FIGI
FINANCIAL INCLUSION
GLOBAL INITIATIVE

Digital Identification Mexico

WORLD BANK GROUP

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 funds 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 report forms part of a broader project under the Financial Inclusion Global Initiative Mexico country implementation. 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 including The World Bank, its Board of Executive Directors, or the governments they represent, or the views of the Committee for Payments and Market 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

Acknowledgments

This document is the result of work developed by an international team in coordination with a local team. The international team was coordinated by Fredesvinda Montes (Senior Financial Sector Specialist, World Bank) with the support of Rekha Reddy (Senior Financial Sector Specialist, World Bank), Jonathan Marskell (ID4D), and Robert Palacios (Social Protection and Labor Team Leader, World Bank). The international team conducted missions to Mexico between April and July 2017. The local team included officials from the Secretaría de Hacienda y Crédito Público (SHCP) and was coordinated by Ana Laura Villanueva (Directora General Adjunta de Banca y Valores Unidad de Banca, Valores y Ahorro, SHCP). The report has benefited from extensive inputs and comments received from colleagues from within the World Bank Group. These include the core members of the ID4D Working Group, representing World Bank Global Practices responsible for Finance and Markets and Social Protection. Valuable feedback has been received from Harish Natarajan, Emile J. M. Van der Does, Matei Dohotaru, and Mia Harbitz. Their helpful comments and inputs have significantly enriched this report.

The mission team held several meetings with the objective of understanding various aspects of the identification management systems in Mexico. In addition to meetings held with SHCP staff coordinating unit, the team attended meetings with the SHCP (*Unidad de Inteligencia Financiera*), Banco de México (*Disposiciones de Banca Central, Información del Sistema Financiero, Sistemas de Pagos, Directora de Regulación y Supervisión, Gerencia de Autorizaciones, Regulación y Sanciones*), SAT (*Administración General de Servicios al Contribuyente)*, IMSS (*División de Vigencia de Derechos Coordinación de Clasificación de Empresas y Vigencia de Derechos and División de Soporte a los Procesos de Afiliación. Coordinación de Afiliación*), CONDUSEF (*Desarrollo Financiero Estadístico y de Tecnologías de Información and Desarrollo y Evaluación del Proceso Operativo*), Secretaría de Economía (*Regulación de Servicios de Firma Electrónica y Sistemas Registrales*), Registro Nacional de Población, Consejo Nacional de Funcionarios de Registro Civil (CONAFREC), Cámara de Comercio de México, Lex Informática, Buró de Crédito, Circulo de Crédito, Colegio de Notarios D.F., Colegio de Corredores Públicos, Comisión Nacional de Banca y Valores (CNBV, División de Análisis e Información), FIMPE, Procesar, Asociación Mexicana de Estándares para el Comercio Electrónico, GS1 México, Asociación de Bancos de México, INEGI, Registro Federal de Electores, INAI (Secretario General de Protección de Datos, Normatividad y Consulta, Investigación y Sanción, Prevención y Autorregulación, Derechos y Sanción y Asuntos Internacionales), and *Asociación de Bancos de México.* The team also held meetings with relevant organizations involved in digital identification initiatives in Chile, India, Nigeria, Perú, South Africa, Sweden, Uganda, and the United Kingdom to provide benchmark and international perspective to the situation in México. The team had an opportunity for open discussions with these institutions and believes that it has been able to obtain representative views of the financial community in the country and relevant institutions involved in the issuance and usage of identification management systems and ongoing and planned reforms. The team wants to express its appreciation to the management and staff of the SHCP and to all the representatives of the institutions visited for their full and enthusiastic support of the mission's activities and objectives.

Abbreviations

ABM	Banks Association of Mexico (*Asociación de Bancos de Mexico*)
AFOREs	Retirement Funds Administrators (*Administradoras de Fondos para el Retiro)*
AML	anti-money-laundering
API	application programming interface
CFT	countering the financing of terrorism
CLEE	Business Statistics Code *(Clave Estadística Empresarial)*
CNBV	National Banking and Security Commission *(Comisión Nacional de Banca y Valores)*
CONSAR	National Commission on Savings and Retirement *(Comisión Nacional de Sistemas de Ahorro para el Retiro)*
CURP	Unique Population Registry Code (*Clave Única de Registro Nacional de Población*)
DLT	distributed ledger technology
FATF	Financial Action Task Force
FEA	Advanced Electronic Signature (*Firma Electronica Avanzada)*
IMS	identity-management system
IMSS	Mexican Institute of Social Security *(Instituto Mexicano de Seguro Social)*
INAI	National Institute for Access to Information *(Instituto Nacional de Transparencia)*
INE	National Electoral Institute *(Instituto Nacional Electoral)*
INEGI	National Institute of Statistics and Geography *(Instituto Nacional de Estadística y Geografía)*
ISSTE	Institute for Social Security and Services for State Workers (*Instituto de Seguridad y Servicios Sociales de los Trabajadores del Estado*)
KYC	know your customer
LEI	Legal Entity Identifier
LOU	Local Operating Unit
PAFI	Payment Aspects of Financial Inclusion
RENAPO	National Registry of Population and Personal Identification (*Registro Nacional de Población)*
RFC	Federal Tax Payer Registry *(Registro Federal de Contribuyente)*
SAT	Tax Administration Service (*Servicio de Administración Tributaria*)
SHCP	Secretariat of Finance and Public Credit (*Secretaría de Hacienda y Crédito Público*)

