ID systems available in the jurisdiction and how they fit into existing requirements on customer ID and verification, and ongoing due diligence.

A harmonized adoption of security and technical standards can also support the ability to enhance the security and accessibility of cross-border payments. Faster, cheaper, more transparent, and more inclusive cross-border payment services, including remittances, that also maintain their safety and security would have widespread benefits for individuals and economies worldwide, supporting economic growth, international trade, global development, and financial inclusion.

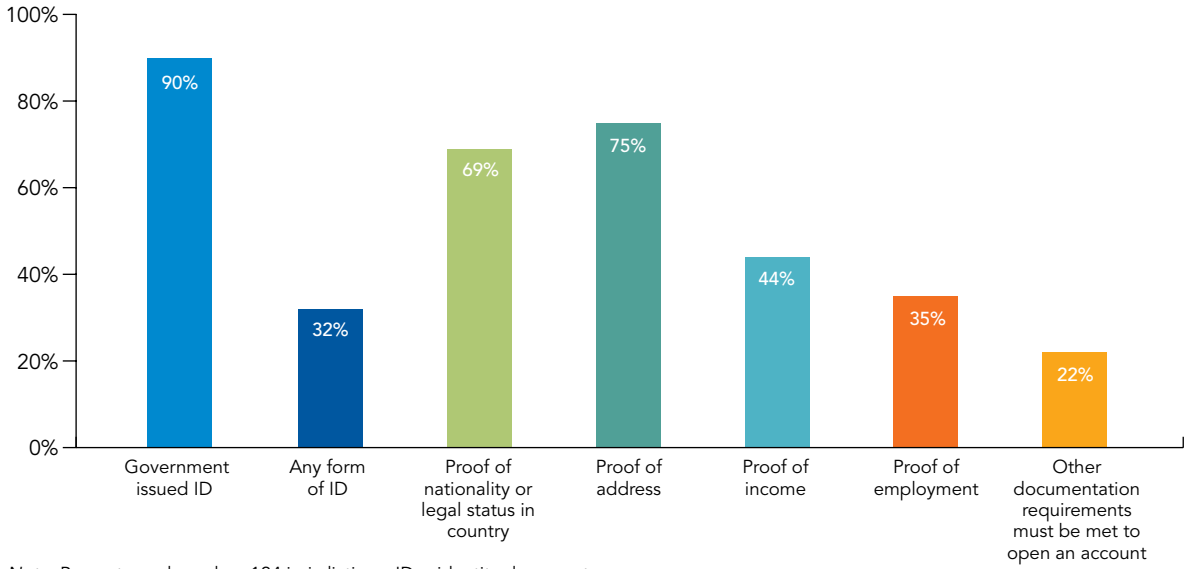
Harmonization is also important for cross-border transactions. The Committee on Payments and Market Infrastructures (CPMI) set out 19 building blocks (BBs) intended to be used flexibly in combination with other existing or new enhancements to cross-border arrangements and infrastructures. BB8[17] specifically states the need to "Foster(ing) KYC and identity information sharing." Other relevant building blocks include BB15, "Harmonising API protocols for data exchange" (detailed in 2.4.1b); BB16, "Establishing unique identifiers with proxy registries"; and BB17, "Considering the feasibility of new multilateral platforms and arrangements for cross-border payments."

BB8 is structured around the following three main actions: (1) fostering better alignment and cross-border recognition of identity requirements, CDD requirements, and the digital ID assurance frameworks and technical standards; (2) improving the coverage, access, and quality of the official ID databases for individuals and identifiers for legal entities; and (3) implementing shared or interoperable CDD infrastructure to allow financial institutions to access digital ID databases to meet their CDD obligations in a cost-effective way, domestically and across borders.

c. Consider if simplified CDD (SCDD) would be appropriate based on a risk-based analysis, and establish measures to basic accounts under the a simplified CDD framework.

The rapid digitization of financial services has greatly increased the importance of reliable, independent digital ID systems for financial inclusion, especially in developing countries,[18] where digital ID systems and digital financial

FIGURE 5: Customer Identification Requirements for Opening a Bank Account



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

Source: Global Financial Inclusion and Consumer Protection Survey, 2017

services have emerged as core drivers of financial inclusion.[19] Leveraging digital ID systems to adopt a risk-based approach to meeting AML/CFT requirements would entail making available "financial products or services that provide appropriately defined and limited services to certain types of customers, so as to increase access for financial inclusion purposes" (**FATF 2013 revised in 2017**) through a tiered CDD regime based on the risk level of money laundering and the financing of terrorism and products/channels used. Basic transaction accounts with limitations on the number and value of transactions provide a first step into the formal financial sector for otherwise unbanked individuals. The main objective of this type of account is to enable access while preventing money laundering and the financing of terrorism. A risk-based approach to simplifying CDD would thus include flexibility in legislation pertaining to identification requirements for opening accounts for customers without official documents based on the tier level pertaining to the account. For an example of simplified CDD in practice, see box 1 on Pakistan's Asaan account.

d. Assess whether the existing regulations and guidance on CDD cover the use of a digital ID system and electronic ways to verify customer identity and revise as appropriate in light of the jurisdictional context and identity ecosystem.

While some jurisdictions have developed specific regulations related to CDD, the use of digital ID might require a review and adoption of additional language to reflect differences between using physical credentials versus using digital ID as the main ID document to validate the identity of clients. While physical credentials used in the financial sector are typically issued by the government, digital ID might be issued by a private identity service provider (IDSP) that could require either licensing, authorization, or adherence to governance and data-management standards to enable its use.

The process of assessing and establishing a legal and regulatory framework for the use of digital ID—other than government issued or authorized—in the financial sector will need to be based on two factors: the level of assurance applicable to a specific jurisdiction, and interagency dialogue or stakeholder consultation with relevant entities. To understand if the level of assurance of a digital ID is adequate to a particular risk of money laundering and financing of terrorism, authorities would also need to understand the governance system, including data governance, operational aspects, and risk management. It might be the case that a digital ID system that is suitable for identifying a user of a public library is not suitable for accessing a financial service.

Bank Negara Malaysia issued a regulation on e-KYC, establishing minimum requirements for e-KYC solutions adopted by regulated entities.[21] (See more details in Policy Consideration 4.) Some of the measures are related to digital ID features, including the following: (i) utilize biometric technology to verify the customer against a government-issued ID; (ii) utilize fraud-detection technology to ensure that the government-issued ID used to support e-KYC customer verification is authentic; and (iii) utilize liveness-detection technology to ensure that the customer is a live subject and to detect impersonation attempts (for example, use of photos, videos, and facial

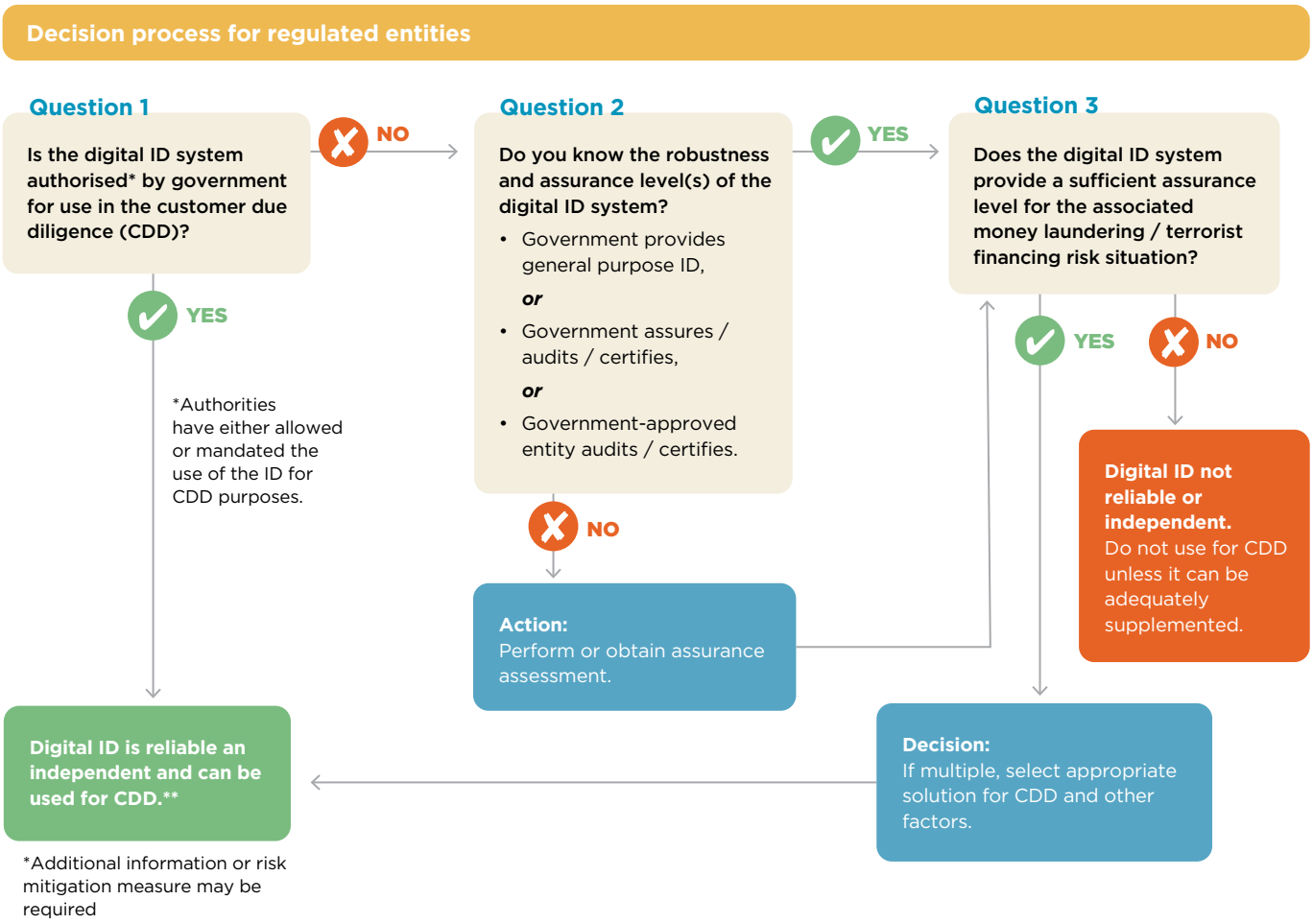
BOX 1

PAKISTAN ASAAN ACCOUNT: SIMPLIFIED CUSTOMER DUE DILIGENCE

According to the 2014 Global Findex, 21 million adults in Pakistan are estimated not to have an account due to a **lack of adequate documentation** (Demirguc-Kunt, et al. 2015). Circular 11 of 2015 of the State Bank of Pakistan established specific guidelines for verifying low-risk accounts with simplified due diligence. The regulation allows several documents to be used as a proof of identity for opening Asaan accounts, including (i) the Computerized Smart National Identity Card, (ii) the National Identity Card for Overseas Pakistanis, (iii) the Pakistan Origin Card, (iv) the Alien Registration Card issued by the National Aliens Registration Authority, (v) a passport, and (vi) a pension book. Verification of the documents provided can be obtained through the National Database and Registration Authority up to three days after opening the account. The Asaan accounts are for individuals only and include a maximum monthly transaction limit of Prs 500,000 and a minimum deposit of Prs 100. Each individual can open only one Asaan account. These accounts can be opened at the bank branch through a simplified form not exceeding one page that requires the signature of the customer either wet or electronic.

Source: State Bank of Pakistan, Circular 11 (2015)

FIGURE 6: Decision Process for Regulated Entities[20]



Source: Guidance on Digital ID, FATF 2020

masks). Other measures refer to governance and require the FSP board to approve the e-KYC solution, conduct a risk assessment, and implement policies and protocols to identify and address potential risks from an operational, information technology, and AML/CFT perspective.

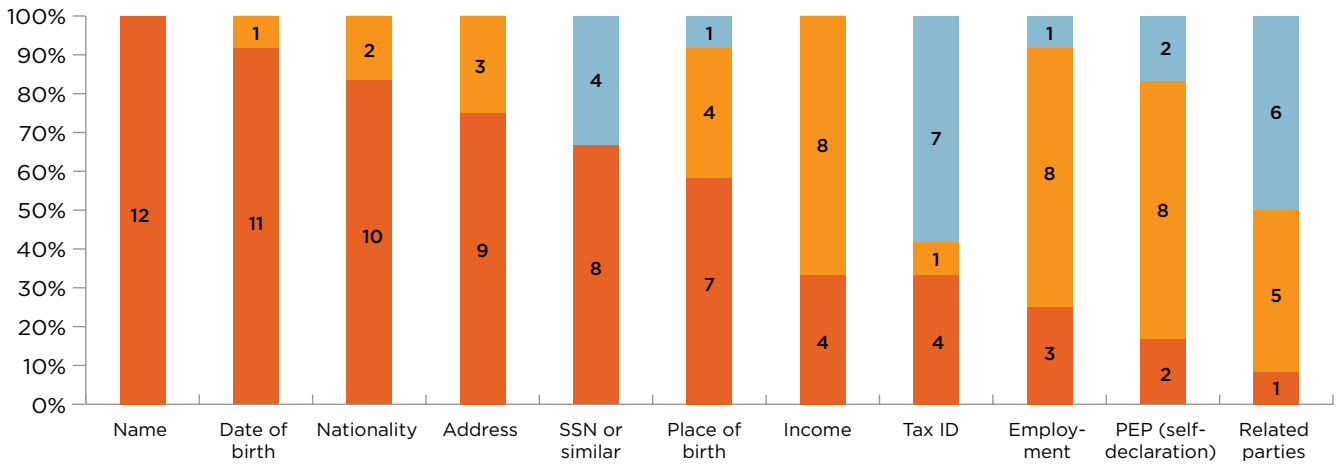
e. Harmonize CDD requirements for all FSPs, including banks and nonbank FSPs.

In many jurisdictions, the customer-identity documentation and verification requirements for banks under a tiered CDD scheme are more intensive than the documentation requirements for non-bank digital FSPs. Such differences in CDD requirements/provisions for financial products across financial institutional categories create an uneven playing field in the delivery of financial products and services, limiting the quality and variety of services that certain population groups can access. Hence, it will be important for financial-sector regulators to harmonize the AML/CFT regulatory framework to ensure consistency in CDD requirements across institutional categories. Differences in requirements should be based on risks and criteria related to the jurisdictional context of the country (for example, countries with preferential tax regimes, bank-secrecy provisions, high volumes of international remittances, cash-intensive economies, or a relevant number of nonresidents); the type of product (for example, cross-border transactions, government payments, person-to-person e-transactions, or lending operations); and the type of client (for example, persons of concern, legal entities, gatekeepers, and politically exposed persons). Based on a World Bank survey conducted in 2019,[22] the charts in figure 7 illustrate the requirements in different jurisdictions for opening a bank account, making wire transfers, and opening a mobile-money account.

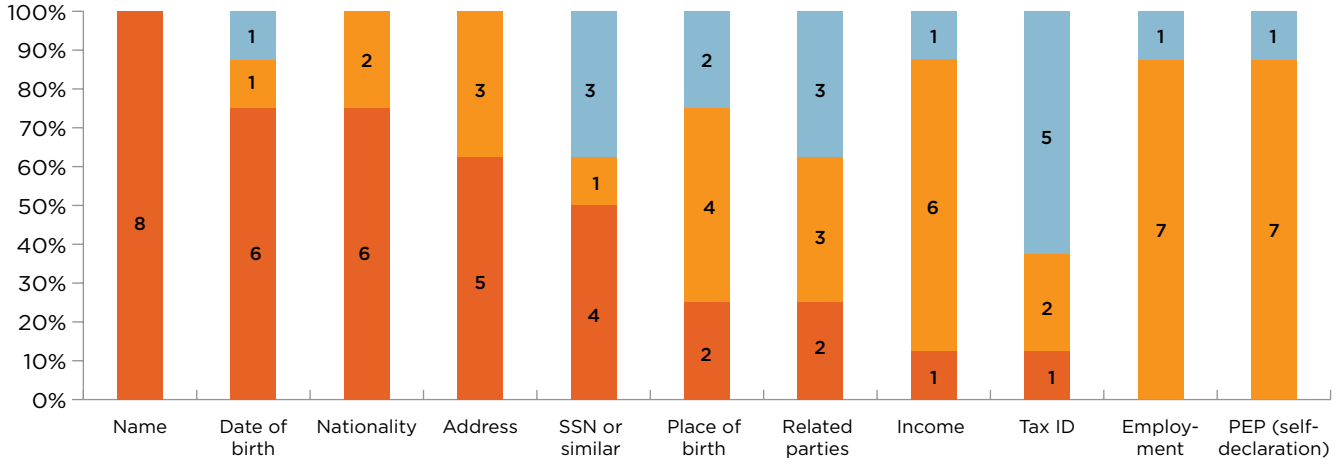
f. Adapt the regulatory framework pertaining to the use

FIGURE 7: Data Requirements

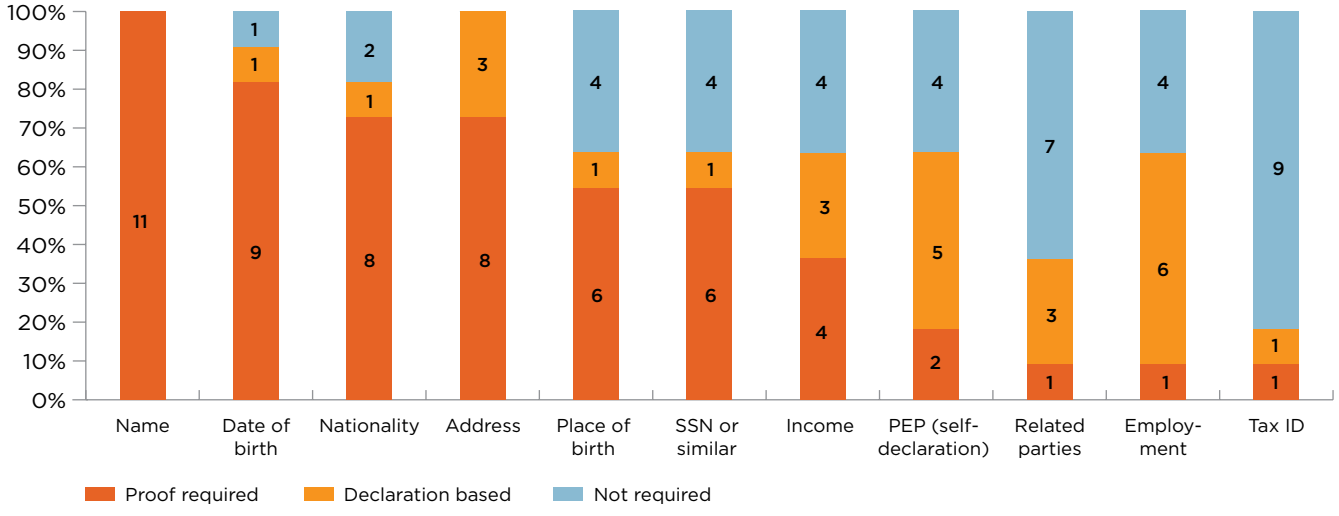
a) Data Requirements for Opening a Bank Account



b) Data Requirements for Opening a Mobile-Money Account



c) Data Requirements for Making Domestic Wire Transfers



of digital ID in the financial sector to the underlying digital ID assurance frameworks and technical standards that apply to a jurisdiction's digital ID system.