I. Executive Summary

The objective of this document is to describe the identity-management system (IMS) in Mexico and its importance to the financial-sector environment while reflecting on the need for digital identification and authentication procedures and processes. The document will analyze the different options for, and policy implications of, the digital identification of individuals and legal entities in Mexico when meeting financial policy objectives and regulation. This document builds on the principles established by the G20 on digital financial inclusion, the Identity Management System Analysis, and the Common Principles on Identification for Sustainable Development. It takes into account standards and guidelines issued in the financial-sector context that recognize the need to identify individuals and legal entities and intends to provide guidance to Mexican authorities when defining policies that involve the need to identify individuals and legal entities. The report also builds on *Identity Systems Analysis Country Report for Mexico*, which was issued by the World Bank in 2015 and incorporates the identification of legal entities, and focuses on needs related to the financial sector regarding consumer identification.

The document is organized as follows: First, an executive summary presents key observations and recommendations for authorities. A discussion of identification systems in the financial sector comes next, followed by a description of the IMSs in Mexico, including the institutional arrangements, and then by sections on digital identity and the legal framework supporting such infrastructures. Finally, the report concludes with a section on potential actions, which build on initiatives in other countries, which are included along with the report. International standards are attached as appendixes to support the methodology used to elaborate this document.

The World Bank's 2017 Identification for Development dataset shows that 11,082,404 people are still unregistered in México, or 8 percent of its population. While this number does not seem high when compared to other countries, the people most affected are the financially underserved or unserved. It is also noteworthy that Mexico shows a high rate of identity theft, which in 2017 reached 20,000 cases,[1] and all existing IMSs are affected by duplication of numbers.

Authorities in Mexico are seeking solutions to the complex task of improving efficiency in the financial and government sectors when identifying individuals and legal entities, while balancing other public-policy objectives, such as governance, technological neutrality, safety, privacy, and universal coverage. The expansion of digital ID technologies presents opportunities to reach the overall objective while also presenting trade-offs that require thorough consideration from the authorities. The adop-

tion of these technologies, for example, implies policy questions related to governance, efforts to coordinate and collaborate between authorities, ownership and data governance, privacy, and integration of legacy systems.

The identity-management ecosystem in Mexico includes many different government-issued identification credentials and little coordination between the entities that issue credentials. This creates a risk of duplication of efforts, information, and identities, since each entity provides its own type of ID to registrants. It also makes it difficult to verify the identity of an individual in Mexico. Mexico has developed digital features of identification systems through different initiatives, but these are not coordinated under a common vision and strategy at the federal level.

The primary federal foundational identification system for individuals is the National Registry of Population and Personal Identification (*Registro Nacional de Población, RENAPO*). RENAPO is responsible for assigning a unique identity number, the Unique Population Registry Code (Clave Única de Registro Nacional de Población, CURP) and by 2017 had issued 186 million numbers. The population of Mexico is around 130 million. Since non-Mexican residents can also be issued a CURP, it can be assumed that there is an overregistration of CURP credentials.[2] RENAPO does not attach biometrics to the CURP.

Mexico has several functional registries that were created for specific purposes. The National Electoral Institute (*Instituto Nacional Electoral*, INE) issues voter credentials to all citizens of voting age. The INE credential has emerged as a de facto primary source for identity verification for many users, also in the financial sector.

The registration number provided by the Federal Tax Payer Registry (*Registro Federal de Contribuyente*, RFC) is also used as an identification credential for individuals by financial service providers. The database of the Tax Administration Service (*Servicio de Administración Tributaria*, SAT) is also queried to verify identification. Other functional IDs are widely used, including the number from the Mexican Institute of Social Security (*Instituto Mexicano de Seguro Social*, IMSS), which covers members or beneficiaries mostly linked to pensions and social security enrollment.

In the case of legal entities, the RFC number is the primary ID number used for verification in the financial sector. However, deficiencies have also been observed in the RFC number, including duplications and a lack of universal coverage. The Legal Entity Identifier (LEI) has started making its way to the Mexican companies, but few legal entities have been registered through the Mexican-certified Local Operating Unit (LOU). This is due to two main factors: First, the request for an LEI is voluntary except for those clients of credit institutions that are involved in over-the-counter operations—mostly derivatives—and, second, for verification, the LOU that issues LEIs needs the operations manual that was recently issued by the Banco de México. The adoption of LEIs in Mexico follows a gradual approach based on risk, and regulation to make it mandatory has focused on those entities that pose higher risks vis-à-vis anti-money-laundering (AML) and countering the financing of terrorism (CFT). In this sense, the adoption of LEIs is perceived as a long-term goal for financial-sector authorities, while other government authorities concerned with the registration of legal entities, such as the Public Registry of Commerce and the National Institute of Statistics and Geography (*Instituto Nacional de Estadística y Geografía*, INEGI), have learned about the existence of LEIs only recently.

The level of integration and uptake of the CURP into other functional registries is low and does not mitigate the duplication or forgery-related problems. This situation prompted initiatives led by the financial sector, mostly banks, to increase efficiency in identifying their clients while meeting regulatory requirements. These initiatives included the adoption of biometric systems in the banks and an agreement between the INE and banks to validate information captured from the consumers against INE's database (for example, biometrics and personal information). Still, not all banks and financial institutions are able to collect biometric data directly from their clients or integrate such information into a consolidated database.

The adoption of digital financial services also prompted the development of methods to authenticate users of financial services through smart cards, PINs, and biometrics. However, these authentication methods are built on top of information collected from official credential databases to identify individuals and require the acquisition of readers that are not always available or affordable to all users. New technologies might open the path to the adoption of solutions to build a cost-effective digital identity that could be linked to existing official credentials and serve to standardize IMS features across databases.

The current legal framework covering aspects related to identity, identification, and authentication presents gaps that need to be addressed to provide for legal certainty regarding the development and further use of digital identity by all types of users. Although the temporary nature regarding the use of INE credential for verification and authentication purposes by third parties has been clarified in recent regulation, there is still a need to clarify

the role of RENAPO toward the INE database. In addition, for the development of digital IMSs, it might be necessary for additional credentials to be recognized to operate in the digital environment by defining a set of minimum attributes that can be accepted. Financial-sector laws should include specific requirements to identify consumers and ultimate beneficiaries of financial services. Finally, access to personal information related to the identification of individuals should be vested with rules that protect personal information while allowing compliance with know-your-customer (KYC) and related rules for identification proofing and verification and authentication of individuals. In this context, consistent implementation of the Law on Transparency and the Law on the Protection of Personal Data is necessary, in particular when application programming interfaces (APIs) are involved in the usage of personal information for authentication and identification purposes, and data is transferred from public authorities to private actors. It might also be necessary to revisit KYC requirements for digital onboarding when building a digital identification.

The adoption of digital identity in Mexico requires coordinated action and a common vision from all the stakeholders, including public and private actors. To minimize the burden caused to financial service providers, the following actions should be considered:

a. Authorities should develop a national strategy to achieve universal registration and unique identities. In this process, RENAPO, as the holder of the primary mandate to maintain the population database at national level, must be an active partner.

b. Promote digitization of civil registry records and link them with the CURP.

c. Develop a strategy to deduplicate existing databases and develop procedures for interconnectivity; consider a federal database to serve as the primary electronic archive (for example, RENAPO or INE), which should include biometrics.

d. To the extent possible, potential solutions should allow some degree of interoperability to enable queries for verification purposes by financial service providers.

e. Foster the adoption of LEIs and the Advanced Electronic Signature (Firma Electronica Avanzada (FEA).

f. Define legal amendments to enable the digital identity reform. (A list of potential amendments is included under the legal and regulatory framework section.)

g. Any registry or database must build on the principles of protecting personal data and, particularly, implement privacy by design.

h. Databases holding personal information designed to identify and authenticate identities should be considered critical infrastructure and be vested with cybersecurity measures against data loss, data corruption, data abuse, and unauthorized access from third parties.

i. A close collaboration between agencies and ministries is key to enable the reform. This collaboration could be vested with memorandums of understanding to ensure accountability and that the liability of each agency is not undermined.

II. Introduction

Individuals need mechanisms to prove their identity for a wide range of services and activities, including, among others, opening a bank account, receiving government payments, making payments to third parties, accessing credit, or buying prepaid mobile phone services. Identification can also serve to meet other financial-stability and social interests, such as countering the financing of terrorism and strengthening anti-money-laundering efforts. The report *Principles on Identification for Sustainable Development: Toward the Digital Age* defines identity as a "*set of attributes that uniquely describes an individual or entity.*"[3] Societies and economies typically require formal systems—traditionally physical tokens, such as paper-based ID cards that include the signatures or representations of their holders and are verified against documents stored in a central registry. But these formal systems are failing in the developing world. Nearly 1.1 billion people worldwide lack a legal identity (World Bank, 2017), which means that they're often excluded from school, health care, welfare, and financial services. The recent Global Findex report[4] states that 26 percent of unbanked adults in low-income countries and 19 percent of adults in developing countries without an account at a financial institution reported lacking the documentation needed to open one.

The international community recognizes identity as one of the key enablers of sustainable development but also considers it significantly relevant to advancing financial-inclusion objectives and preserving financial stability. In 2015, the United Nations set the following as a Sustainable Development Goal: to "*promote peaceful and inclusive societies for sustainable development, provide access to justice for all, and build effective, accountable, and inclusive institutions at all levels.*" To achieve this goal, it recognized that it is necessary to "*provide legal identity for all, including birth registration, by 2030*." A year earlier, in 2014, the World Bank Group created the Identification for Development Initiative in recognition of identity as a key factor for sustainable development. As countries increasingly rely on digital networks to deliver important public and private services, the ability of individuals to access those services remotely through identification becomes extremely important. In such a context, the G20 High-Level Principles on Digital Financial Inclusion, which were issued by the Global Partnership for Financial Inclusion in 2016, include the need to facilitate customer identification for digital financial services[5] as a key pillar for financial inclusion under its principle 7. In addition, easier verification of individuals and legal entities supports the efforts of regulators and service providers to facilitate more

efficient customer registration while meeting AML/CFT requirements where these efforts follow a compliance or a risk-based approach. Finally, achieving an identification mechanism to be used across a range of sectors and users leads to both benefits and concerns for individual consumers. The ability to verify someone's identity in developed countries is taken for granted, while poor record keeping, a lack of adequate security measures, and weak rules on data access pave the way for abuses, such as identity theft and fraud.