Assurance levels (ALs) or levels of assurance measure the level of confidence in the reliability of the digital ID system in each of the three stages of the digital ID process—enrollment, verification, and authentication. Jurisdictions may establish their own assurance frameworks or rely on consensus-driven assurance frameworks and technical standards developed by other jurisdictions or standard-setting entities, such as the digital ID assurance framework of the US National Institute of Standards and Technology (NIST)[23] or the European Union's e-IDAS regulation. For more details, refer to the draft FATF digital ID guidance.

An example is the ID platform in Thailand that is based on NIST, incorporates both Identity Assurance Levels (IALs) and Authentication Assurance Levels (AALs), and was adjusted to the country context.

g. Support various models of KYC solutions and collaborative CDD, so that public and private entities can share data or rely on existing data to streamline customer CDD across FSPs.

To improve the cost and time burden associated with CDD, national ID systems can potentially be employed to support service providers with the verification of customer identity. To support this type of collaboration, digital ID systems will need to include a component that enables proof of identity to be portable. Portable identity means that an individual's digital ID credentials can be used to prove official identity for new customer relationships at unrelated private-sector entities, such as FSPs or government entities, without requiring the systems to obtain and verify personal data and conduct customer identification/verification each time. Hence, portability can be supported by different digital ID architecture and protocols. In Europe, the eIDAS Regulation provides a framework for cross-recognition of digital ID systems based on mutual recognition.[24]

The Dutch Payments Association launched the iDIN service, which refers to both the electronic ID as well as the PIN code traditionally used to authenticate oneself to a bank. iDIN (formerly known as BankID) allows consumers to access other organizations using the secure and trusted logins of their own bank. The iDIN scheme is based on participating entities having signed licensing agreements and being subject to operational rules. There are two types of participants: (i) digital identity service providers, and (ii) acquirer license holders. The service allows customers to identify themselves, to log in into existing services, and to confirm age.

Collaborative arrangements and approaches to CDD

TABLE 3: Levels of Assurance for ID Proofing

Requirement	Assurance Level 1	Assurance Level 2	Assurance Level 3
Presence	No requirement	In person	In person; supervised remote
Resolution	No requirement	• The minimum attributes necessary to accomplish identity resolution • • Knowledge-based verification may be used for added confidence.	Same as Assurance Level 2
Evidence	No evidence is collected	• One piece of SUPERIOR or STRONG evidence, depending on the strength of the original proof, and validation occurs with the issuing source, OR • Two pieces of STRONG evidence, OR • One piece of STRONG evidence, plus two (2) pieces of FAIR evidence.	• Two pieces of SUPERIOR evidence, OR • One piece of SUPERIOR evidence and one piece of STRONG evidence, depending on the strength of the original proof, and validation occurs with the issuing source, OR • Two pieces of STRONG evidence, plus one piece of FAIR evidence.
Validation	No validation	Each piece of evidence must be validated with a process that is able to achieve the same strength as the evidence presented.	Same as Assurance Level 2
Verification	No verification	Verified by a process that is able to achieve a strength of STRONG	Verified by a process that is able to achieve a strength of SUPERIOR
Address confirmation	No requirement	Required	Required. Notification of proofing to postal address
Biometric collection	No	Optional	Mandatory
Security controls	N/A	Moderate baseline	High baseline

Source: Guidance on digital ID (FATF, 2020)
See appendix B for NIST definitions of strong, superior and fair

FIGURE 8: Identity Assurance Levels

		Identity Assurance Level (IAL)				
		Face2Face		Non F2F—Kiosk		
	IAL 3 *2 Encrypted identity evidence with biometric comparison*	Dip chip online to DOPA	or Use NFC to download data from passport with digital signature from ICAO	+ KIOSK: Must take a photo + Liveness F2F: Must take a photo + Liveness	+ Biometric comparison (At least 1 method)	+ VDO call (optional)
IAL 2 (1 Encrypted identity evidence) (Identification + verification)	IAL 2.3	Dip chip online to DOPA	or Use NFC to download data from passport with digital signature from ICAO	+ KIOSK: Must take a photo + Liveness F2F: Must take a photo + Liveness	+ Biometric comparison (At least 1 method)	
	IAL 2.2	Dip chip online to DOPA	or Use NFC to download data from passport with digital signature from ICAO	+ KIOSK: Must take a photo F2F: Must take a photo		
	IAL 2.1	Dip chip (offline)	or Use NFC to download data from passport	+ KIOSK: Must take a photo F2F: Take a photo (optional)		
IAL 1 (No require identity evidence) (Identification)	IAL 1.3	Show citizen ID to staff (might be copy of ID)		Scan citizen ID to kiosk		Photo record (optional)
	IAL 1.2	Use copy of citizen ID to staff (Not require identity card)		Upload photo of copy of citizen ID		Photo record (optional)
	IAL 1.1	Trusted on user (not any document required)		Trusted on user (not any document required)		Photo record (optional)

Source: National Digital ID Limited Thailand, 2019

BOX 2

eIDAS INTEROPERABILITY AND MUTUAL RECOGNITION

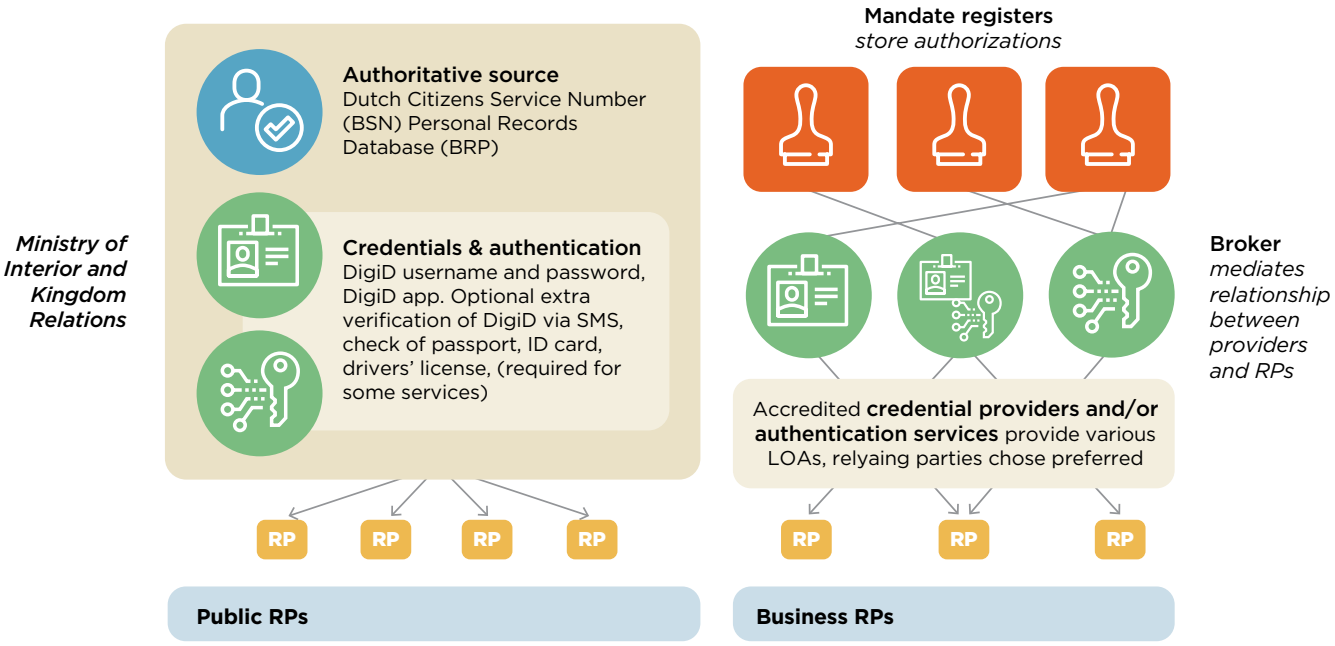
The eIDAS Regulation defines three different assurance levels—low, substantial, and high—depending on the degree of confidence in the claimed or asserted identity of a person.

Under the eIDAS framework, member states are free to use or introduce means for the purposes of electronic identification for accessing online services. They should also be able to decide whether to involve the private sector in the provision of those means. Member states should not be obliged to notify the European Commission of their electronic-identification schemes. Under the principle of mutual recognition, member states are obliged to accept other member states' notified means of electronic identification. This obligation applies if the member states allow the use of the means of electronic identification for online access to their public services, and if the assurance level of the notified means is equal or higher than the one necessary to access the service.

The security of electronic-identification schemes is key to trustworthy, mutual, cross-border recognition of the means of electronic identification. In this context, European Union member states cooperate with regard to the security and interoperability of the electronic-identification schemes at the level of the European Union. Whenever electronic-identification schemes require specific hardware or software to be used by relying parties at the national level, cross-border interoperability calls for those member states not to impose such requirements and related costs on relying parties established outside of their territory. In that case, appropriate systems should be discussed and developed within the scope of the interoperability framework.

Source: Guidance on digital ID (FATF, 2020)

FIGURE 9: Netherlands DigiID



Source: Guidance on digital ID (FATF, 2020)

between FSPs are beginning to be used more commonly and can present different designs, infrastructures, scopes of data, types of participants, and governance. They are a way to reduce the full burden—and cost—of CDD being carried by individual FSPs. An example of collaborative CDD is the KYC registry, which stores data in a common database or single repository to be used by multiple FSPs. The governance structure of the KYC registry could rely on a government agency acting as the administrator of the database or commercial third-party service providers. The latter calls for fair and transparent rules regarding liability, as providers will be unwilling to rely on third-party data and services if they risk being held liable for gaps and errors outside of their control. By pooling resources, reducing duplicative efforts, and digitizing processes through KYC registries, FSPs can shorten the time required for identity checks and verification, reduce CDD compliance costs, and potentially improve the quality and reliability of customer data. Some additional aspects to be considered when designing a collaborative platform are included in table 4.

Despite the promise of these innovations in collaborative approaches to CDD, there are barriers to implementing them effectively on a global scale. Country-level regulations often limit FSPs' ability to share information, a problem that becomes vastly more challenging in the cross-border context. However, the cross-border issue is limited not only by data sharing limitations but also by harmonization, connectivity, governance arrangements, and technical standards, among other things.

The Monetary Authority of Singapore (MAS) tested a KYC utility for financial services based on the MyInfo[25] digital identity service[26]—which was developed jointly by the Ministry of Finance and GovTech, the lead agency for digital and data strategy in Singapore.

The KYC utility contains data provided by the user and data pulled from the databases of various government agencies, such as the national ID number, passport number, registered address, and date/country of birth. Data is obtained with the consent of the customer, and FSPs can rely on the information provided by MyInfo to comply with AML/CFT requirements regarding KYC, including non-face-to-face business relations. The main regulatory aspects of MyInfo are that it has been recognized by MAS as a reliable and independent source for the purposes of verifying a customer's name, unique ID number, date of birth, nationality, and residential address, which allows FSPs to fulfill their CDD requirements efficiently. Another relevant element of Myinfo is that MAS recognizes that, when MyInfo is used, there is no need for additional ID documents or to verify customers' identity, and MAS will not expect FSPs to obtain a photograph of the customer.

Another example is that of Bangladesh Bank, which issued guidelines on e-KYC in December 2019 to foster e-KYC solutions. The guidelines aim to provide additional information to FSPs on how to implement the FATF risk-based approach to CDD that was captured under the Bangladesh Bank's Vision 2021—aligning financial-inclu-

TABLE 4: Key Features for a Collaborative CDD Platform

Feature	Explanation
Use cases	Define the cases in which the scheme would be used (for example, onboarding and what level of CDD, ongoing monitoring, new product offering)
Users	Requirements to become a user of the system
Data protection	Principles (data quality, retention period, data minimization, ARCO rights, legal bases for data collection and access, localization)
Security	Measures to protect the network, system, and data against unauthorized access, data misuse, loss, and corruption. Also, to ensure system integrity and business continuity.
Governance	Establishment and enforcement of system rules, risk-mitigation policies, pricing, and reliability of the infrastructure. Technical and governance standards defined.
Interaction with other databases	Either to verify data in the system or to fetch additional complimentary data
Customer self-registration capability	Convenient for the customer (a) to take a selfie photograph to an agreed standard and upload it into the KYC facility, (b) to upload biometric data, (c) to provide liveliness proof, and (d) to log in to existing digital credentials and agree to share such credentials with other FSP.
CDD output	The output should be defined (for example, politically exposed person, pass-or-fail confirmation, online dashboard of details, age confirmation, or other specific attribute)
CDD output	The system might be able to generate a digital ID credential for the customer to download and use in subsequent FSP transactions
CDD output	Ad hoc designed output for the specific user (for example, AML/CFT risk assessment)

Source: Authors' elaboration

BOX 3

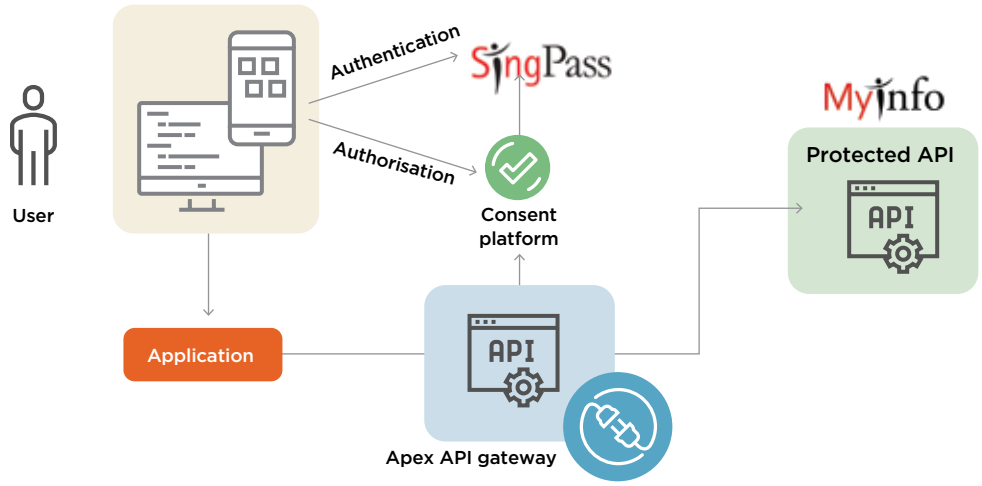
INDIA: AADHAR AND CENTRAL KYC RECORDS REGISTRY

Collaborative CDD has been illustrated in India, which allows FSPs to consider customer ID verification data obtained through the national digital ID system to be correct without verifying the data. The Unique Identification Authority of India (UIDAI) has made e-KYC and authentication services available for FSPs. An FSP can verify a customer's identity using the customer's Aadhaar number (a random 12-digit number issued by the UIDAI to the individual) and a fingerprint and/or iris scan. When the identity of a prospective customer is confirmed biometrically, the account-opening form, with the consent of the customer, is automatically populated with the customer's basic demographic data. This measure has allowed providers to rely on a government-issued ID system without fear of liability, ensuring good uptake of the system.

India also has a centralized repository of capital market investors' 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 an 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. The main purpose of the KRA was to eliminate duplication of CDD efforts that a customer must undergo while dealing with multiple market intermediaries, such as mutual funds, private equity funds, brokers, and depository participants. There are efforts to expand this solution to the broader financial sector.

Source: Central Registry of Securitisation Asset Reconstruction and Security Interest of India (CERSAI)

FIGURE 10: MyInfo Workflows, Singapore



sion objectives and AML/CFT goals.

Prior to issuing the guidelines, Bangladesh Bank conducted a pilot on customer onboarding using biometrics and different technologies, where a customer's identity was checked by using the national ID card issued by the National Identity Registration Wing of the Election Commission of Bangladesh. The pilot was based on fingerprint scanning, face-matching technology, and artificial intelligence.

In Bangladesh, when the risk of money laundering and the financing of terrorism is low—based on limited wallet use and a low value of transactions—the Bangladesh Financial Intelligence Unit allowed simplified CDD for mobile financial services, digital financial services, and other low or limited risks in banking, insurance, and securities products. Conversely, for situations with a higher risk of money laundering and the financing of terrorism, FSPs may adopt additional independent means of reliable information to verify customers' identity details.

The guidelines provide for the following;

i. Simplified CDD (SDD): For low-risk customers, the FSP shall be required to conduct simplified e-KYC requiring only a limited set of characteristics, which includes electronic customer onboarding and shorter verification of the customer's identity and preservation of the customer's profile digitally. SDD is the lowest level of due diligence that can be completed on a customer and is characterized by a shorter verification process. It is only permitted where there is a low risk of AML/CFT risk.

ii. Regular and enhanced CDD (EDD): For customers under regular and higher-risk scenarios, the e-KYC process includes electronic customer onboarding and the verification of a customer's identity and preservation of KYC forms and risk grading digitally. The e-KYC requirement under this scenario can be based on biometric verification, which applies only to individuals. In a regular or enhanced CDD process, more evidence or monitoring is required compared to SDD.