The evolution of the internet from a publishing medium to an interactive platform enabling the delivery of personal services allowed individuals to engage in electronic commerce, e-government, and many other online interactions, from electronic health and electronic learning to social networks and the broader participative web. Many of these transactions involve financial services. Therefore, the availability of digital identification has become critical today to access to financial services. Examples of transactions that require remote identification include making payments,[6] obtaining credit,[7] opening an online bank account, and gaining insurance. In sum, transactions that involve the delivery of financial services require identification of the consumer (both individuals and legal entities). This requirement responds to business needs but also to regulatory requirements—mostly resulting from the implementation of the 40 recommendations of the Financial Action Task Force (FATF)[8] related to KYC and customer due diligence. The report *Payment Aspects of Financial Inclusion* (PAFI) from the Committee on Payments and Market Infrastructures and the World Bank Group,[9] aiming at enabling legal entities and individuals to access and use at least one transaction account, also recognizes the need for identification as a key condition to access such financial services as government-to-person payments, which involve payments characterized by a very large number of transactions, normally of small individual value. Government-to-person payments are typically associated with social-benefit transfers (for example, conditional cash transfers, child-support payments, and student allowances), salaries of government employees, pensions, and tax refunds, among others, operated by a regulated payment service provider.

The need to identify legal entities involved in cross-border financial transactions became evident after the 2008 financial crisis and prompted the launch of the G20 initiative to address fundamental problems related to identification through the Global Legal Entity Identifier System, which was built under the leadership of the Financial Stability Board. The Global Legal Entity Identifier System has developed a single ID associated with a legal entity that allows for consistent identification of parties to financial transactions, facilitating an integrated view of exposures. As in the case of individuals, giving an entity a unique identifier requires an unambiguous and exclusive assignment of an identifier to a single entity, based on a reliable process of identification. Direct physical reality does not necessarily offer a straightforward means of distinguishing an entity (for example, a fund). Sometimes, the essence of an entity may have very little extent in the physical world, other than a notation of its existence or the traces of its actions. Legal personhood or similar legal, regulatory, administrative, or other formal constructions may serve to define the identifiable essence of a specific entity at a given point in time.

A unique identifier is a type of formal and legally accepted label for which a value or code is assigned uniquely and exclusively to a person specified by a unique combination of values of the relevant underlying identifying information. Identification requires matching attributes of a distinct person with a set of recorded information taken to be sufficient to define a person uniquely in a specific context. Such information might be defined in terms of attributes directly connected to the reality of the person or attributes that reflect choice. However, unique identification of individuals is not always present in all countries or efficiently assigned. The World Bank report on identification shows that 18 percent of developing countries have a scheme that is used for identification purposes only; 55 percent have IDs that are used for specific functions and services such as voting, cash transfers, or health; and only 3 percent have foundational ID schemes that can be used to access an array of online and offline services.

Recent innovations have addressed the issue of identification through mechanisms that enable digital identity systems,[10] central registries storing personal data in digital form and credentials that rely on digital, rather than physical, mechanisms to authenticate the identity of their holder. Twenty-four percent of developing countries have no ID system.[11] While some functional identification systems have been developed lately that serve broader purposes than those initially intended, when developing digital identification infrastructure the following key aspects are to be considered:[12] (i) birth registration and other foundational identity systems should be universal and affordable; (ii) government identity databases (for example, birth registration and tax ID registries) should appropriately and securely be made available to other parts of government, subject to client consent when required by data-protection laws; (iii) IMSs that link relevant civil registration and identity systems should be interoperable and technology neutral, where appropriate; and (iv) IMSs should appropriately and securely be accessible to authorized parties, such as financial service

providers, subject to client consent where required by data-protection laws. Digital ID also requires existing conditions, such as (i) digital databases that replace paper files with electronic files and (ii) biometrics, capturing either facial or iris patterns or fingerprints to authenticate a person's identity.

Digital ID schemes rely on a backbone of connected systems, databases, and civil or population registries. In developed countries, moving to digital identification might mean enhancing existing infrastructure and making them serve other purposes more efficiently (for example, France, Singapore, or South Korea). In many emerging markets, a lack of robust civil registration and identification registries and a lack of trustworthy ID credentials led to the creation of digital systems without building on foundational identification systems (for example, Guinea, Kenya, and Uganda) to serve a specific function or purpose or even multipurpose or several functions. In some countries that do not issue national ID cards, other ID credentials have become de facto foundational ID cards (for example, Mexico's INE credential or the Togolese voter card).