The e-KYC process in Bangladesh allows for two different approaches: (i) an assisted process, by which the onboarding is conducted by an officer or agent, and (ii) a self-check-in, by which the customer uploads the information at a kiosk or using a smartphone, computer, or other digital device. The device used should allow for fingerprint and face matching, although other modalities are also accepted, including iris or voice matching. The e-KYC is based on individuals who have a valid national ID card and covers:

a. Digital financial services (mobile financial services, payment service providers, payment service operators, and fintech companies under the low-risk scenario)

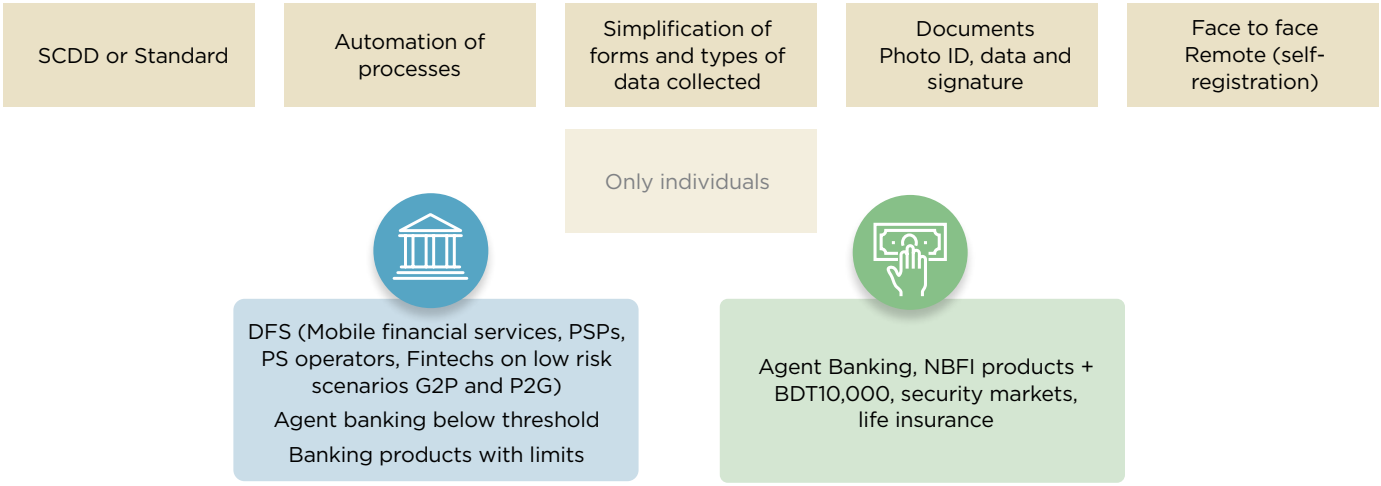
b. Financial-inclusion products (government-to-person payments for government social programs, person-to-government payments, and existing financial-inclusion products)

c. Agent banking products (existing agent banking products within the transaction limits set by Bangladesh Bank from time to time)

d. Banking products (deposit or withdrawal not exceeding Tk 1,000,000 per month in a checking account, a term deposit up to Tk 10,000,000, and a special deposit scheme with maturity value exceeding Tk 10,000,000)

e. Products from non-bank financial institutions (any type of products not exceeding Tk 10,000,000)

FIGURE 11: Illustration of a Collaborative CDD Framework (Bangladesh)



h. Allow for non-face-to-face account opening in which digital ID or alternative mechanisms can be used for remote customer identification/verification and authentication.

Difficulties in opening transaction accounts is a barrier for rural population segments to access formal financial services. The requirement to be present in a banking or agent office creates additional burdens to this segment of the population. In jurisdictions with comprehensive digital ID coverage, the regulatory framework should allow for non-face-to-face or remote account opening through an electronic device for low-value transaction accounts, where a lower level of assurance might be sufficient—that is, allowing the identity evidence to be *obtained remotely* and/or allowing identity attributes and other information to be *remotely verified and validated against a digital database(s).*[27] The 2017 Global Financial Inclusion and Consumer Protection Survey shows that, of 124 jurisdictions, 30 percent of jurisdictions report that banks can use non-face-to-face CDD (for example, by agents and/or via mobile devices).

Figure 12 provides an example of ID verification for remote account opening using IDnow.

More recently, several jurisdictions have responded to the COVID-19 pandemic by delivering different types of government subsidies to individuals and legal entities. Although some of these government payments are typically disbursed in cash, there is an increasing trend to find digital forms of disbursements, which opens financial-inclusion opportunities. This scenario calls for remote account opening. Under an AML/CFT framework, government-to-person payments are considered as low risk, as the origin of the funds is known, amounts are low, and the beneficiaries are based on predefined criteria. Under this scenario, there is still the need to identify the beneficiaries and to strike a balance between the level of fraud tolerance that the program can bear and the positive outcomes of rapid customer onboarding. Additionally, the COVID-19 crisis has prompted the extensive use of digital financial services that increasingly use remote onboarding to open transaction accounts and other forms of financial services.

If permitted by the jurisdiction, a regulated FSP could rely on third parties (for example, agents) that satisfy the criteria described under FATF Recommendations 10 and 17 to conduct customer identification/verification at customer onboarding using a digital ID system, provided that the third party enables the relying regulated entity (FSP) to do the following:[28]

i. Immediately obtain the necessary information concerning the identity of the customer (including the level of assurance or confidence, where applicable). For example, the digital ID system could enable the prospective customer to assert identity to the relying regulated entity and the third party to authenticate the person's identity and provide information such as the person's name, date of birth, a government-issued unique ID number, or other attributes required to prove official identity to establish a business relationship in the jurisdiction.

ii. Take adequate steps to satisfy itself that the third party will make available copies or other appropriate forms of access to the identity evidence (documents, data, and other relevant information) relating to Recommendation 10(a) requirements upon request without delay. For example, the relying entity could take appropriate steps to satisfy itself that (1), as part of identity proofing and enrollment, the third party established a digital ID account for the identified person that contains adequate attribute evidence and other identity data and

BOX 4

MEASURES ADOPTED IN MEXICO IN RESPONSE TO COVID-19 FOR REMOTE ACCOUNT OPENING

The banking supervisor Comisión Nacional Bancaria y de Valores (CNBV) has enacted the following regulatory measures to facilitate account opening:

- Individuals can open accounts remotely, including obtaining credit. FSPs can decide the most suitable manner to ensure the accuracy of the identity documents and information provided by the customer.
- Legal entities will be able to open accounts remotely, including credit, under the following specific conditions:
  - Transactions below 30,000 UDIs *(Unidades de Inversión*, or investment units)
  - Credits below 60,000 UDIs
- Bank customers will be able to access additional products and services by validating biometrics against an independent and reliable source.
- Videocalls that last 30 seconds and allow for artificial intelligence can be used for remote account onboarding.

Source: CNBV

BOX 5

MEASURES ADOPTED IN RESPONSE TO COVID-19 ALLOWING NONOFFICIAL IDS FOR GOVERNMENT-TO-PERSON PROGRAMS

On April 1, 2020, the Bangko Sentral ng Pilipinas issued regulations in response to the COVID-19 pandemic that relaxed measures related to types of documents required for account onboarding. The new measures were adopted for only a limited term, comprising the duration of the enhanced community quarantine, until June 30, 2020.

Measures adopted apply to face-to-face and electronic transactions and involved the submission of official and nonofficial IDs by beneficiaries. This is aimed at facilitating the disbursement of government funds to beneficiaries with no existing FSP account.

Even under a low-risk scenario, FATF requires additional measures to mitigate the risks of money laundering and the financing of terrorism. The safeguards adopted in the Philippines for this period include (i) a transaction limit of $985 per day, (ii) ongoing monitoring, (iii) having beneficiaries declare that they have no official credentials, and (iv) requiring beneficiaries to reside in a location under enhanced community quarantine or community quarantine.

Source: Bangko Sentral ng Pilipinas

information, and that (2) the third party's authentication processes enable it to provide that information to the relying party upon request without delay.

i. Provide clear and consistent guidance on the use of digital signatures that enables acceptance of terms and conditions remotely.

Despite the existence of electronic templates to collect customer information for account applications made online or through digital devices, a customer's signature is required as a mechanism to accept the terms and conditions of the contract. Digital signatures replace wet signatures in performing three main functions: (i) identifying a person, (ii) providing certainty as to the personal involvement of that person in the act of signing, and (iii) associating that person with the content of a document. The purpose of various e-signature solutions is to offer technical means by which some or all of the functions identified as characteristic of handwritten signatures can be performed in an electronic environment. Certain techniques would rely on authentication through a biometric device based on handwritten signatures. In such a device, the signatory would sign manually, using a special pen, either

on a computer screen or on a digital pad. The handwritten signature would then be analyzed by the computer and stored as a set of numerical values that could be appended to a data message and displayed by the relying party for authentication purposes. Such an authentication system requires that samples of the handwritten signature have been previously analyzed and stored by the biometric device. Other techniques would involve the use of PINs, digitized versions of handwritten signatures, and other methods, such as clicking an OK box.[29]

Digital signature using public key infrastructure is a scheme that is used to authenticate the sender of an electronic document through a set of data and algorithms and is relevant to providing digital services—including traditional electronic payments—with the same level of legal validity, certainty, and security as face-to-face transactions, including traditional electronic payments. However, for e-signatures to produce all those benefits, they must meet certain conditions to strengthen confidence in, and general acceptance of, the new technologies. Those conditions include (i) legal recognition, (ii) having a certification mechanism and governance in place, (iii) allowing interoperability of certificates, and (iv) adequate security and data-protection legal safeguards. In addition, overcoming the anonymity challenge is another critical aspect of meeting AML/CFT requirements. Therefore, as the acceptance of e-signatures increases and documents are passed around virtually, the opportunity to screen and verify who is linked to the documents becomes more critical, as does the need for flexible options in authentication.

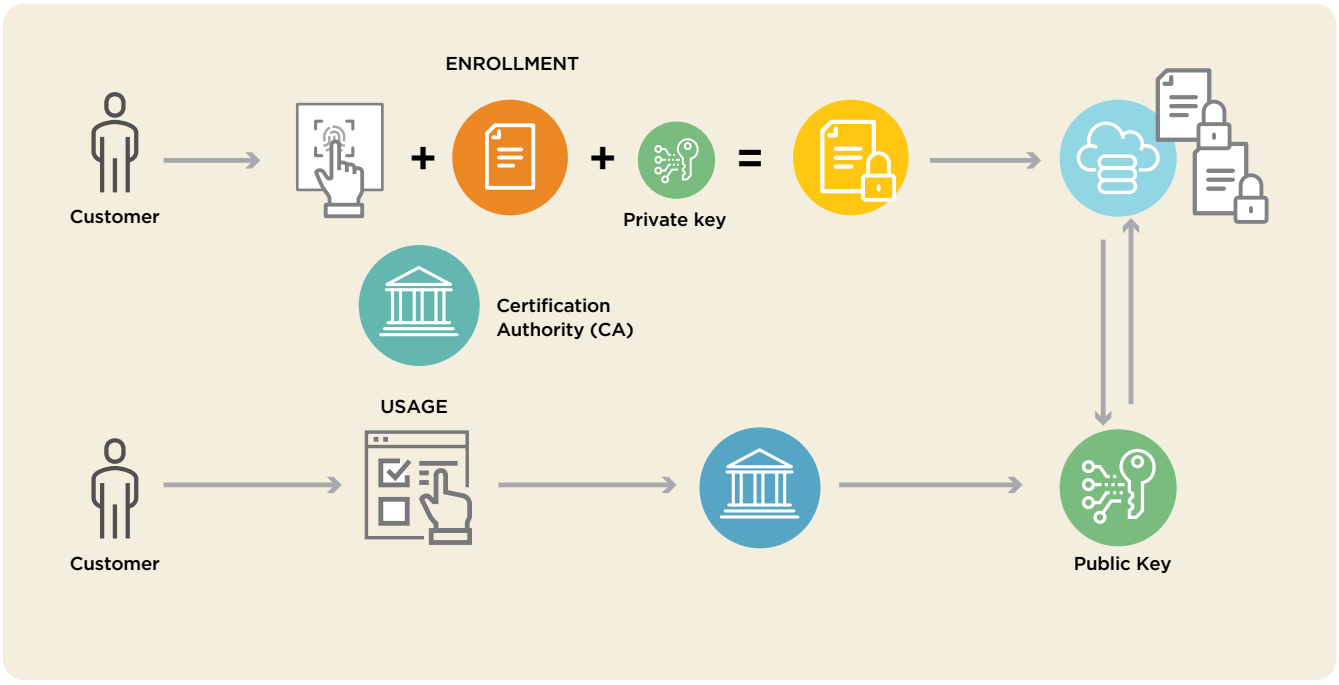
It is important that financial-sector authorities define the type of e-signature necessary to open an account and whether the type of signature required will vary with the type of product/service offered (for example, a transaction account versus a credit account). The process to issue the e-signature, as well as the role that financial institutions might play in this process as accredited issuers, is also something that needs to be defined in the legal and regulatory framework for FSPs. A key constraint on the issuance and usage of e-signatures is the need for individuals to present themselves in a certification office. During such processes, some data is collected, including ID data. However, digital signatures can be issued one time and used for multiple purposes.

MAS allows the identity of a customer to be verified through a document that the customer has signed with a secure digital signature using a set of credentials based on public key infrastructure issued by a certified certificate authority under the Electronic Transaction Act, when business relations are started under non-face-to-face scenarios and MyInfo is not used for account opening.[30]

j. Mitigate exclusion risks to ensure that no segment of the customer population is placed at a disadvantage.

Certain population groups may not have the evidence documents, such as a birth certificate, passport, or driver's license, required to obtain a digital ID in the first place (for example, refugees and displaced persons). The lack

FIGURE 12: Illustration of e-Signature Issuance Using Public Key Infrastructure



Source: Authors' elaboration

BOX 6

IRAQ SOLUTION FOR UNITED NATIONS CASH TRANSFERS TO REFUGEES

In 2018, Iraq hosted more than 283,200 refugees and asylum seekers, mostly coming from Syria. The United Nations High Commissioner for Refugees (UNHCR) and its partners have provided humanitarian assistance through cash transfers.

The Central Bank of Iraq supported flexible requirements for registration and the creation of "humanitarian wallets" or "temporary wallets" using simplified CDD processes. The simplified CDD framework recognized UNHCR's registration credentials as official identity to open an e-wallet. As a result, UNHCR could provide the full "survival minimum expenditure basket" for vulnerable refugees living outside camps. The amount of the transfers was fixed at ID 292,500 ($250) per month per family. In 2019, these arrangements were enhanced by the introduction of biometric authentication of identity for low-value transactions, strengthening risk-mitigation measures.

Source: United Nations High Commissioner for Refugees

of access to digital technology (mobile phones, smart phones, or other digital-access devices) or low levels of technology literacy, or a lack of coverage and/or unreliable connectivity, may exclude poor and rural populations. Customers with certain physical characteristics may be precluded from having their biometrics captured (for example, altered features due to aging or illness, an inability to read manual laborers' worn fingerprints, and disproportionate facial-recognition failures related to darker pigmentation, eye shape, or facial hair). Therefore, the legal and regulatory framework should provide alternative mechanisms to carry out CDD processes for those customer segments.

2.2 POLICY CONSIDERATION 2: *Consider the Full Range of Risks Associated with Use of Digital ID in the Financial Sector*

Digital ID systems, while promising significant benefits, also pose risks that must be understood and mitigated. As laid out in the FATF digital ID guidance, large-scale digital ID systems that do not meet appropriate levels of assurance pose cybersecurity risks, including allowing cyberattacks aimed at disabling broad swaths of the financial sector or at disabling the digital ID systems themselves. There are additional risks related to privacy and fraud or other related financial crimes. Risks related to governance, data security, and privacy also have an impact on AML/CFT measures. These risks vary in relation to the components of the digital ID system, but they can be more devastating than breaches associated with traditional ID systems due to the potential scale of the attacks.

Such risks threaten the financial sector as well as individual customers. The use of digital ID in the financial sector involves the collection and processing of personal data that can be made vulnerable or exposed to bad actors. Digital ID databases may include such personally identifiable information as a customer's name, age, height, date of birth, and biometric information, such as fingerprints or iris scans. Misuse of personal data and breaches in security can result in a lack of trust in the ID system and the financial sector.

2.2.1 Implementing Approaches for Policy Consideration 2

a. Establish robust governance arrangements for the collection, use, and management of a customer's personal data.

While there needs to be a robust data-protection and privacy framework at the national level, the preservation of the confidentiality, accuracy, and integrity of the data falls on the multiple stakeholders that access data linked to the digital ID system. Therefore, there needs to be clear guidelines for the various data controllers, including the IDSP and FSPs, on the collection, use, management, and disclosure of a customer's personal data. The role and definition of a data controller should be specified, in addition to appropriate measures, at the level of both an FSP and the digital ID provider to ensure that a customer's personal data is used only for the specific purpose mentioned to the customer. Ecosystem-wide trust frameworks must establish and regulate governance arrangements for digital ID systems. Such guidelines for the digital ID provider and FSPs that access a customer's personal information for verification purposes will be integral to ensuring that adequate security measures and safeguards are in place to preserve customer privacy and prevent unauthorized access, data loss, or corruption and abuse.

b. Encourage a privacy-by-design approach in the architecture of information systems, business process, and networked infrastructure used within the financial sector.

The privacy-by-design approach envisages building privacy into all stages and architecture of information systems, business processes, and networked infrastructure related to the digital ID system. It takes on a proactive, preventive approach to mitigating data vulnerabilities and protecting customer privacy. The protection of personally identifiable data should be ensured by default across the full life cycle of digital ID systems and their use in the financial sector. Protecting an individual's personal information should be a core component built into all stages of technical design, governance architecture, and operational processes or practices.

c. Conduct a data-protection impact assessment.

Financial-sector regulators can conduct, or ask the data controllers of the e-KYC or collaborative CDD solution to conduct, a data-protection assessment. The assessment would consider existing data-protection guidelines and standards, to understand their compatibility across sectors and their impact on ensuring the privacy of customer information. Based on the assessment and potential challenges identified, financial-sector regulators should implement appropriate risk-control measures by designing systems, protocols, and procedures that meet data-protection and privacy regulations pertaining to their jurisdiction and develop requirements for data-sharing contracts between FSPs, IDSPs, and other relevant entities that may need to be established. The design framework pertaining to data protection should clearly describe the various components of the collaborative CDD system or e-KYC solution, the roles and responsibilities of different stakeholders, how and which data is to be collected, the liability of system participants and recourse for customers and relying parties, the circumstances in which data can be shared, the correction of inaccurate data attributes, and how inclusion and nondiscrimination will be maintained.[31] In conducting such assessments it is important to consider the following aspects:[32]

i. Data cycle (data quality, processes, and data storage)
   a. Type of data
   b. Volume of data
   c. External and internal users and data processors

ii. Evaluation of compliance (legal and operational aspects)
   a. Procedures
   b. Infrastructure (system architecture, databases, networks, devices, connectivity)
   c. Services

iii. Risk analysis

iv. Action to implement areas of improvement

d. Encourage data minimization, whereby FSPs collect only the minimal amount of data required for the intended purpose. Data minimization also applies when allowing third parties to access data for verification purposes.

Implement mechanisms to minimize the amount of personal data collected for each use case. The collection of personal information must be limited simply to what is necessary for proving customer identity for a specific purpose. Most privacy and data-protection frameworks embrace the concept of data minimization or proportionality in that only the minimal amount of data should be collected based on what is adequate and relevant, and limited to what is necessary in relation to the intended purpose. It is critical for digital ID systems to evaluate the minimum data attributes that are necessary to identify and/or verify the identification of the customer. To implement rules related to data minimization, a privacy-by-design approach is desirable, so that the technology is designed to prevent abuses by users. In addition, specific scenarios should be considered, such as data from minors, or other categories of data subjects that might require additional safeguards. Encourage minimal data disclosure through authentication protocols that provide, for example, a yes-or-no confirmation of a claimed identity.

FATF allows different forms of document retention, including electronic storage, which includes the following:[33]

i. Scanning the verification material and maintaining the information electronically

ii. Keeping electronic copies of the results of any electronic verification checks

iii. Merely recording reference details on identity or transaction documents

For digital ID scenarios, the FATF digital ID guidance encourages service providers to have such information at the disposal of the regulatory authorities to serve as evidence of the ID proofing process.

Finally, FSPs should be required to establish a system by which data collected and held for a specific purpose is archived, anonymized, or deleted once that purpose has expired.

e. Mitigate fraud-related threats.

Digital ID systems and e-KYC solutions used by FSPs might be susceptible to fraud and abuse. Given that they rely on official identity documents, any weaknesses in the reliability of that documentary evidence can have a

domino effect on the risks posed by digital ID systems. The "reliability, independence" requirement of ID documents can be undermined by identity theft or the counterfeiting of official identity documents (impersonation), including where official identity documents either lack advanced security features to prevent tampering or counterfeiting, or are issued without adequate identity proofing. For example, a customer might use the credentials of another customer to obtain a financial product or service especially when branchless banking channels are used and the technological infrastructure to accept digital ID is inadequate. The "reliability, independence" requirement can also be undermined by combining real (usually stolen) and fake information to create a new (synthetic) identity for a person that does not exist in the real world. These synthetic IDs can then be used to obtain credit cards or online loans and to withdraw funds and then abandon the account shortly thereafter. Below are other examples of fraud:[34]

Credential stuffing (also referred to as breach replay or list cleaning): A type of cyberattack in which stolen account credentials (often from a data breach) are tested for matches on other systems. This type of attackcan be successful if the victim has used the same password (that was stolen in the data breach) for another account.

Phishing: A fraudulent attempt to gather credentials from unknowing victims using deceptive emails and websites—for example, a criminal attempt to trick its victim into supplying names, passwords, government ID numbers, or credentials to a seemingly trustworthy source.

Man-in-the-middle or credential interception: Attempts to achieve the same goal as phishing and can be tool to commit phishing but does so by intercepting communications between the victim and the service provider.

PIN code capture and replay: Involves capturing a PIN entered on the keyboard of a PC using a key logger and, without the user noticing, using the captured PIN to access services when the smartcard is present in the reader.

For the purposes of illustration, table 5 sets out these risks and presents some strategies for mitigating threats to identity proofing and enrollment processes under the NIST guidelines.

The risk that a "fake" digital ID was obtained under intentional false premises can be mitigated by having a higher identity assurance and authentication level for accounts that permit high-value transactions—that is, by encouraging multifactor authentication for transactions above a threshold limit. Consider factors that provide higher levels of assurance for higher-risk scenarios. Relying on factors based on knowledge have proven to be less reliable than factors based on inherence or possession. The adoption of several factors would allow for broader adoption in different population segments. Recently, authentication factors based on inherence or possession have proven to be more robust than those based on knowledge.[36] FIDO (Fast Identity Online) authentication has emerged in recent years as a standardized way to combine possession- and inherence-based factors in any mobile device, laptop, or PC.[37]

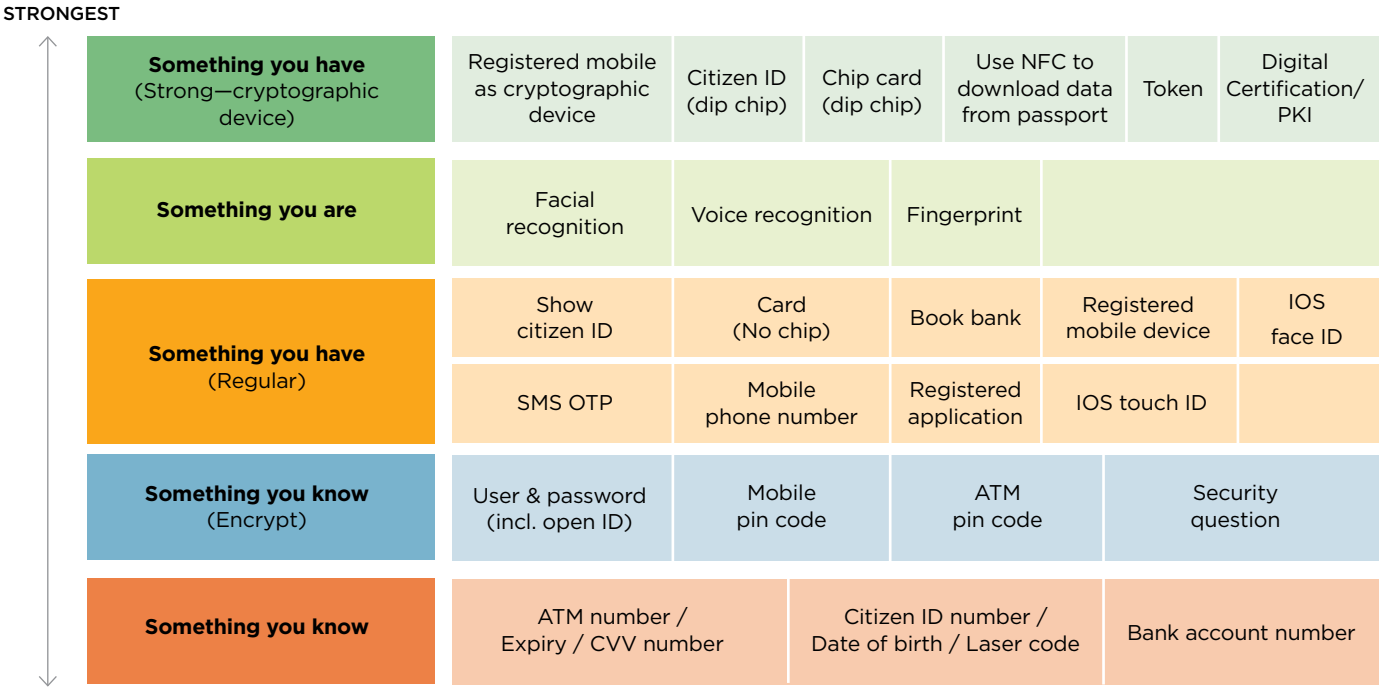
- Consider the exclusion risks associated with applying biometric authentication to a large customer base and how these might uniquely affect the financial sector.
- Encourage FSPs to use privacy-enhancing technologies, such as data-centric encryption, tokenization, and multifactor authentication.

Privacy-enhancing technologies comprise measures that protect privacy by eliminating or reducing the collection of personal data, preventing unnecessary or undesired processing of personal data, and facilitating compliance with data-protection rules without losing the functionality of the data system.[38] Such technologies—data-centric encryption, tokenization, and multifactor authentication—should underpin the CDD process that FSPs undertake.

TABLE 5: NIST—Identity Proofing/Enrollment Risk-Mitigation Strategies[35]

Type of Risk	Description	Potential Risk-Mitigation Strategies
Falsified identity proofing evidence	An applicant claims an incorrect identity by using a forged driver's license.	IDSP/FSP validates physical security features of the presented evidence. IDSP/FSP validates personal details in the evidence with the issuer or another authoritative source.
Fraudulent use of another's identity	An applicant uses a passport associated with another individual.	IDSP/FSP verifies identity evidence and biometrics of the applicant against information obtained from the issuer or another authoritative source.

FIGURE 13: Examples of Authentication Factors Used in Thailand



Source: Thailand ID reform

TABLE 6: Comparison of Authentication Assurance Levels in the United States and European Union

US NIST 800-63(b)		EU eIDAS	
Level 1	Provides some assurance that the individual claiming identity for account authorization controls an authenticator(s) bound to the customer's account. Authenticator factors are low, and multifactor authentication is optional (for example, biometrics alone).	Low	Provides a limited degree of confidence in the claimed identity of a person.
Level 2	Provides high confidence that the claimant controls authenticator(s) bound to the customer's account. It requires multifactor authentication (either multifactor or two single-factor) that incorporates the approved cryptographic techniques and information security controls at a moderate baseline (for example, biometrics plus a device).	Substantial	Provides a substantial degree of confidence in the claimed or asserted identity of a person.
Level 3	Provides very high confidence that the claimant controls authenticator(s) bound to the subscriber's account. Level 3 requires multifactor authentication that uses both a hardware-based authenticator and an authenticator that provides verifier impersonation resistance, based on proof of possession of a key through an approved cryptographic protocol. Claimants must prove possession and control of two distinct authentication factors through secure authentication protocol(s), using approved cryptographic techniques.	High	Provides a higher degree of confidence in the claimed or asserted identity of a person than the substantial assurance level.

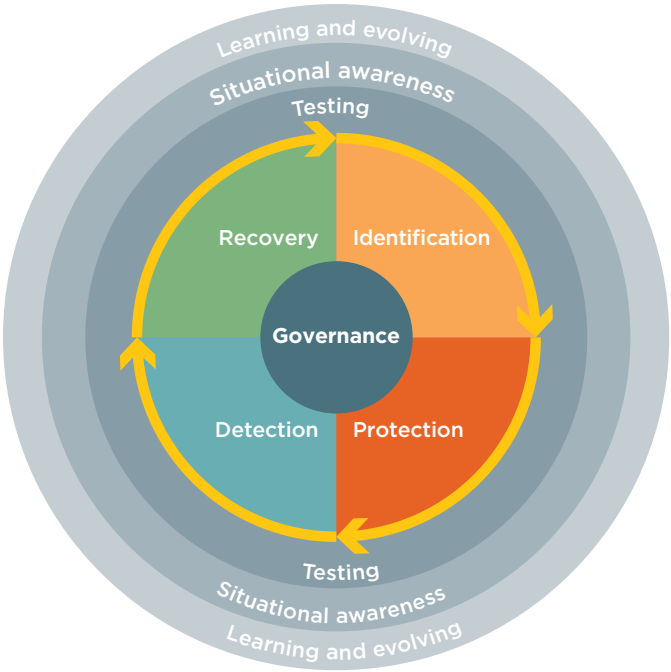
f. Establish guidelines on legal and technical requirements for cyber resilience and cyber incidents.

To maintain the cyber resilience of digital ID systems and banking or payment systems used by FSPs, it will be essential to adopt a risk-management framework on cybersecurity applicable to the financial sector, to enable IDSPs and FSPs to preempt cyberattacks, respond rapidly and effectively to them, and achieve faster and safer recovery if attacks succeed, will be essential.

Typically, cybersecurity has been covered under operational risks, but the rapid evolution of digital financial services, coupled with more sophisticated cyberattacks, has prompted the need to develop a specific cybersecurity framework separate from operational risk. The Financial Stability Board provided guidance on key elements to build cyber resilience. Guidance from the CPMI and the International Organization of Securities Commissions (IOSCO) on cyber resilience for financial market infrastructures outlines five primary risk-management categories and three overarching components that should be addressed across a financial market infrastructure's cyber resilience framework. The risk-management categories are governance, identification, protection, detection, and response and recovery. The overarching components are testing, situational awareness, and learning and evolving.

Guidelines on legal and technical requirements and liabilities could be developed based on the cyber resilience framework developed by CPMI-IOSCO. This should include continuity planning and established processes for crisis response by IDSP and FSPs. To operationalize the guidelines at the provider level, FSPs should be required to identify a data-security officer and follow procedures for prompt response to minimize the consequences of a cyber incident.

FIGURE 14: CPMI-IOSCO Framework for Cyber Resilience of Financial Market Infrastructures[39]



g. Establish protocols for incident responses when there is a data breach.

The incident response protocol should require FSPs to notify customers when there has been a data breach, which includes the bare minimum information that should be included in that notification from the FSP to the governance body of a CDD collaborative solution. Data breaches can result from multiple sources, both intentional and accidental, including employees who fail to follow proper procedures, hackers who gain access to inadequately protected databases, and thieves who steal inadequately secured portable devices. The incident responses should also address the different levels of data-breach notification, including the regulatory authority, other existing cyber incident data-sharing platforms, and, ultimately, the customer, including the maximum time period for customer notification and the minimum information that should be included in that notification from the FSP to the customer.

Canada Pan-Canadian Trust Framework

In 2014, the Digital ID and Authentication Council of Canada was launched as a public-private effort, and in 2016, the Pan-Canadian Trust Framework Overview was published to enable public- and private-sector stakeholders to work collaboratively to safeguard digital identities by standardizing processes and procedures. In 2017, as part of components under the Pan-Canadian Trust Framework, the Digital ID and Authentication Council of Canada and Identity Management Steering Committee collaborated to develop conformance standards criteria for trust framework components.

European Union's Data Breach Framework

The European Union's General Data Protection Regulation requires the supervisory authority to be notified of any personal data breach "without undue delay and, where feasible," within 72 hours of becoming aware of it, "unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons." The notification must include certain data about the breach, such as: (i) categories, (ii) the approximate number of data subjects concerned, and (iii) the expected consequences of the breach. The data subjects affected must be notified if the breach "is likely to result in a high risk to the rights and freedoms of natural persons," and the notification must contain the same data that was sent to the supervisory authority.

2.3 POLICY CONSIDERATION 3: Provide for Consent Mechanisms for Users to Maintain Control over Data Collected for Use within the Financial Sector

When using a digital ID, although the context differs from one jurisdiction to another, it is important to understand the legal basis for the collection and use of personal data by FSPs and third parties offering solutions related to KYC or digital ID. Regardless of whether a data-protection legal framework is in place or not, customers should be able to authorize the use of their personal information by third parties. Consent means that individuals knowingly register for and use the digital ID with knowledge of what personal data will be captured and how it will be used. Obtaining consent to how FSPs will share and use data linked to a customer's digital ID is critical to the delivery of financial services. In addition to customers having control over their data, from a proactive privacy-by-design perspective, FSPs should obtain customer consent at the outset of the relationship, given that personal data on financial transactions can be leveraged to generate credit scores and build customer profiles for the more efficient delivery of services.

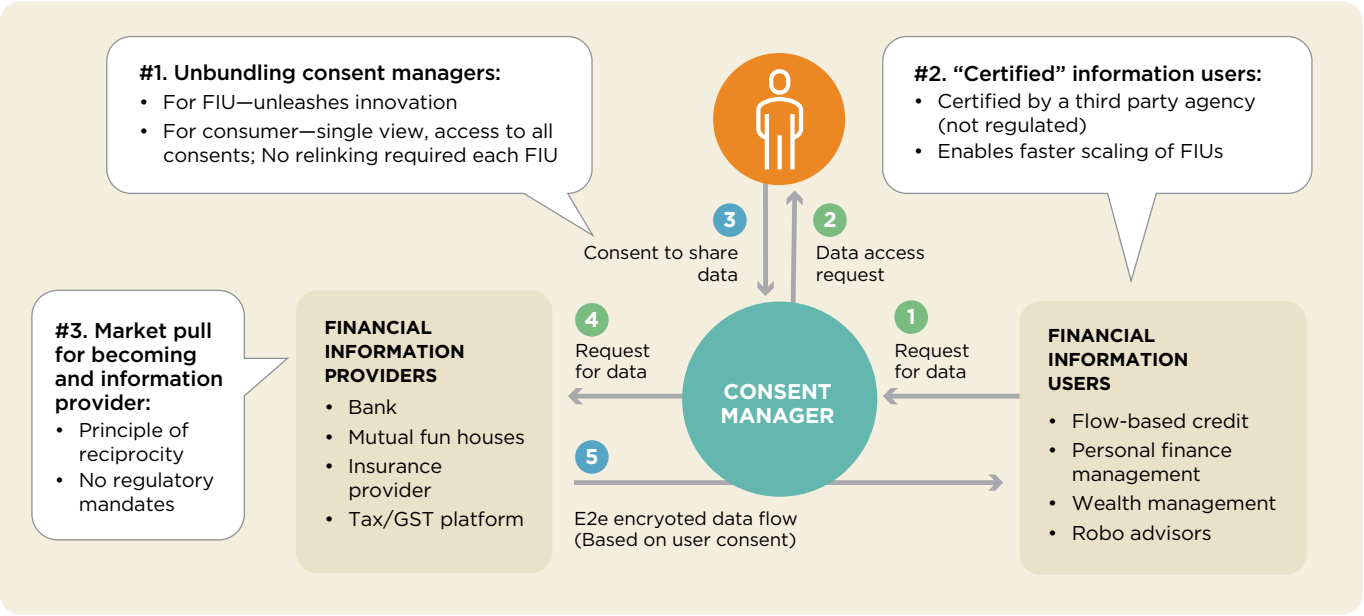
Several governments have implemented or are in the process of implementing "open banking," which will require specified types of FSPs to share product and customer data with third parties (with customer consent). This customer data is typically shared through application programming interfaces (APIs) between two or more unaffiliated parties.[40] The implementation of open banking allows customer account data to be accessed that could contribute to KYC solutions, including collaborative CDD and KYC conducted by a relying party. These scenarios call for adequate mechanisms for the consumer to provide consent.

2.3.1 Implementation Approaches for Policy Consideration 3

a. Build easy-to-understand consent mechanisms.