Creating an efficient IMS and particularly transitioning to digital Identification schemes require a high level of collaboration between ministries, government agencies, private-sector service providers, and users. Although the form of government-issued credentials varies across countries, they generally enable high-value public and private services offline. To migrate such services online and foster the blossoming of innovative digital high-value services, market participants need to establish end-to-end digital identity-management processes. However, in the absence of a unifying vision or coherent strategy, this can result in duplication and waste of public and private resources.

Building an ecosystem for digital authentication involves an enabling framework for its further usage through managed access, interoperability, and authentication. (See figure 2.) These stages include the following:

i. ***Enrollment:*** The moment when relevant data on the individual is captured and stored. The information stored typically involves biographical data (for example, name, address, gender, date of birth, email, and mobile number) and biometric data (for example, iris, voice, or fingerprints). However, other attributes might also be required. For example, the European Union's eIDAS Implementing Regulation (2015/1501) established that the minimum data set of unique identity attributes for an individual should include both mandatory attributes (current last name[s]), current first name[s], date of birth, and a unique identifier that is as persistent as possible in time) and additional attributes (first and family name[s] at birth, place of birth, current address, and gender). This information is included in an electronic database.

   a. *Validation and verification:* A key aspect of the authenticity, accuracy, and validity process is data validation. As in any type of database, the validation process starts with a cross- (verification) check against existing data—for example, with other registries, such as birth and death registries; with existing information from other individuals with exact attributes; or by validating the veracity and consistency of the given data (that is, telephone num-

FIGURE 1: Principles on Identification

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

Source: Identification Assessment Guidelines, ID4D, 2017 and G20 High-Level Principles on Digital Financial Inclusion

ber or address). This process also validates that all given evidence is correct and genuine and that it can be associated with a living individual or active legal entity.

ii. ***Issuance:*** The process of creating and distributing virtual credentials. Credentials issued are electronic, which means that information contained in the cards can be electronically stored and read. These credentials could include smart cards, 2D barcodes, QR codes, SIM cards, and unique identifiers with biometrical information.

iii. ***Authentication:*** The process of verifying an identity claim against the registered identity information.

iv. ***Authorization:*** Defines the access rights to third parties. With some exceptions for government authorities, these rights should ideally be defined by the data subject.

v. ***Record management:*** This process refers to retrieving, updating, and deleting identity attributes or data fields and policies governing users' access to information and services.

FIGURE 2: Identity-Management Cycle

Source: ID4D, Emerging Technologies, 2018

III. Relevance of Identification Systems to the Financial Sector

Access to reliable identity data is critical for achieving financial-inclusion goals,[13] including those resulting from derisking practices. The use of identification information by financial-sector participants also poses risks to consumers (that is, identity risk). Financial-sector participants traditionally rely on existing credentials to identify individuals and legal entities (for example, national ID documents, tax ID numbers, passports, and social security credentials). However, current conditions—including regulatory costs, the introduction of digital financial services, and inefficient foundational identification-management systems—prompted financial-sector both public and private participants to seek alternative ways to identify individuals and legal entities effectively.

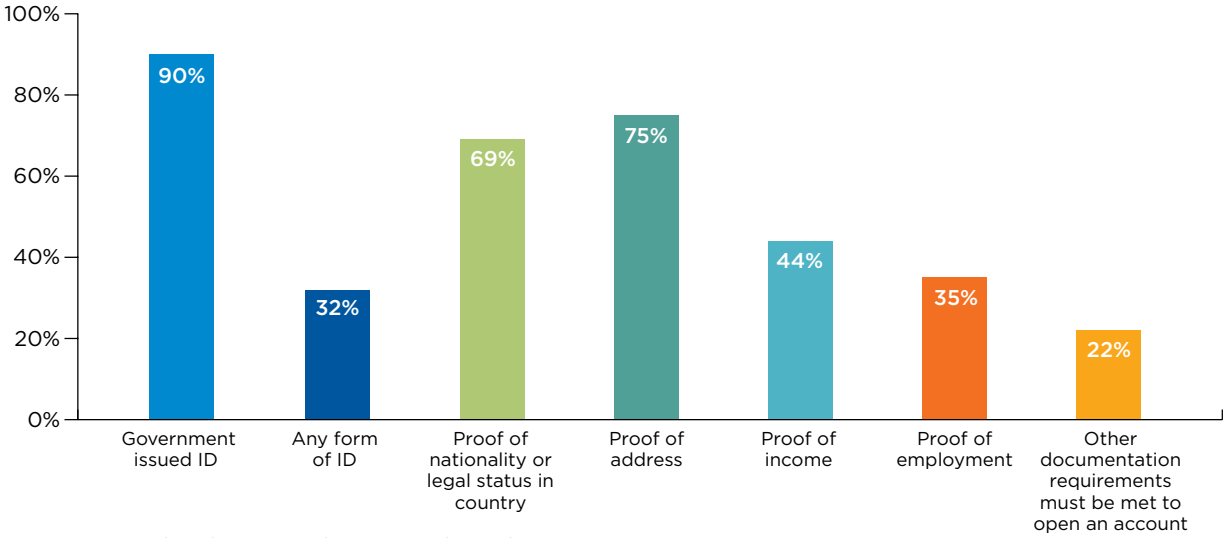
The growth of digital financial services and increased regulatory requirements concerning clients and their counterparties in such different levels as tax AML/CFT, trading, and credit have triggered the search for alternative digital and cost-effective ways of conducting KYC. Having strong KYC processes and protocols has become a key priority for financial-sector participants. In 2012, FATF's 40 revised recommendations for countering money laundering and the financing of terrorism bar financial institutions from keeping anonymous accounts or accounts in obviously fictitious names and require institutions to undertake customer due diligence measures in certain situations, including: (i) onboarding, (ii) carrying out occasional transactions (above certain threshold and wire transfers), (iii) when there is a suspicion of money laundering or the financing of terrorism, and (iv) when the financial institution has doubts about the veracity of previously obtained customer identification data.