This means that a message should be easily understandable for the average person and not only for lawyers. Controllers cannot use long privacy policies that are difficult to understand or statements full of legal jargon. Consent must be clear and distinguishable from other matters and provided in an intelligible and easily accessible form. This consideration essentially means that information relevant for making informed decisions about consent may not be hidden in general terms and conditions. A controller must ensure that consent is provided on the basis of information that makes it easy for data subjects to identify who the controller is and to understand what they are agreeing to (notice). Moreover, consent should enable consumers to know the type of data being collected and for what purpose prior to authorizing its processing and each time final users request access to a customer's data (informed consent). Depending on the nature of the request (for example, account opening versus monitoring), the type of data to be accessed would also differ, and the mechanism should be allow different levels of authorization (granularity). Figure 16 shows the consent mechanism deployed in India.

FIGURE 15: Consent Mechanism Used in India



Source: Data Empowerment and Protection Architecture, iSPIRT Foundation, 2021

b. Data controllers should be able to prove the capture of consent and expiry of consent.

A key element of consent is control by the data subject. The European Data Protection Board states, "Accordingly, consent will not be considered to be free if the data subject is unable to refuse or withdraw his or her consent without detriment. The notion of imbalance between the controller and the data subject is also taken into consideration by the General Data Protection Regulation (GDPR)." In the view of the European Data Protection Board, when consent is obtained via electronic means through only one mouse click, swipe, or keystroke, data subjects must, in practice, be able to withdraw that consent equally as easily. Where consent is obtained through the use of a service-specific user interface (for example, via a website, an app, a log-on account, the interface of an Internet of Things device, or by e-mail), there is no doubt that a data subject must be able to withdraw consent via the same electronic interface, as switching to another interface for the sole reason of withdrawing consent would require undue effort. Furthermore, the data subject should be able to withdraw his or her consent without detriment. This means, among other things, that a controller must make withdrawal of consent possible free of charge or without lowering service levels. In this context, the mechanism developed should be auditable, and the consent provided should be traceable, allowing for data controllers' accountability.

c. Establish a mechanism to handle disputes.

KYC and ID verification service providers should access, process, and retain only the personal data necessary for the provision of their services, with the explicit consent of consumer. While regulations established in several countries effectively cover the aspect of consent, in practice, data subjects might also face situations where their information has been used without their consent. Allowing a process for consumers to dispute the unauthorized use of their ID information can also help investigations of ID theft and fraud. The mechanism to handle disputes is often provided by a specialized unit or center set up to resolve consumer/data subjects claims. Disputes might also involve errors in data or decisions made based on wrongful data. This unit could be established under the service provider itself (for example, MyInfo in Singapore) or through a coordinated mechanism in the financial institutions.

2.4 POLICY CONSIDERATION 4: *Collaborate and Engage with the Private Sector to Develop e-KYC Solutions, Including Collaborative CDD, and Monitor Emerging Technologies Relevant to ID Verification in the Financial Sector*

By developing or upgrading the digital ID infrastructure and ensuring inclusive access for all citizens and residents, governments play a critical role in bridging the identity gap and nurturing an ecosystem crucial for achieving digital and financial inclusion. Digital ID can serve as a core public-sector platform on which the private sector can build solutions that meet the growing needs of the financial sector and beyond. The involvement of the private sector, sharing their insights and practical expertise, as well as delivering change, will be beneficial in developing a cost-effective and robust ID-management system that keeps pace with market changes.

Financial-sector authorities may consider partnering with private-sector entities (such as MNOs, information technology service providers, and others) to leverage their extensive reach and network assets or technological expertise. Governments have the opportunity to engage with private-sector entities at several points along the ID-management life cycle. (See appendix C.) Therefore, financial-sector authorities would need to identify if there are opportunities for, and the benefits of, using private-sector solutions to enhance ID solutions. This is especially true for technology companies that supply ID credentials, authentication solutions, consent dashboards, and user-controlled data vaults that can be leveraged by FSPs.

The ability of the private sector to build solutions that meet the needs of the financial sector and the regulator depends on the state of the national ID infrastructure. To enable a private-sector role, the ID platform should ideally be

- ***Comprehensive*** (for example, it covers a critical mass—at least 80 percent—of the population);
- ***Trusted*** (that is, it is able to establish an identity that is unique, secure, and accurate); and
- ***Query-able*** (that is, an API is in place to allow private-sector entities to query the ID platform when onboarding an individual to a digital ID–linked service).

If the national ID platform is not sufficiently advanced, the private sector may be engaged to support enrollment and to build out the necessary infrastructure, such as open APIs. This is detailed in the implementation approaches below.

BOX 7

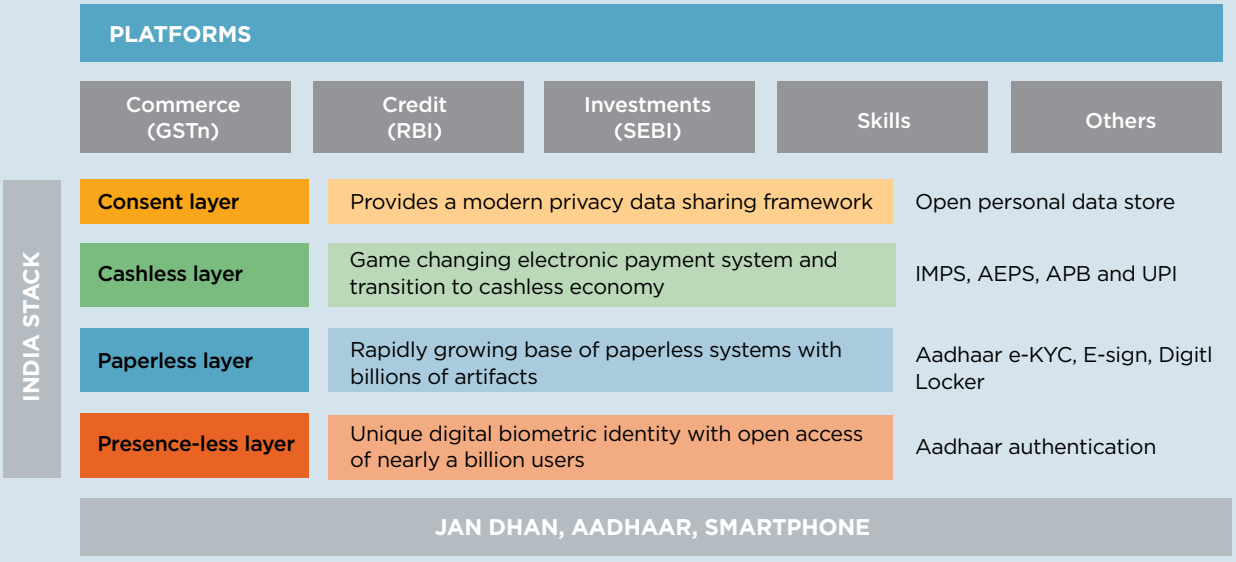
INDIA STACK

India Stack is a set of APIs that allow governments, businesses, start-ups, and developers to utilize a unique digital infrastructure. The stack involves four distinct technology layers: (a) a presence-less layer that includes Aadhar, the universal biometric digital identity; (b) a paperless layer that links digital records with the individual's identity; (c) a cashless layer that helps with the democratization of payments through a single interface to all bank accounts; and (d) a consent layer that allows data to move freely and securely.

Signatures in electronic form have been recognized by law in India since 2000, when the Information Technology Act was passed. Aadhaar eSign is an online e-signature service that allows an Aadhaar holder to sign a document digitally and forms the core of the paperless layer of the India Stack. (See figure.) It is integrated into service-delivery applications via an API and needs an individual to have an Aadhaar card and a mobile number registered with Aadhaar to function. eSign APIs are designed to interact with one or more eSign online e-signature service providers, supporting interoperability.

DigiLocker, another ancillary service, was launched in 2015 and is intended to facilitate the ability to save and share documents. It's a secure cloud-based platform that makes it easy to issue, share, and verify critical lifelong documents or certificates—from driver's licenses to university results. It currently has over 51.24 million registered users, 4.2 billion issued authentic documents, 674 issuer organizations, and 142 requestor organizations.* The sustainability of this solution will be tested with having all major government and nongovernment organizations and agencies on board. The government has issued thresholds to allow certain private players to obtain licenses that would allow them to operate digital lockers.

India Stack: Powering digital services platforms



Source: iSpirit

*https://digilocker.gov.in/public/dashboard#!

In some countries, there has been a noticeable effort by government agencies responsible for the ID systems to develop ancillary services. For example, in India, the services e-Sign and Digital Locker (DigiLocker) both rely on Aadhaar to offer additional services, such as an e-signature service and an online document-storage service, respectively. (See box 7.)

Another point to note is that technology is constantly evolving—and policy needs to evolve with it. Policy makers need a way to keep up to date on new and emerging technologies and standards, as well as to assess their appropriateness for use in ID systems. This requires modernizing legacy policies, laws, and regulations to support the use of new ID technologies in a way that protects the rights of individuals and minimizes the capacity of new technologies to cause individual or societal harm.

2.4.1 Implementation Approaches for Policy Consideration 4

a. Establish a platform (such as a working group) for partnership and dialogue between public- and private-sector stakeholders to enable a shared vision and maintain ongoing discussion of key topics.

Close collaboration with, and direct action from, the private sector can achieve tangible solutions and improvements through the sector's insights and expertise. The financial-sector regulator should establish a platform, potentially in the form of a working group, for public and private stakeholders to collaborate. The working group can discuss issues such as the state of the market, financial-sector vulnerabilities, reaching underserved segments, and concepts to enhance functionality and synergies, including for cross-border payments

The purpose of the working group would be to ensure that emerging digital ID ecosystems cater to the needs of the financial sector and the specific needs of various customer groups—including those that are marginalized and underserved. The working group can consider issues such as 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.

b. Consider the supportive role that MNOs can play in ID enrollment and verification.

As previously mentioned, a key pathway to financial inclusion in many developing nations is via mobile wallets, as people don't have access to traditional brick-and-mortar banks. While identity is critical to gaining access to mobile connectivity and a range of financial services deployed over mobile, mobile technology can be well positioned to enable digital ID. The GSMA Digital Identity Program[41] has been advocating for and raising awareness of mobile-enabled digital ID by working with mobile operators and governments to demonstrate the opportunities, address the barriers, and highlight the value of mobile as an enabler of digital ID.

MNOs have been useful in supporting governments in enrolling citizens in national ID registries, as in Nigeria (see box 9), or in digital birth registries, as has been illustrated in Pakistan and Tanzania. MNOs have also been useful in supporting remote ID verification—against a government registry of smartcards, tokens, or biometric data—for the purpose of validating ID when accessing a third-party ser-

BOX 8

PUBLIC-PRIVATE COLLABORATIONS

Australia: Fintel Alliance in Australia is a public-private partnership led by Australia's AML/CFT regulator, AUSTRAC. It brings together financial intelligence units, law-enforcement agencies, and FSPs to share information about criminal behavior and to launch joint investigations into specific priority crimes and criminals.* The intention is to collaborate on investigative and intelligence projects to address specific priority crimes and challenges by viewing patterns.

Singapore: A utility committee of local and foreign banks led by the private sector and working closely with MAS explored the establishment of a KYC utility that would support both identification and verification and beneficial ownership checks in relation to corporate customers. This resulted in the corporate customer utility project of the Association of Banks in Singapore. However, it was found that project costs were high, due to the need to migrate away from legacy systems, highlighting that, in the short term, costs might actually increase before they decrease.**

*Expanding the Capability of Financial Information-Sharing Partnerships, Nick J Maxwell, 2019.Maxwell (2019)

** https://i-kyc.com/the-failure-of-the-kyc-utility-project-in-singapore-a-practical-view/

vice. One example of this is the access to credit granted to owners of informal small businesses in Nigeria using the mobile delivered economic ID which is based on data generated by the usage of mobile phone products and services; financial transactions (including bank or savings deposits); online and digital profiles used to market products and services; buying or selling items on credit; and utility payments.[42]

c. The private sector should have the ability to build on top of, or supplement, foundational infrastructure and resources.

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 online connectivity.

BOX 9

USING MNOS TO SUPPORT ID ENROLLMENT IN NIGERIA

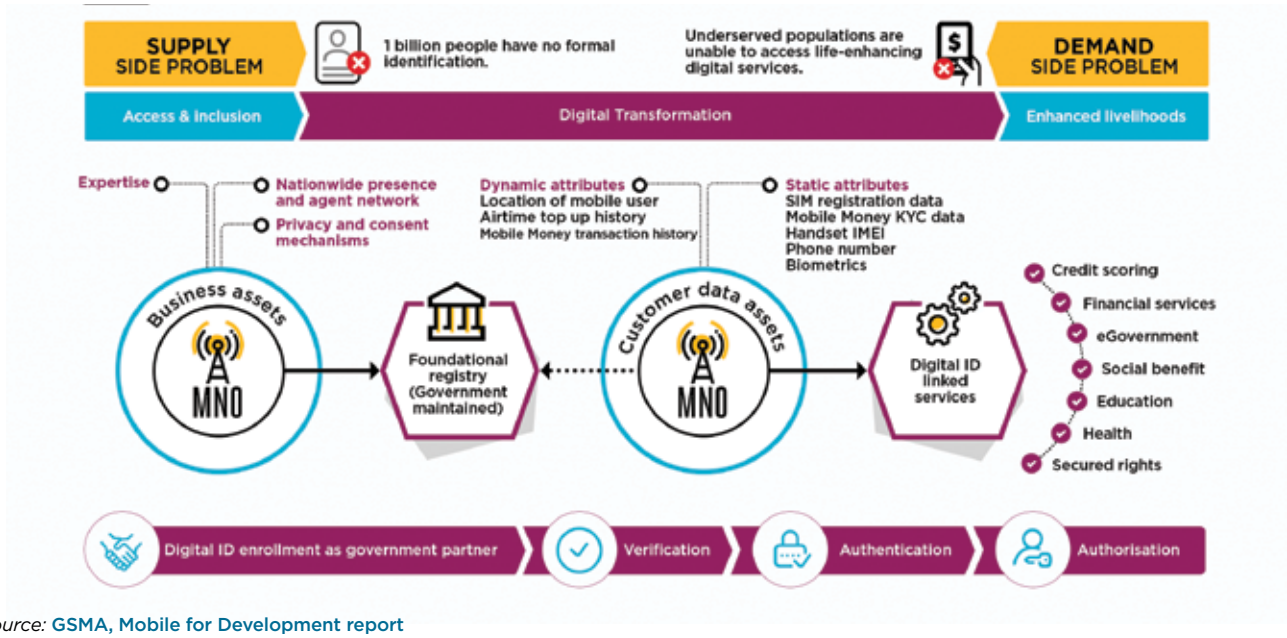
After a three-year consultation, the Federal Government of Nigeria formally licensed 173 private-sector organizations, including all MNOs, to act as official enrollment agents into the National Identity Database on behalf of the National Identity Management Commission. To qualify as agents, all bodies needed to satisfy a series of threshold conditions. (See details here.)

This enables MNOs to leverage their nationwide retail locations to reach millions of Nigerians and register them onto the new national digital ID platform (earning a fee from the government for each successful enrollment).

Once many more Nigerians acquire their national ID number, they will be able to be included digitally and financially in their own names, as they would be able to register SIM cards and open mobile-money wallets. This is particularly significant today, during the COVID-19 pandemic, when remote ID verification is increasingly relevant.

Source: GSMA and Vanguard

FIGURE 16: MNOs Can Play Various Roles in Supporting Digital ID Ecosystems



Source: GSMA, Mobile for Development report

BOX 10

SWEDEN'S BANKID

It is estimated that 7.5 million Swedish citizens currently use BankID, a form of electronic identification issued by a consortium of Swedish banks. First issued in 2003, it can be used by members of the public, authorities, and companies. Citizens can use their BankID for identification and as a means of digital signature for signing transactions and documents remotely. Its usage rate is over 90 percent, and it has been adopted by the government, municipalities, banks, and companies to validate identity. In accordance with Swedish law, as well as with laws in the European Union, a signature via BankID is legally binding.

Source: Grönlund, A., "Electronic Identity Management in Sweden: Governance of a Market Approach," *Identity in the Information Society,* July 2010.

BOX 11

GRAVITY'S SELF-SOVEREIGN DIGITAL ID-MANAGEMENT SOLUTION

Gravity is building a self-sovereign digital ID-management solution that is intended to be sufficient for customer identification and verification. Currently piloting in Kenya, the service allows users to verify their identity through a range of means that contribute to an identity score, including using a customer's social network to confirm that the data is true and accurate. Gravity users can increase their score by getting a government official to confirm data (for example, having a police officer attest to having reviewed the customer's government-issued ID card). These inputs are used to create the customer's identity score.

The **identity score increases with the quality and quantity of verifications received**, accounting for the different levels of trust placed in the various actors within a community or an ecosystem (GSMA 2017). The authenticity of the verifications is guaranteed by leveraging blockchain technology and peer-to-peer certifications. Gravity has a pay-per-data revenue model: services providers are charged a fee to access customer data for identification. A part of the fee is returned to the customer as compensation for the collection and use of personal data. Gravity is currently collaborating with a nongovernment organization in northern Kenya to implement a self-sovereign digital ID education wallet for refugee students that would allow the organization to track student attendance and course completion better.

Source: Lyman, Timothy, Louis de Koker, Chrissy Martin Meier, and Mehmet Kerse, *Beyond KYC Utilities: Collaborative Customer Due Diligence for Financial Inclusion,* CGAP Working Paper (Consultative Group to Assist the Poor, August 2019)

In a few countries with reliable and universal coverage of official ID, banking and other industry consortiums have developed digital capabilities that are built on top of these official IDs and leverage the value of them. These services seek to offer an open and general-purpose authentication that can be used to avoid the need for dedicated passwords and security credentials.

Another method of leveraging existing infrastructure is the use of algorithms contained in the SIM card allows for encrypted communication between the customer and the network. For authentication, the authenticating body generates a random sequence of numbers that are sent to the customer's mobile; the sequence is the customer's public key. The public and private keys, along with the authentication algorithm contained in the SIM, verify the customer. This method of authentication can be applied to high-value, high-risk transactions.

d. Encourage the use of collaborative platforms and APIs to support identity management, including interoperability, efficient data exchange, and data portability.

The use of collaborative approaches to reduce the cost and burden of conducting CDD is beginning to gain traction. Private-sector companies as well as the public sector,

BOX 12

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 ID services driven by MNOs globally and delivered as a federated identity framework.

Mobile Connect leverages the reach and inherent trust in the mobile network. 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. MNOs 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 ID, 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.

Source: GSMA

together and separately, are pooling resources and leveraging new approaches to help FSPs meet their CDD obligations. They are conducting customer identification and verification, establishing beneficial ownership, and monitoring transactions for any suspicious behavior that may signal money laundering or the financing of terrorism.[43]

There are many types of collaborative CDD, and they can vary greatly in form and functionality. Data sharing is one of the key areas for the use of collaborative CDD in the form of shared KYC registries or APIs. Over the last few years, we have seen a sizable shift in the role of APIs with the recognition that preexisting functionality needn't always be reinvented. This has been used for some time in the payments landscape for providing payment functionality to applications. APIs essentially democratize functionality by making it openly available. However, the ability to use APIs effectively will depend in part on whether the ID infrastructure is built to allow for this. For APIs to function, an array of different policy initiatives across jurisdictions have emerged, ranging from direct regulatory requirements (such as in Australia, the European Union, Mexico, Turkey, and the United Kingdom) to market coordination (Hong Kong and Japan), guidance (Singapore), and industry-led initiatives (Colombia and New Zealand).

It's not just the style of intervention that differs, but also the scope, with substantial variations across the following characteristics:

- The scope of entities participating into the CDD platform
- Products and services that justify access to the CDD platform
- What information should be accessible by third parties, with the customer's consent (that is, data-sharing agreements)
- The kind of operations for which the CDD collaborative platforms can be used—that is, identification, verification, beneficial ownership, monitoring transactions, and so on

APIs can reduce the cost of compliance and the rates of human error while increasing productivity and introducing potentially a better customer onboarding service with shorter onboarding times. However, user data breaches can cause severe customer-protection and reputation concerns. The security environment changes constantly, and data-hacking techniques have become supercharged with the power of cloud computing. Recent research has shown that the average application has a staggering 26.7 serious vulnerabilities.[44] Regulators should have guidelines in place (such as outsourcing rules) that ensure that companies monitor, maintain, and patch their code and libraries constantly to ensure that user data is secure. The human element of data security also needs to be considered, by periodically reviewing access protocols, ensuring that staff are adequately trained, and taking other steps.

Layers such as OpenID Connect (an interoperable authentication protocol) is built on top of the OAuth 2.0 protocol,[45] allowing clients to verify the identity of the end user based on APIs. FSPs can use the identity API to get an access token that will then allow them to access user data from a service that supports OAuth2 access (such as Google or Facebook). It also allows participants to use optional features, such as encryption of identity data.

BOX 13

STRIPE IDENTITY: HANDLING VERIFICATION WITH THE API

Stripe is a technology company that first became well known as a payments aggregator. It has added to its services the ability to verify users' identities with a "few lines of code." While this has not been corroborated, platforms with accounts created using the API can provide Stripe with information about their users that is necessary for CDD verification purposes.

Before enabling charges and payouts for a connected account, Stripe collects certain information that varies based on the following characteristics:

- The country in which the connected account is located
- The capabilities the connected account needs
- Whether the business entity is a company or an individual

Connect platforms collect the required information from users and provide it to Stripe. This may include personal information and a scan of a government-issued ID. Stripe then conducts the verification based on each country's restrictions and regulations.

Source: https://stripe.com/docs/connect/identity-verification-api

BOX 14

THE MANSA PLATFORM

The Mansa platform was launched in 2018 by the African Export-Import Bank (Afreximbank) to provide a collaborative CDD solution. Afreximbank is a pan-African multilateral financial institution with the mandate of financing and promoting intra- and extra-African trade. The solution is intended to be a repository of CDD data for FSPs, corporate entities, and small and medium-sized enterprises and was developed to address the perceived risk of doing business in Africa and with Africans.

The platform aims to create a single source of the primary data required for the conduct of CDD on African entities engaged in trade and is available to both FSPs and companies. It is said to "*store information needed to conduct ML/FT evaluations with the objective to make it cheaper and easier for international FSPs to onboard African banks and businesses of all sizes*." The platform is named after Mansa Musa, the ruler of the West African Malian empire in the 1300s, who was responsible for opening trade across Africa by establishing Timbuktu as a commercial, cultural, and religious centre.

The platform has two types of patrons—contributors and users. Contributors are non-fee-paying entities that voluntarily upload information about various aspects of their organization using standardized KYC/AML templates. The information is then published after going through an independent corroboration process. At last count, the platform had onboarded nearly 200 African FSPs and corporations and a handful of international institutions as contributors of data to Mansa.

Users, on the other hand, pay a subscription fee to access the data and are expected to be international FSPs breaking into the African market. The platform became operational only in December 2020, so the effectiveness of the solution is still being considered.

Source: https://www.afreximbank.com/afreximbank-launches-mansa-africas-digital-due-diligence-repository/

APIs can also support additional functionality. In-house development resources may be able to handle identity basics, such as account creation, log-in, and password reset. However, customers today are increasingly demanding greater functionality and security, which often increases the scope of projects. Advanced features, such as single sign-on support, customer data partitioning, token authentication, multifactor authentication, and the ability to use social log-ins, require considerably greater effort to build.

e. Develop robust procurement guidelines and support open design standards to promote innovation and competition and allow for greater flexibility, efficiency, and functionality within and across borders.

Policy makers should develop robust procurement guidelines and support open design standards for services provided by private-sector players, to facilitate competition and innovation. Policies that point to a specific vendor's technology can cause possible technology and vendor "lock-in," which can increase costs and reduce flexibility to accommodate changes over time. In contrast, policies that support open standards offer the benefit of support from multiple vendors, thus ensuring competition and a wide range of choices that come with it.

A conglomeration of global entities, both private and public, have formed international alliances to create open standards on foundational ID and authentication infrastructure. An example is the FIDO Alliance, which has brought together major industry players and governments to develop technical specifications that define an open, scalable, interoperable set of mechanisms to authenticate users in a way that is both more secure than legacy authentication approaches and easier to use.

As mentioned previously, it will be important to analyze the need to consider standards that work across borders in line with CPMI's BB8 ("*Fostering KYC and identity information sharing*") and the role that the private sector can play in this. A road map put together by the Financial Stability Board to achieve these building blocks includes as one of its focus areas "committing to a joint public and private-sector vision to enhance cross-border payments."

This is a foundational focus area and can provide a shared understanding of the needs and challenges for financial transactions to be efficient and secure across borders. It includes setting quantitative targets at the global level for addressing the challenges of cost, speed, transparency, and access, as well as a framework that stakeholders can use for establishing more granular service-level agreements.

f. View emerging technologies and applications as an opportunity, but recognize the potential risks posed to regulatory objectives, including consumer protection and stability.

Several emerging technologies and new combinations of existing technologies have the potential to leapfrog the need for a centralized national ID platform, digital or traditional. The ubiquity of mobile devices that include multiple biometric sensors is further challenging the status quo and enabling new models for delivering identity services.

Emerging technologies, such as artificial intelligence and distributed ledger technology, are providing opportunities for greater information sharing and a more collaborative, risk-based approach to CDD that lowers costs while potentially increasing effectiveness.[46] In addition, biometrics make it possible to verify uniqueness or to authenticate a person using less biographic data. It may also not be considered an emerging technology anymore.

It will be important for policy makers to keep pace with emerging technologies and the applications they bring to the financial sector while maintaining a regulatory framework that supports the use of new technologies in a way that protects the rights of the individual and minimizes the capacity of new ID technologies to cause individual or societal harm.

FSPs can leverage additional (digitally captured) attributes held by private-sector players to add to the robustness of a digital ID or its authentication. For example, real-time location data using GPS data or the cell tower nearest to a customer's mobile phone/electronic device could be used as a measure to prevent and detect fraud, based on appropriate safeguards to protect the privacy of customers.

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

g. Consider the use of regulatory "sandboxes" and other unconventional approaches to crafting policy as a way to close the gap between innovation and regulation.

One approach to allow leading-edge technologies to be tested—and for policy makers, particularly the financial-sector regulator, to gain valuable insight and knowledge—is to use a regulatory sandbox. A regulatory sandbox allows new business models and technology to be demonstrated or piloted on a small scale in a controlled, time-bound environment, creating a dynamic evidence base that regulators can learn from and use to develop appropriate regulatory policy.

BOX 15

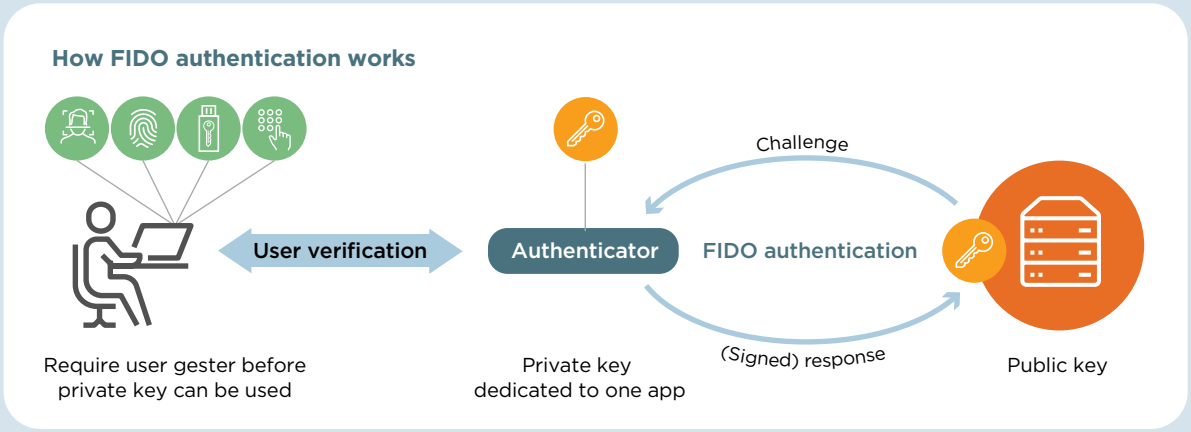
FIDO ALLIANCE

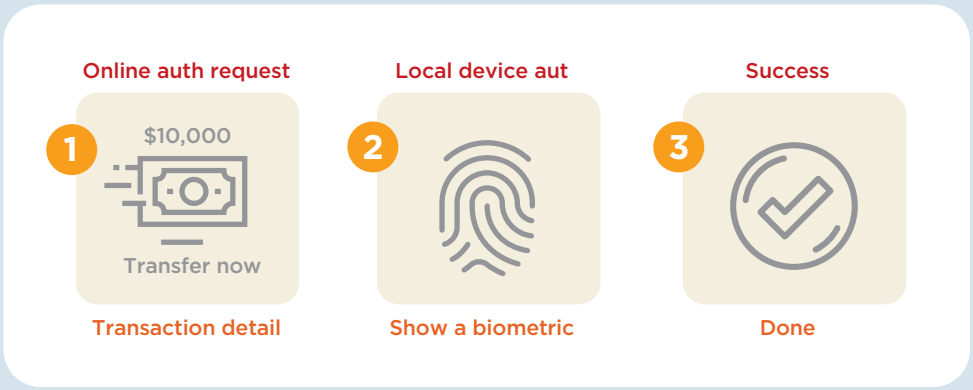
The FIDO Alliance is a nonprofit industry alliance launched in 2012 to address both the lack of interoperability among strong authentication devices and security and usability challenges caused by legacy authentication tools such as passwords, smart cards, or one-time password tokens.

FIDO standards are recognized by ISO and the International Telecommunication Union (X.1277 and X.1278), as well as the World Wide Web Consortium. FIDO standards combine a possession-based authentication factor based on asymmetric public key cryptography with a second user-verification factor—most commonly an on-device biometric match but sometimes a PIN code—to deliver strong multifactor authentication. FIDO is based on strong MFA that can be "built into" devices, rather than "bolted on," meaning that providers of digital financial services can deliver high-assurance services more quickly and cheaply.

In many cases, FIDO standards can be used to enable password-less authentication that is both more secure and easier to use.

Biometrics, if used, are stored only on device, mitigating the privacy and security risks associated with the collection and centralized storage of biometrics.





Source: FIDO Alliance

BOX 16

THE KIVA PROTOCOL

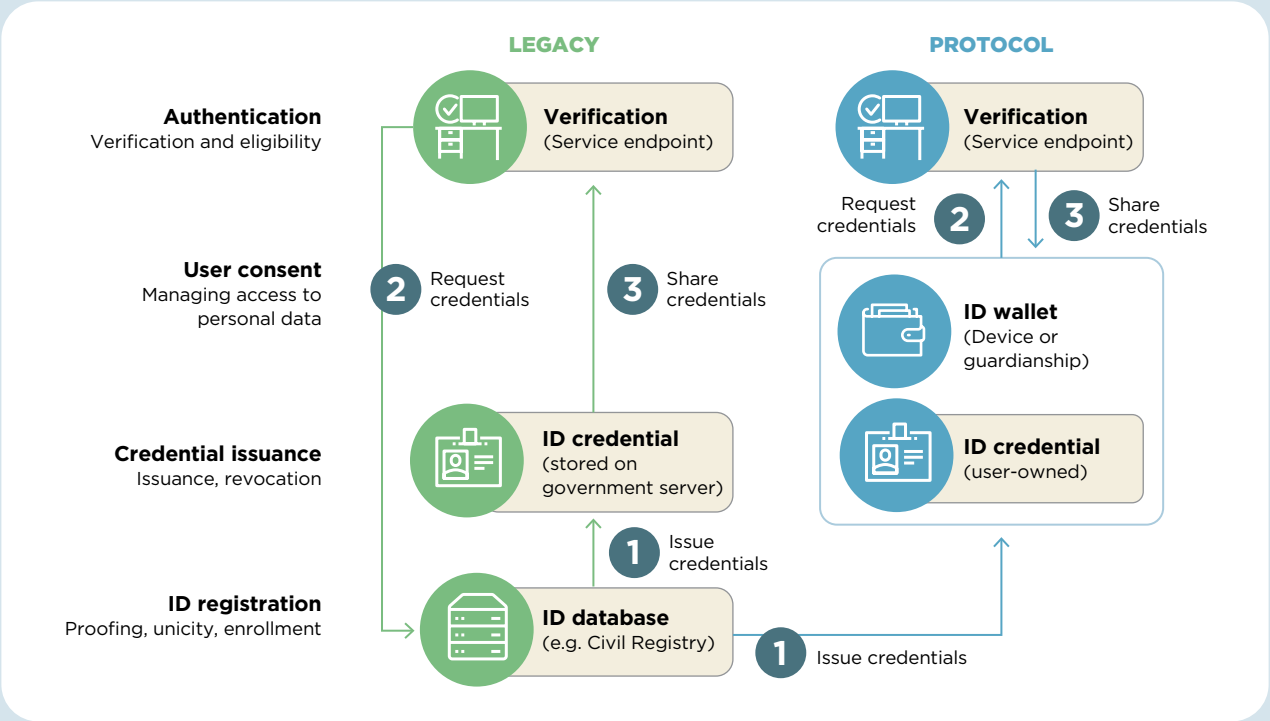
The Kiva Protocol was introduced to give unbanked people a digital identity and allow them to have control over their own credit information. Created in 2018 and being rolled out first in Sierra Leone, it is designed to help the country's seven million citizens—80 percent of whom are currently unbanked—access financial services.

The protocol consists of a verifiable identity combined with user-owned data and leverages distributed ledger technology. In essence, it allows all credit events—that is, loans and payment of loans, including those in the informal sector, such as credit from a local shopkeeper—to be associated with a veritable claim that the user can upload onto a Kiva digital wallet. The user is verified by a fingerprint that links to a central database. The system allows the unbanked to fully leverage the transactions that they are already a part of, and it costs little to operate, eliminating the type of fees that might prevent people or institutions from using other credit reports.[47]

Although the information and access to the information is controlled solely by the user, individuals can access their digital wallet through an application on their cell phones or can work through a microfinance institution or government "agent" who is already working in their community. These agents will be able to use the application online or offline. The government of Sierra Leone has worked with Kiva to ensure that the protocol is practical for its users and recognized as a foundational identity.

In this way, the government has ensured that the ID does the following:
Is portable with the user

- Is secure and lowers new customer onboarding costs by up to 90 percent*
- Extends (does not replace) foundational identity credentials into secure digital wallets
- Enables real-time, consumer-permissioned access by FSPs for seamless, compliant e-KYC and CDD
- Enables data from multiple ID issuers to be collated, supporting vendor neutrality
- Enables government-to-person payments that can be upgraded to private-sector rails



Source: Kiva, 2020

BOX 17

IDENTITY VERIFICATION SERVICES POWERED BY ARTIFICIAL INTELLIGENCE

Some private-sector entities are using sophisticated identity analytics that are driven by artificial intelligence (AI) and can be overlaid onto legacy ID solutions. The increasing use of online social and professional networks, e-commerce platforms, and connected devices (Internet of Things) 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, such information as where the person lives (based on, for example, the shipment of e-commerce purchases and taxi rides) and where the person works (based on geolocation coordinates during typical business hours). This data has often been used in peer-to-peer lending platforms to gauge the identity of users who might not have a formal credit history.

ID-verification solutions utilizing AI and machine learning can process many ID verification requests quickly. They can play a pivotal role in identifying fraud. An example is the "live" tests conducted by facial-verification services that recognize if an actual person is trying to verify an identity and that no facial spoof is being implemented to perform KYC verification.

Once it has been established that a real person is performing a verification, the authenticity of the presented ID document is checked. The use of AI can support the verification of people from different countries and can potentially be used to verify ID documents issued in different jurisdictions. With the added advantage of machine-learning algorithms, an AI-powered system can detect attempts to forge documents or fake information on ID documents faster and more efficiently than a non-AI system or manual review process.

The biometric features captured during the facial-verification process can be matched with the facial image present on an ID document. This establishes the verdict either against or in favor of the identity of the incoming user. However, while potentially useful, this can also have several disadvantages, such as breach of privacy and data protection, when used for gaining access to a variety of services. Several private-sector players, such as Stripe (see box 13), are using AI to verify documents.

Source: Authors' elaboration

BOX 18

IBM'S USE OF OPEN-SOURCE SOFTWARE TO REDUCE COSTS FOR FSPS

In 2016, IBM announced a blockchain project with the Singapore fintech start-up KYCK! to help enable FSPs to onboard their customers more rapidly in a secure environment. This and other KYC projects like it using IBM blockchain seek to help reduce the time and expense required to onboard a new client.