BOX 1

CCD MEASURES UNDER FATF RECOMMENDATION 10

Verifying the customer's identity using reliable, independent source documents, data, or information and identifying the beneficial owner and taking reasonable measures to verify the identity of the beneficial owner such that the financial institution is satisfied that it knows who the beneficial owner is. For legal persons and arrangements, this should include financial institutions taking reasonable measures to understand the ownership and control structure of the customer.

FIGURE 3: Type of Document Required to Open an Account



Source: 2017 Global Financial Inclusion and Consumer Protection (FICP) Survey, World Bank Group.

Financial-inclusion objectives require simplified measures that balance financial access with adequate risk-management policies. The PAFI framework issued in 2016 by the Committee on Payments and Market Infrastructures and the World Bank Group recognizes that customer due diligence costs and strict requirements for customer identification can be barriers to financial inclusion for financial institutions.[14] The PAFI report also recognizes the significance of flexible KYC measures for low-risk electronic fund transfers based on an amount threshold (below 1,000 dollars or euros). In some countries, transactions below a certain amount do not require identification of the account holder or the beneficiary.

The availability of credit histories has become a key condition to access credit for both individuals and firms. Credit histories are built by consolidating information collected from different sources and require the identification of the consumer with the underlying payment behavior data items collected and consolidated, typically through credit reporting systems. The *General Principles for Credit Reporting* issued in 2011 by the International Committee on Credit Reporting recognize the need for data included in the credit reporting systems to be unambiguously linked to the consumer (*data subject* is the term used in the GPCR).[15] The International Committee on Credit Reporting also recognizes that, to be effective for disadvantaged individuals, credit reporting systems require reliable mechanisms for identifying individuals and firms, as well as for linking them unequivocally with their financial obligations. Therefore, to achieve this goal, it is important that government authorities (i) *ensure the efficiency and consistency of national ID systems, as well as other public agencies, such as tax authorities and social security agencies;* (ii) *devise effective and efficient methods to register new firms and also link a firm's new ID key with any previous ID key(s) that that firm or its predecessors may have had; and (iii) allow credit reporting service providers access to a wider set of information sources for establishing identities, including ID validations.*

Financial consumers are accessing their services from multiple platforms and devices, and managing identification is becoming extremely difficult and costly, but technology can become an opportunity to leapfrog traditional paper-based approaches and build strong and efficient identification-management systems on a larger scale. Fintech companies aim to provide services in a convenient, remote, and speedy manner, yet they still need to identify unique consumers. Without a digital identification system, the process of validating a person's attributes and characteristics needed to establish his or her digital identity (that is, a set of electronically captured and stored attributes and credentials that can uniquely identify a person)[16] might delay the provision of services and require the collection of a larger set of personal data items.

Digital identity has become a key priority for financial service providers that are willing to facilitate services through new channels, such as online or by phone (for example, via smartphones, tablets, and computers). A traditional way to enable remote identification is by offering some sort of authentication that enables access to those underserved and unserved populations located in rural areas in a safe and efficient manner. In the past, the use of a username and password was widespread, but this mechanism has failed due to its weaknesses. An increased

need of security and the availability of larger volumes of personal information have paved the way for the development of digitally trusted identity solutions that include additional features capturing data on (i) identity credentials, (ii) account details, (iii) biometrics, (iv) behavioral data, and (v) geolocation data (for example, IP, social networks, and mobile numbers).

Individuals become more cautious about the entities with whom they should be sharing information as the privacy risks associated with multiple redundant and potentially inconsistent copies of personal information proliferate. As technology evolves and consumers engage in more transactions online, the potential for fraud grows. As individuals use their identities to apply for goods and services—credit, loans, electronic communication, electronic payments—certain patterns of behavior emerge. Individuals might be victims of ID theft, by which a thief steals an individual's personal information, such as a full name or social security number. The identity thief then uses the information to apply fraudulently for credit, to file taxes, or to get payments and services.

IV. Digital Identity

Robust digital ID systems, if developed in a highly interoperable and scalable manner, can produce savings for citizens, governments, and businesses. Digital ID is increasingly becoming key to the effectiveness of technological innovations, such as open banking and marketplace lending. Technology is being deployed to validate a person's attributes and characteristics—including uniqueness—to establish an individual's digital identity.[17] A lack of IMSs prompted the need to develop digital identity. This is also the case when existing IMSs are inefficient or when there is a need to verify an individual's digital identity using one or more factors to establish that they are who they claim to be.

PINs are the most widely used form of authentication in financial services. They are used by almost any payment card service, particularly in cash transactions at ATMs. Also, mobile-money service providers rely on PINs for consumer authentication. Most of today's smart cards are payment cards that include new chip technology to authenticate PINs. A PIN is transformed into a reference value using encryption keys that are then stored in the authorization systems of the financial service provider, while the PIN is temporary.[18] A PIN differs from a password in that it is transformed into a reference value using encryption keys that are then stored on the authorization systems of the service pro-

FIGURE 4: Characteristics of ID Systems

PURPOSE	RECOGNITION	TECHNOLOGY	UNIQUENESS
• **FOUNDATIONAL** (Civil registration, national ID, universal resident ID) • **FUNCTIONAL** (Voters roll, tax ID, SSN, driver's license)	• Legal recognition • Mandate and powers to the issuer	• Digital • Interoperable	• No two people share the same identity • Each individual has one identity

Source: Adapted from ID4D Glossary, May 2018

BOX 2

BANK ID: SWEDISH SOLUTION FOR AUTHENTICATING USERS

Sweden has a population of 10 million people. Through the e-identification board *E-legitimationsnämnden,* the Swedish government has been working with several service providers to offer a nationwide solution that easily links people's physical identities to their digital identities.

In 2000, one million Swedes had access to the internet, and the banking sector required a convenient solution to identify their clients. First issued in 2003, BankID was enhanced to a smart card by 2005 and, later, to a mobile bank ID that covered 7.2 million individuals in March 2017. The ID is created by each client's first bank and then shared across the banks. The credentials accepted to develop BankID include a passport, a driver's license, or an ID issued by a tax authority based on KYC provisions applicable in Sweden. Other government agencies, such as the tax authority, social security authority, pension agency, and local government agencies, can also access the BankID for authentication and verification purposes. Private-sector entities, such as stock brokers, e-commerce platforms, schools, and mutual fund companies, can also access the verification services.

BankID is an electronic identification solution (based on an official credential plus authentication based on public key infrastructure) that allows companies, banks, organizations, and governments agencies to authenticate and conclude agreements with individuals over the internet. BankID is an electronic identity document comparable to passports, driver's licenses, and other physical ID documents, and it is certified by the Swedish e-identification Svensk e-legitimation.

Source: BankID

vider, while the PIN itself is temporary in nature. There are also downsides to using PINs, such as the lack of familiarity with the technology, illiteracy by consumers, or sharing PINs with other users, which poses security risks.

Mobile technologies related to identity consist of phone- and tablet-based hardware and software solutions used to register, authenticate, and verify an individual's identification. As mobile phones have proliferated, and since more than 50 percent of them are smartphones, mobile identity solutions present opportunities that fit well with financial-inclusion objectives while also meeting needs for convenience and user-friendliness. The following mobile technologies enable the collection of biometric data even through the user itself, which allows the authentication of individuals as they are performing transactions using mobile devices:

a. Username and password.

b. ***SIM authentication:*** The algorithms contained in the SIM card allow for encrypted communication between the user and network. For authentication, the authenticating body generates a random sequence of numbers that is sent to the user's mobile—this is the user's public key. The public key, together with the user's private key and the authentication algorithm contained in the SIM, verifies the user.

c. ***One-time password and tokens:*** Dynamic password technology is used to authenticate a user for one session only. It uses highly compatible devices and tokens although it can increase the risk of cyber incidents due to the required sharing of data.

d. ***Smart ID.*** An electronic identification app available on tablets and smartphones. It enables the authentication of users seeking to access online services. The solution works across devices, but users must register each device individually for the authentication to work. They can register in the app by using their digital ID cards and valid certificates.[19]

e. ***Cryptographic SIM.*** SIM cards use cryptographic algorithms that turn the card into a user-identification tool. Estonia and Moldova have adopted cryptographic SIM cards.

f. ***Registration using mobile device.*** Mobile registration technologies comprise hardware and software solutions that enable the enrollment of individuals into an ID system.

g. ***Mobile Connect*** is a mobile-based identity services driven by mobile network operators globally. In this case, mobile network operators give users control over their own data and enable users, businesses, and gov-