Through the application of blockchain technologies in the cloud, banks can streamline operations by adopting a one-time process with secure data protection and enhanced identity verification. This instance uses the open-source Hyperledger Project Fabric, hence offering immutability, traceability, and privacy of the information on a permissioned distributed ledger, which is critical in a highly regulated environment.

KYCK! intends to provide brokerages a platform for video conferencing and the submission of encrypted documents for the secure onboarding of new customers. The platform aims to provide enhanced ID validation through a trusted blockchain-based business network that will potentially include banking and governmental entities. Once identity verification is confirmed, KYCK! will enter the customer's information into current bank-based checks or third-party KYCK! systems before account onboarding.

This shows the potential of both leveraging new and emerging technology and using collaborative and open approaches.

Source: IBM

BOX 19

BANK NEGARA MALAYSIA'S THEMATIC E-KYC SANDBOX TRACK[48]

Bank Negara Malaysia[49] introduced a specialized thematic track for its sandbox. Called a "specialized sandbox," it is intended to accelerate innovations with clear potential to improve financial services. The first specialized sandbox focused on e-KYC and digital onboarding in an attempt to evolve KYC regulation that was historically performed in person. Under the specialized sandbox, two fintech companies and seven banks tested new e-KYC technologies.[50]

One of the first participants of the regulatory sandbox, MoneyMatch—an online cross-border remittance service provider—offered peer-to-peer remittance services and tested digital onboarding by conducting multiple video conferences to verify potential clients. The firm created a platform to match individual buyers and sellers of currencies with a focus on small and medium-sized enterprises that conduct a lot of cross-border transfers over the course of one day. For verification, MoneyMatch used third-party facial recognition powered by artificial intelligence. Using the sandbox for a controlled rollout and to test the effectiveness of the e-KYC process, MoneyMatch successfully graduated in June 2019, exiting Bank Negara Malaysia's e-KYC sandbox and receiving approval to operate and use its new KYC methods within the Malaysian market.[51]

The sandbox results helped Bank Negara Malaysia enable digital verification and develop new e-KYC policies. In December 2019, the bank issued an exposure draft, proposing requirements and guidance for e-KYC implementation.[52]

The advantages offered by such an approach are notable for both policy makers and industry. It is a way to get policy makers thinking about appropriate applications of a new technology without creating material risks in the market, and policy makers get an opportunity to engage closely with and understand new technology and the potential risks that innovation may pose to their objectives.

There is no truly perfect way to align policy with technology, but sandboxes provide one way to accelerate the process without rolling unproven or controversial technology immediately into the mass market. This is especially relevant in the highly regulated financial sector, particularly with regard to AML and CDD requirements, where sandboxes can be particularly helpful in identifying relevant technologies that enhance the CDD process.

2.5 POLICY CONSIDERATION 5: Ensure That There Is an Adequate Governance Framework for the e-KYC Solutions (Particularly on Collaborative CDD)

Regulated FSPs are subject to supervision and adhere to certain requirements as dictated by the financial-sector regulator, given that the services they provide carry significant implications for financial stability, integrity, and consumer protection. Oversight related to using digital ID for financial services needs to be maintained not only by the financial-sector regulator but also by other entities within the ecosystem that contribute, collect, store, or disseminate personal information related to digital ID.

Given that the digital ID ecosystem goes beyond the financial sector, there can be a lack of clarity about where the onus of responsibility for data security and privacy, data sharing, and overall accountability lies. Hence, *Principles on Identification for Sustainable Development* includes specific governance via a legal and regulatory framework and clear accountability and independent oversight as key focus areas. A clearly defined oversight framework will be critical to ensuring that a safe, secure, and transparent system underlies digital ID applications in the financial sector. Oversight of digital ID systems would broadly need to ensure the implementation of policies that cover customer decision and access rights, enforcement mechanisms, and contingency planning.

2.5.1 Implementation Approaches for Policy Consideration 5

a. Establish clear institutional mandates.

The multiple players in the digital ID ecosystem will need clarity on where regulatory liability lies across the various stakeholders—IDSPs, FSPs, third-party authentication services, and so forth. Rights and responsibilities across relevant stakeholders will need to be delineated clearly with respect to any failures or errors in customer identification, verification and authentication, and access processes.

b. Develop a transparent, proportionate, and equitable framework.

A framework should be developed that does not stifle competition, innovation, or investment. Given that digital ID can be leveraged by multiple sectors beyond the financial sector, measures should be taken to ensure that the same level of measures to safeguard privacy and security is applied to all sectors. The appropriate classification of data and adherence to data-governance rules and procedures while the data is at rest and in transit should be key to the functioning of the framework. This framework should enable different entities to act as relying parties, provided that they meet certain requirements subject to the oversight-designated authority.

c. Establish an independent oversight body.

Implementation of the oversight framework should be subject to an independent body with adequate representation from relevant stakeholders. The independent oversight body will periodically monitor, evaluate, and verify compliance with policies and procedures, to ensure safety and transparency. It should have the power to protect customers against inappropriate access and use of their data without informed consent or legitimate purpose. Based on the periodic assessment, it will draw conclusions about the effectiveness of the oversight framework and incorporate changes to oversight or the governance mechanism as it sees fit.

To carry out its monitoring and evaluation functions, the independent oversight body will establish a monitoring and evaluation system that includes targets and indicators to ensure compliance and measure progress toward other national targets, such as financial inclusion or reducing gender gaps in access to the financial sector.

3. Methodology for Country Implementation

This section describes the methodology to apply the policy considerations included in the present document at the country level and to understand the landscape of the financial sector and preparedness to adopt digital ID solutions. While the document presents several scenarios for using digital ID in the financial sector, the methodology aims at a comprehensive approach that might require collaboration between different authorities involved in the process.

The methodology intends to describe the process and provide guidance without regard to whether authorities conduct a self-assessment or the assessment is conducted by independent evaluators. The methodology also allows for country comparison when used in different jurisdictions, although it does not include a rating scheme, as it is not the intention of this document.

COUNTERPARTIES

The following is a list of potential counterparties. This list is indicative and not exhaustive. Potential counterparties should be discussed with the assessor prior to the assessment based on policy objectives and priorities.

- Central bank (payment systems unit/financial intelligence unit/financial supervision/financial inclusion)
- Financial supervisory authority (authorities
- Ministry of finance

Other authorities with which to coordinate:

- Ministry of information, communication, and technology
- Data-protection or privacy regulators
- Ministry of interior or government agency with a mandate over the foundational ID system
- Below is a description of the different steps to follow when deploying the toolkit.

Scope of assessment	1.1 While the exercise should ideally comprise all the potential FSPs, it might happen that a specific authority may not have legal powers over a specific financial activity or service provider. It might also happen that the authority may have conducted a risk assessment based on predefined criteria (for example, identity theft in a specific group of service providers or in a new product introduced in the market or a service to meet an emerging need) that calls for a limited scope in the nature of the exercise. 1.2 The scope should be clearly defined before fact gathering begins. 1.3 It is encouraged that financial-sector regulatory authorities coordinate with the authorities leading the national ID system, if this exists, or any other initiatives related to ID-management systems, regardless if they are digital or not.
Fact finding	2.1 Assessors should gather sufficient facts to be able to develop conclusions for each of the policy recommendations. Assessors should also consider if existing challenges cannot be framed under the provided policy considerations. 2.2 A detailed list of guiding questions has been developed to help the assessor gather facts. (See section 4.) 2.3 Previous relevant work performed by national authorities/regulators or external assessors should also be considered.
Develop conclusions	3.1 For each of the policy considerations, the assessor should summarize current practices and achievements. 3.2 For any gaps, the assessor will need to determine the materiality or relative importance of that particular component and its interactions with other individual components 3.3 Assessors should identify the entity(s) (for example, a regulator, an ID provider, or a relying party) that would be responsible for implementing the various recommendations that have been made. 3.4 Identification of roles might also lead to different entities being responsible for implementing one policy consideration—the assessor should clearly identify if there is an entity with primary responsibility over the relevant recommendation.
Timeframe for addressing each area of concern	4.1 It is highly recommended that the assessor establish a timeline for the relevant entity or entities to take action based on the concerns identified and the recommendations provided. 4.2 Frequently, the party or parties intended to implement the recommendations will need further guidance with regard to prioritization and the associated timeframe. 4.3 The assessor should establish priorities based on the level of impact that the area of concern poses to the overall safety, effectiveness, and reliability of the system. 4.4 It might also be necessary to conduct a pilot to understand the impact of a given policy consideration in a jurisdiction.

4. Guiding Questions to Assess Digital ID in the Financial Sector

GUIDING QUESTIONS FOR POLICY CONSIDERATION 1:

Ensure that the legal and regulatory framework is supportive of the usage of digital ID by financial service providers

Guiding Questions	Yes/No (Add explanation)
Does the legal framework allow for the sharing of information between different authorities for AML/CFT purposes?	
Are the financial-sector regulators in correspondence with other relevant regulators?	
Does the legal framework allow third parties to conduct the CDD process and share information from different sources?	
Does the legal framework recognize a digital ID for financial-sector use?	
What ID credentials (or ID-verification mechanisms) are legally accepted/required to verify a customer's identity in the CDD context?	
Is the digital ID recognized as valid for all types of CDD levels?	
Is the legal framework clear regarding the service provider's accountability for errors?	
Does the legal framework allow for a simplified CDD regime?	
Is the flexible approach recognized by FATF implemented under the country's legal framework?	
Does the law allow for all types of FSPs to use an e-KYC solution?	
Are there any challenges for any particular type of FSP to adopt an e-KYC solution?	
Is the legal framework for the adoption of e-KYC solutions fair and nondiscriminatory to all FSPs (banks and non-banks)?	
Does the legal framework provide for the use of digital ID for individuals only?	
Is there any situation in which the legal framework allows the use of digital ID for legal entities (micro, small, and medium-sized enterprises and sole proprietors)?	
Is there a framework for e-signature? (Please explain if this is a three-pronged approach or how is it structured.)	
Does the legal framework allow the use of digital signature as a form of ID?	
Does the legal framework take into consideration the use of digital ID for cross-border transactions?	

GUIDING QUESTIONS FOR POLICY CONSIDERATION 2:

Consider the full range of risks associated with use of digital ID in the financial sector

Guiding Questions	Yes/No (Add explanation)
Are risks identified by the financial-sector regulators?	
Are risk-mitigating measures identified in the regulation for the adoption of digital ID by FSPs?	
Does each FSP have to develop a strategy to identify and address risks related to the adoption of digital ID solutions?	
Has the financial-sector regulatory authority issued any guidance in this area?	
Are risks associated with digital ID managed by another regulatory authority (data protection, competition, consumer, ministry of technology, financial intelligence unit, cybersecurity)?	
Is there a process to authorize digital ID/KYC solution service providers in the country?	
Does the framework allow for the provision of digital ID/KYC solutions across borders?	

GUIDING QUESTIONS FOR POLICY CONSIDERATION 3:

Provide for consent mechanisms for users to maintain control over data collected for use within the financial sector

Guiding Questions	Yes/No (Add explanation)
Does the digital ID scheme allow for the customer to authorize the processing of the customer's personal data?	
Does the digital platform/application allow for real-time authorization by the customer each time the data is to be shared with a new entity?	
Does the process allow customers to withdraw consent?	
Is the process of consent recorded and stored?	
Do the relevant authorities have access to the consent evidence (for example, financial intelligence unit or data protection)?	
Is the consent process easy to explain to customers?	
Is the consent process bundled with other services?	
Is there a process that allows customers to authenticate themselves and access the record of previous uses of their digital ID?	

GUIDING QUESTIONS FOR POLICY CONSIDERATION 4:

Collaborate and engage with the private sector to develop e-KYC solutions, including collaborative CDD, and monitor emerging technologies relevant to ID verification in the financial sector

Guiding Questions	Yes/No (Add explanation)
Is there any platform that is used for collaboration between the private and public sector?	
Have you identified any gaps where you believe the private sector can play a role?	
Is the private sector currently involved in any services in relation to ID? If so, what?	
Have you considered collaborative approaches with the private sector, such as the use of KYC registries?	
Does the current ID infrastructure support the ability for private-sector players to build on top of and leverage the underlying infrastructure?	
If yes, do private-sector players need a license to access the infrastructure?	
Does the ability exist to connect and use APIs from regulated and unregulated institutions to support ID-management?	
Are any other open standards in place?	

continued

How are developments in emerging technologies being monitored and adapted for use?	
Are you currently experimenting with, or do you know of, technologies that are being used in the identity life cycle?	
Has the regulator considered the use of innovation facilitators, such as regulatory sandboxes, to support the development of policy for the application of emerging technologies?	
Have the risks from emerging technology and from the use of collaborative approaches been adequately considered?	

GUIDING QUESTIONS FOR POLICY CONSIDERATION 5:

Ensure that there is an adequate governance framework for the e-KYC solutions (particularly on collaborative CDD)

Guiding Questions	Yes/No (Add explanation)
Is there a transparent, proportionate framework in place that encourages innovation and competition but balances the risks?	
Does the framework include those firms outside the financial sector that provide ID services?	
Is there an independent body that oversees the framework?	
Are there clear institutional mandates that define where regulatory liabilities lie?	
Have clear targets and indicators been defined?	
Does the arrangement include clear data-governance rules?	
Is an evaluation of the governance framework conducted periodically?	

Glossary

Application programming interface (API): A set of functions and procedures allowing the creation of applications that access the features or data of an operating system, application, or other service.

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.

Collaborative CDD: A term used to cluster existing and emerging approaches that relieve, through some measure of collaboration, the burden of CDD compliance that traditionally was carried individually by FSPs or that improve the effectiveness of CDD processes.[53]

Commercial bank: A bank that is (a) not subject by law or regulation to (i) a specified maximum size of loan or savings product or (ii) any limitation on the type of client that may be served, and (b) not tasked by law or regulation with serving any particular industry.

Consumer protection: Federal and state statutes governing sales and credit practices involving consumer goods.

Customer due diligence (CDD): Facts about a customer that should enable an organization to assess the extent to which the customer exposes it to a range of risks. These risks include money laundering and the financing of terrorism.

Customer onboarding: The process by which an FSP establishes a business relationship with a customer.

Deposit account: An account held with banks and other authorized deposit-taking financial institutions that can be used for making and receiving payments. Such accounts are known in some countries as current accounts, checking accounts, or similar terms.

Digital identity (ID): A set of electronically captured and stored attributes and/or credentials that uniquely identify a person.

Digital ID system: An ID system that uses digital technology throughout the identity life cycle, including for data capture, validation, storage, and transfer; credential management; and ID verification and authentication.

E-money: Monetary value represented by a claim on the issuer that is stored on an electronic device, such as a chip card or a hard drive in a personal computer, or on servers or other devices, such as mobile phones, and issued upon receipt of funds in an amount not less in value than the monetary value received and accepted as a means of payment by undertakings other than the issuer.

Financial consumer protection legal and regulatory framework: A set of legislative and regulatory instruments governing the practices of FSPs with respect to their dealings with consumers.

Financial cooperative: A member-owned and member-controlled financial institution governed by the "one member, one vote" rule. Financial cooperatives often take deposits or similar repayable funds from and make loans only to members, although some also serve nonmembers. The term includes credit unions, building societies, caisses, cajas, cooperative banks, mutual banks, and savings and credit cooperatives.

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

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.

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

Insurance: A contract, represented by a policy, in which an individual or entity receives financial protection or reimbursement against losses from an insurance company. The company pools clients' risks to make payments more affordable for the insured.

KYC registry: A type of collaborative CDD that refers to a centralized repository of customers' data, including, at a minimum, name and address. It allows interusability of the CDD records across the sector with the objective of reducing the burden of producing CDD documents and getting those verified each time the customer creates a new relationship with a financial entity.

Microcredit: Small-scale credit typically provided to self-employed or informally employed poor and low-income individuals and microenterprises. Other common features of microcredit include a lending methodology characterized by familiarity with the borrower, a lack of collateral, an expectation of a follow-on loan upon successful repayment, and very small loan amounts (although the size of microcredit varies from country to country).

Microfinance institution (MFI): A financial institution that does not take deposits and provides microcredit targeting low-income and poor customers.

Mobile wallet: A virtual wallet that stores payment-card information on a mobile device.

Nonbank e-money issuer (NBEI): An issuer of e-money that is not a bank. The relevant questions in the survey request respondents to indicate whether the nonbank entity is authorized to act as an issuer of e-money.

Other bank: A bank other than a commercial bank. In a given country, this term may include rural banks, agricultural banks, and postal banks, among other types of noncommercial banks. (It does not include cooperative banks or mutual banks, which are categorized as financial cooperatives for the purposes of this survey.)

Other deposit-taking institution (ODTI): An institution authorized to collect deposits or savings that does not fit the definition of bank or financial cooperative. ODTIs include deposit-taking microfinance institutions, and savings and loan associations, among other nonbank deposit-taking institutions.

Postal operator: Any public or private entity providing various types of postal services, including mailing, delivery, and financial services.

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.

Simplified CDD: A set of simplified internal controls that enable a financial institution to establish a customer's identity and predict with relative certainty the types of transactions in which the customer is likely to engage under low-risk scenarios.

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

APPENDIX A

FATF Recommendation 10

Recommendation 10 of the FATF establishes that financial institutions should be prohibited from keeping anonymous accounts or accounts in obviously fictitious names. Also, financial institutions should conduct CDD under the following circumstances:

(i) Establishing business relations (that is, onboarding of new clients);

(ii) Carrying out occasional transactions above 15,000 dollars or euros; or

(iii) Electronic transfers based on interpretative note (IN) R16;[54] for cross-border wire transfers, countries may adopt a *de minimis* threshold not higher than 10,000 dollars/euros where information about the name of the originator, the beneficiary, and the account number is required but there is no need for verification.

(iii) Suspicion of illegal activity of money laundering or the financing of terrorism; or

(iv) When the financial institution has doubts about the veracity or adequacy of previously obtained customer ID data.

The principle that financial institutions should conduct CDD should be set out in law. Each country may determine how it imposes specific CDD obligations, either through law or enforceable means. The CDD measures to be taken are as follows:

(a) Identifying the customer and verifying that customer's identity using reliable, independent source documents, data, or information.

(b) Identifying the beneficial owner, and taking reasonable measures to verify the identity of the beneficial owner, so the financial institution is satisfied that it knows who the beneficial owner is. For legal persons and arrangements, this should include the financial institution's understanding the ownership and control structure of the customer.

(c) Understanding and, as appropriate, obtaining information on the purpose and intended nature of the business relationship.

(d) Conducting ongoing due diligence on the business relationship and scrutiny of transactions undertaken throughout the course of that relationship, to ensure that the transactions being conducted are consistent with the institution's knowledge of the customer, their business, and risk profile, including, where necessary, the source of funds.

Financial institutions should be required to apply each of the CDD measures under (a) to (d) above but should determine the extent of such measures using a risk-based approach in accordance with the Interpretive Notes to this Recommendation and to Recommendation 1.

Financial institutions should be required to verify the identity of the customer and beneficial owner before or during the course of establishing a business relationship or conducting transactions for occasional customers. Countries may permit financial institutions to complete the verification as soon as reasonably practicable following the establishment of the relationship, where the risks of money laundering and the financing of terrorism are effectively managed and where this is essential not to interrupt the normal conduct of business.

Where the financial institution is unable to comply with the applicable requirements under paragraphs (a) to (d) above (subject to appropriate modification of the extent of the measures on a risk-based approach), it should be required not to open the account, commence business relations, or perform the transaction; or should be required to terminate the business relationship; and should consider making a suspicious transactions report in relation to the customer.

These requirements should apply to all new customers, although financial institutions should also apply this recommendation to existing customers on the basis of materiality and risk, and should conduct due diligence on such existing relationships at appropriate times.

APPENDIX B

NIST Definitions[55]

A. IDENTITY ASSURANCE LEVELS

Assurance in a subscriber's identity is described using one of following three identity assurance levels (IALs):

IAL1: There is no requirement to link the applicant to a specific real-life identity. Any attributes provided in conjunction with the subject's activities are self-asserted or should be treated as self-asserted (including attributes a cloud service provider asserts to a relying party). Self-asserted attributes are neither validated nor verified.

IAL2: Evidence supports the real-world existence of the claimed identity and verifies that the applicant is appropriately associated with this real-world identity. IAL2 introduces the need for either remote or physically present identity proofing. Attributes could be asserted by cloud service providers to relying parties in support of pseudonymous identity with verified attributes. A cloud service provider that supports IAL2 can support IAL1 transactions if the user consents.

IAL3: Physical presence is required for identity proofing. Identifying attributes must be verified by an authorized and trained cloud service provider representative. As with IAL2, attributes could be asserted by cloud service providers to relying parties in support of pseudonymous identity with verified attributes. A cloud service provider that supports IAL3 can support IAL1 and IAL2 identity attributes if the user consents.

B. STRENGTHS OF IDENTITY EVIDENCE

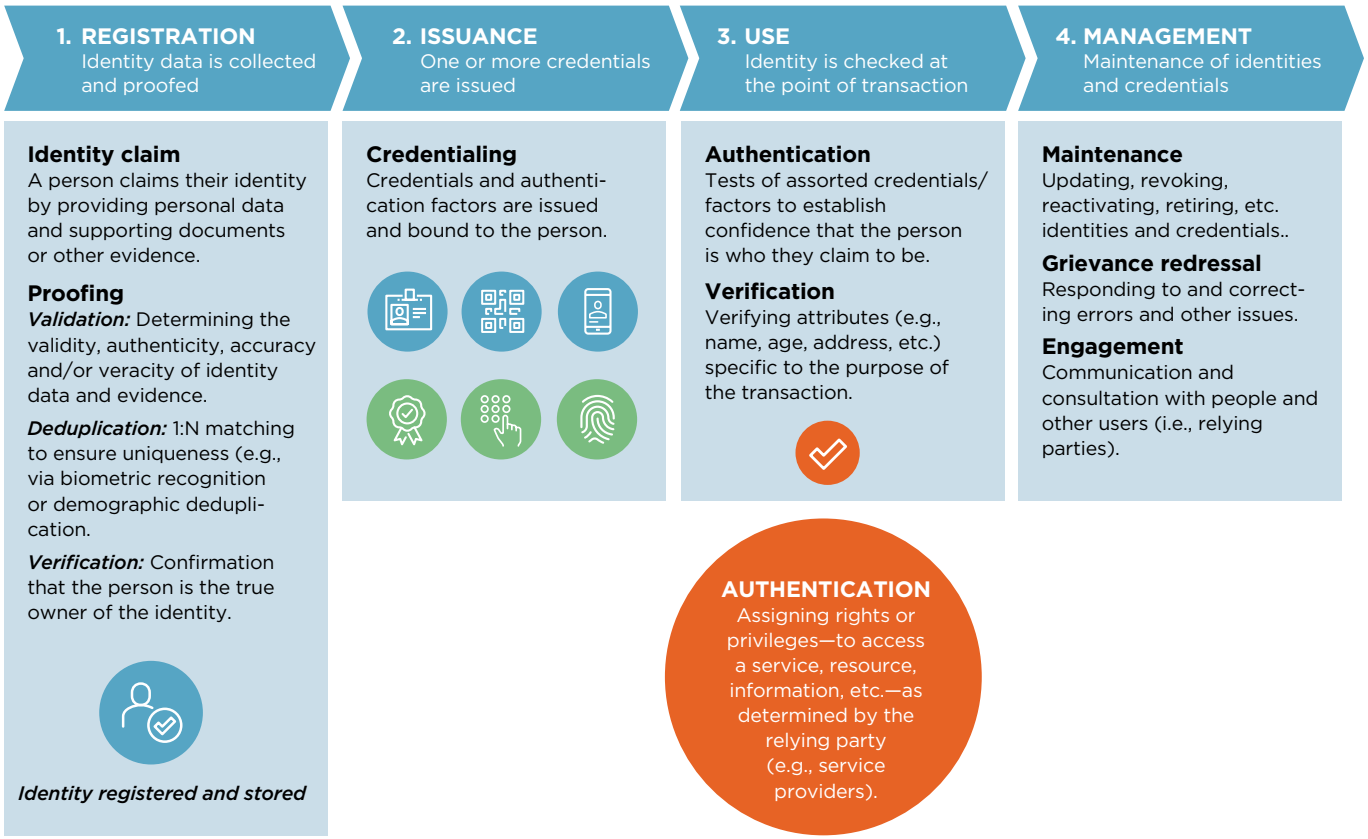
Strength	Qualities of Identity Evidence
Unacceptable	• No acceptable identity evidence provided.
Weak	• The issuing source of the evidence did not perform identity proofing. • The issuing process for the evidence means that it can reasonably be assumed to have been delivered into the possession of the applicant. • The evidence contains: – At least one reference number that uniquely identifies itself or the person to whom it relates. **OR** – The issued identity evidence contains a photograph or biometric template (of any modality) of the person to whom it relates.
Fair	• The issuing source of the evidence confirmed the claimed identity through an identity proofing process. • The issuing process for the evidence means that it can reasonably be assumed to have been delivered into the possession of the person to whom it relates. • The evidence: – contains at least one reference number that uniquely identifies the person to whom it relates. **OR** – contains a photograph or biometric template (any modality) of the person to whom it relates. **OR** – can have ownership confirmed through KBV. • Where the evidence includes digital information, that information is protected using approved cryptographic or proprietary methods, or both, and those methods ensure the integrity of the information and enable the authenticity of the claimed issuing source to be confirmed. • Where the evidence includes physical security features, it requires proprietary knowledge to be able to reproduce it. • The issued evidence is unexpired.
Strong	• The issuing source of the evidence confirmed the claimed identity through written procedures designed to enable it to form a reasonable belief that it knows the real-life identity of the person. Such procedures are subject to recurring oversight by regulatory or publicly accountable institutions. For example, the Customer Identification Program guidelines established in response to the USA PATRIOT Act of 2001 or the **Red Flags Rule**, under Section 114 of the Fair and Accurate Credit Transaction Act of 2003 (FACT Act). • The issuing process for the evidence ensured that it was delivered into the possession of the subject to whom it relates. • The issued evidence contains at least one reference number that uniquely identifies the person to whom it relates. • The full name on the issued evidence must be the name that the person was officially known by at the time of issuance. Not permitted are pseudonyms, aliases, an initial for surname, or initials for all given names • The: – Issued evidence contains a photograph or biometric template (of any modality) of the person to whom it relates. **OR** – Applicant proves possession of an Authentication Assurance Level 2 authenticator, or equivalent, bound to an IAL2 identity, at a minimum. • Where the issued evidence includes digital information, that information is protected using approved cryptographic or proprietary methods, or both, and those methods ensure the integrity of the information and enable the authenticity of the claimed issuing source to be confirmed. • Where the issued evidence contains physical security features, it requires proprietary knowledge and proprietary technologies to be able to reproduce it. • The evidence is unexpired.

continued

Strength	Qualities of Identity Evidence
Superior	• The issuing source of the evidence confirmed the claimed identity by following written procedures designed to enable it to have high confidence that the source knows the real-life identity of the subject. Such procedures are subject to recurring oversight by regulatory or publicly accountable institutions. • The issuing source visually identified the applicant and performed further checks to confirm the existence of that person. • The issuing process for the evidence ensured that it was delivered into the possession of the person to whom it relates. • The evidence contains at least one reference number that uniquely identifies the person to whom it relates. • The full name on the evidence must be the name that the person was officially known by at the time of issuance. Not permitted are pseudonyms, aliases, an initial for surname, or initials for all given names. • The evidence contains a photograph of the person to whom it relates. • The evidence contains a biometric template (of any modality) of the person to whom it relates. • The evidence includes digital information, the information is protected using approved cryptographic or proprietary methods, or both, and those methods ensure the integrity of the information and enable the authenticity of the issuing source to be confirmed. • The evidence includes physical security features that require proprietary knowledge and proprietary technologies to be able to reproduce it. • The evidence is unexpired.

APPENDIX C

Identity Life Cycle



Source: Adapted from *Digital Identity: Towards Shared Principles for Public and Private Sector Cooperation* and *Technology Landscape for Digital Identification*

Notes

1. Global Findex 2017.
2. **http://www.fatf-gafi.org/media/fatf/documents/recommendations/Guidance-on-Digital-Identity.pdf**, 19
3. **https://www.bis.org/cpmi/publ/d144.pdf**
4. Some practices currently rely on verification of paper-based ID systems and credentials with a photo under remote account-opening scenarios that allow for the "real-time" identity verification of the customer (for example, by examining the credential and comparing the photo to the person presenting it). However, the level of assurance would likely be lower than in the case of a digital ID system.
5. (McKinsey, 2019)Digital Identification: A Key to inclusive growth. **https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/digital-identification-a-key-to-inclusive-growth**
6. Bester et al. 2008; Isern and de Koker 2009; Lyman and Noor 2014; Strengthening Financial Inclusion and Integrity, FATF 2017.{-REWRITE THESE CITATIONS? PAPER LACKS REFERENCE SECTION REQUIRED TO MAKE SENSE OF SUCH AUTHOR-DATE CITATIONS-}
7. Recommendation 16 establishes that financial institutions are required to collect accurate information about the originator and beneficiary of cross-border wire transfers and domestic wire transfers, including serial payments and cover payments.
8. Guidance on digital ID, https://www.fatf-gafi.org/publications/fatfrecommendations/documents/digital-identity-guidance.html
9. Guidance on AML/CFT and financial inclusion,
10. **https://www.fatf-gafi.org/publications/fatfgeneral/documents/financial-inclusion-cdd-2017.html**
11. *G20 Digital Identity Onboarding*, https://www.gpfi.org/publications/g20-digital-identity-onboarding
12. FATF guidance on digital ID, https://www.fatf-gafi.org/publications/fatfrecommendations/documents/digital-identity-guidance.html
13. *Principles on Identification for Sustainable Development*, http://documents1.worldbank.org/curated/en/213581486378184357/pdf/Principles-on-identification-for-sustainable-development-toward-the-digital-age.pdf
14. **BIS,** *Payment Aspects of Financial Inclusion*,
15. **https://id4d.worldbank.org/legal-assessment**
16. **Id4d.worldbank.org/research**
17. *Enhancing Cross-Border Payments: Building Blocks of a Global Roadmap*, **https://www.bis.org/cpmi/publ/d193.pdf**
18. In the 2017 Global Findex survey, 26 percent of unbanked individuals in low-income countries cited a lack of official ID documentation as the primary barrier to obtaining financial services.
19. FATF, *FATF Guidance: Anti-Money Laundering and Terrorist Financing Measures and Financial Inclusion with a Supplement on Customer Due Diligence* (FATF, Paris, 2017), **www.fatf-gafi.org/publications/financialinclusion/documents/financial-inclusion-cdd-2017.html.**
20. Based on *Draft Guidance on Digital Identity* (FATF, 2020)

21. The regulation was directed to banks, Islamic banks, investment banks, life insurance companies, takaful operators, money-changing operators, remittance service providers, development financial institutions, and non-bank issuers of payment instruments.
22. The survey involved 15 jurisdictions where a digital ID solution was in place or being developed.
23. The NIST 800-63 Digital Identity Guidelines consists of a suite of documents: *Digital Identity Guidelines* (NIST Special Publication 800-63-3); *Digital Identity Guidelines: Enrollment and Identity Proofing* (NIST Special Publication SP 800-63A); *Digital Identity Guidelines: Authentication and Life Cycle Management* (NIST Special Publication 800-63B); and *Digital Identity Guidelines: Federation and Assertions* (NIST Special Publication 800-63C).
24. **https://digital-strategy.ec.europa.eu/en/policies/eidas-regulation**
25. MyInfo was designed by the Government of Singapore as a service that enables citizens and residents to manage the use of their personal data for simpler online transactions. Users control and consent to the sharing of their data and can view a record of past usage. MyInfo aims to reduce the need for providing verifying documentation during online transactions.
26. Monetary Authority of Singapore, Circular No.: AMLD 01/2018, **http://www.mas.gov.sg/~/media/MAS/Regulations%20and%20Financial%20Stability/Regulatory%20and%20Supervisory%20Framework/Anti_Money%20Laundering_Countering%20the%20Financing%20of%20Terrorism/Circular%20on%20MyInfo%20and%20CDD%20on%20NFTF%20business%20relations.pdf**
27. *Draft Guidance on Digital Identity* (FATF, 2019)
28. Guidance on digital ID (FATF, 2020)
29. For further guidance, please see UNCITRAL Model Law, https://uncitral.un.org/en/texts/ecommerce/modellaw/electronic_signatures }
30. **https://www.mas.gov.sg/-/media/MAS/Regulations-and-Financial-Stability/Regulatory-and-Supervisory-Framework/Anti_Money-Laundering_Countering-the-Financing-of-Terrorism/Circular-on-MyInfo-and-CDD-on-NFTF-business-relations.pdf**
31. *Principles on Identification for Sustainable Development*
32. Data-protection authorities in different countries have developed guidelines to conduct effective data-protection impact assessments (for example, ICO in the United Kingdom or AEPD in Spain). See **https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-impact-assessments/ and https://www.aepd.es/es/derechos-y-deberes/cumple-tus-deberes/medidas-de-cumplimiento/evaluaciones-de-impacto.**
33. *FATF Guidance: Anti-Money Laundering and Terrorist Financing Measures and Financial Inclusion* (2017)
34. Guidance on digital ID (FATF, 2020)
35. NIST Special Publication 800-63A
36. The availability of stolen data to professional fraudsters is rendering knowledge-based authentication increasingly inadequate for distinguishing legitimate customers from fraudsters.
37. FIDO specifications can be downloaded for free from the FIDO Alliance at https://fidoalliance.org/specifications/.
38. *ID Enabling Environment Assessment (IDEAA)*
39. CPMI-IOSCO, *Guidance on Cyber Resilience for Financial Market Infrastructures* (2016).
40. https://www.mckinsey.com/industries/financial-services/our-insights/data-sharing-and-open-banking
41. GSMA, *Economic Identities for Small Business Owners: Insights from Nigeria*, https://www.gsma.com/mobilefordevelopment/resources/economic-identities-for-small-business-owners-insights-from-nigeria/
42. Economic Identities Small Business Owners, GSMA, 2019 https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2019/07/Economic_Identities_for_Small_Business_Owners_Report-Web.pdf
43. Lyman, Timothy, Louis de Koker, Chrissy Martin Meier, and Mehmet Kerse, *Beyond KYC Utilities: Collaborative Customer Due Diligence for Financial Inclusion*, CGAP Working Paper (Consultative Group to Assist the Poor, August 2019), **CDD Utilities CGAP** ? URL PROVIDED DID NOT WORK}
44. https://www.contrastsecurity.com/security-influencers/a-week-of-web-application-hacks-and-vulnerabilities
45. OAuth 2.0 is the industry-standard protocol for authorizing delegated access to APIs. It enables applications to obtain limited access to user accounts such as Facebook and GitHub.
46. CGAP Blog, https://www.cgap.org/blog/collaborative-customer-due-diligence-new-ways-forward
47. https://pages.kiva.org/kiva-protocol-faq
48. **https://fintechnews.my/17548/regtech-fintech-regulation-malaysia/ekyc-malaysia/.**
49. **https://www.bnm.gov.my/files/publication/fsps/en/2018/cp02.pdf.**
50. **https://fintechnews.my/17548/regtech-fintech-regulation-malaysia/ekyc-malaysia/.**
51. **https://fintechnews.my/20883/payments-remittance-malaysia/moneymwatch-graduate-bank-negara-malaysia-Sandbox/; https://dfsobservatory.com/sites/default/files/DFSO%20-%20The%20State%20of%20Regulatory%20Sandboxes%20in%20Developing%20Countries%20-%20PUBLIC.pdf.**
52. **https://www.theedgemarkets.com/article/ekyc-banks-come-soon.**
53. de Koker, Singh, and Capal 2017 Clsosure of Bank Accounts of Remittance Service Providers http://www.austlii.edu.au/au/journals/UQLawJl/2017/6.pdf{-REWRITE CITATION? PAPER LACKS REFERENCE SECTION REQUIRED TO MAKE SENSE OF SUCH AUTHOR-DATE CITATIONS-}
54. Recommendation 16 establishes that financial institutions are required to collect accurate information about the originator and beneficiary of cross-border wire transfers and domestic wire transfers, including serial payments and cover payments.
55. NIST Special Publication 800-63A, **https://pages.nist.gov/800-63-3/sp800-63a.html#ial-section**

THE WORLD BANK
IBRD • IDA | WORLD BANK GROUP