BOX 3

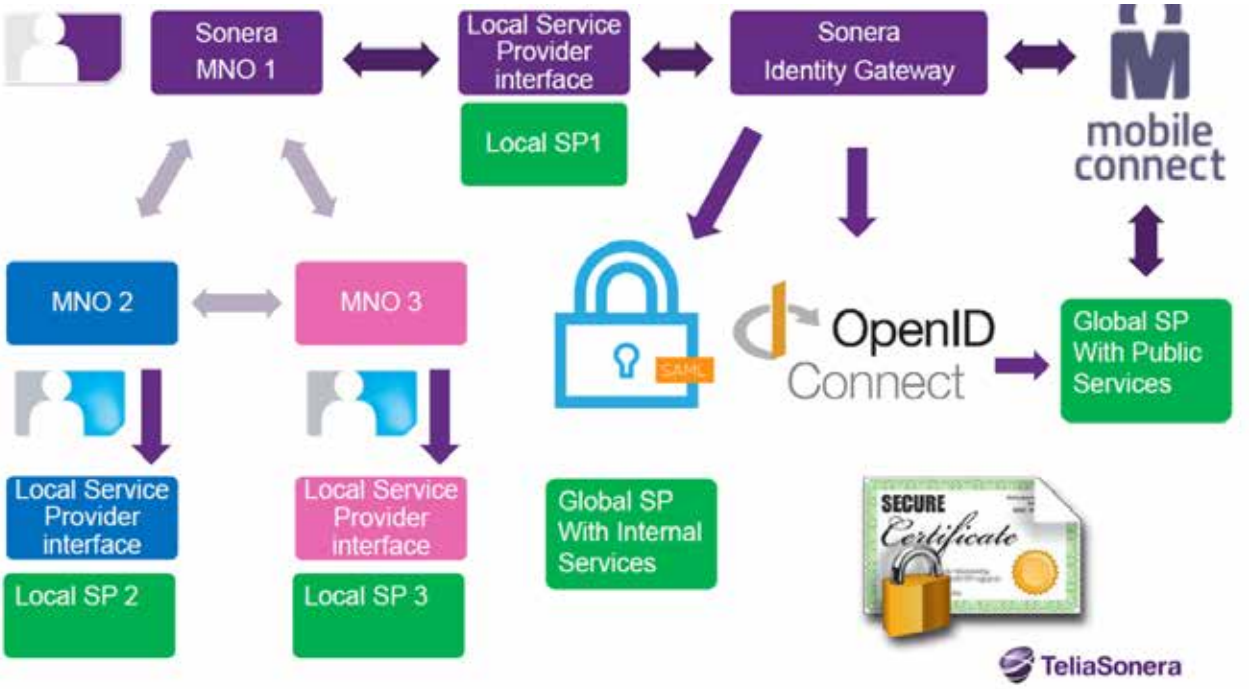
MOBILE ID: FINLAND

In Finland, different electronic ID have been in place since 2001. The Finnish Population Register Center was the only entity with a legal mandate to issue unique identifiers to individuals in Finland. However, the eID required readers that were not available to all users. The financial sector needed an agile method to authenticate individuals, and in 2008, a consortium of government agencies, mobile operators, and the Finnish Federation for Communications and Teleinformatics agreed to launch a mobile identification system. The authentication consists of a two-way authentication based on public key infrastructure (PKI)-SIM card and the telecommunications service provider database. The citizen certificate, incorporated into the SIM card, functions as a qualified certificate, fulfilling the requirements of the Act on Electronic Signatures. An e-signature produced by the service verifies both the signer and the information content of the signed message with the PKI.

Mobile phone users can securely authenticate themselves and legally sign documents by using their mobile phone number and a simple PIN. Based on PKI, mobile ID works in every mobile phone with a SIM card. The private key is stored in the SIM card, and Finnish mobile network operators are trusted service providers that facilitate the authentication. In 2009, the law was amended to allow mobile network operators to issue digital identification services and transfer data to the Population Register Center, which still holds the database for the Finnish population. The ID system in Finland is interoperable to foster infrastructure neutrality.

Source: GSMA

FIGURE 5: Mobile Connect Flows in Finland



Source: Telia Sonera

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

Biometrics. Biometrics are physical and behavioral attributes of a person used as a means of proving one's identity. Interest is increasing around the world in exploring biometrics for authentication as a response to AML and CFT concerns. The introduction of biometrics requires a capture process to enable the authentication later, and this process involves additional costs. Bangladesh, Pakistan, and South Africa are deploying authentication solutions based on biometrics. It is important to consider the accuracy (that is, the liability framework for false positives and false negatives), universality (the presence of the trait universally), stability (permanence over time), and the ease of collection, as well as acceptability and cost components. However, this is becoming the preferred choice for authentication in financial sector.[20]

BOX 4

BIOMETRICS IN INDIA

The 12-digit unique ID number is linked to the individual's biometric readings. This serves as the first block in the India Stack, which consists of a combination of APIs that allow government and the private sector to deploy presenceless products and services (Aadhaar-enabled payment systems, the Unified Payment Interface, e-sign, and DigiLocker).

Cards in various formats can be read by specialized data-input devices or card readers that use technologies that can capture and interpret barcodes or text through optical character recognition, magnetic stripe readers, contact and contactless smart card readers, and other readers using radio-frequency identification (contact cards, smart cards). More recently, biometric-system-on-card technology that combines the biometric sensor and matcher on a smart card is also being deployed. A smart card connects to a reader by means of direct physical contact or through a remote, contactless radio-frequency interface. With an embedded microcontroller, smart cards have the ability to store large amounts of data, carry out their own on-card functions (for example, encryption and mutual authentication), and interact intelligently with a smart card reader. A smart card ID can combine several ID technologies, including the embedded chip, visual security markings, magnetic stripe, barcode, and/or an optical stripe. By combining these various technologies into a smart card ID token, the resulting ID can support both future and legacy physical and logical access applications.

Data analytics for the verification of individuals' digital identity. The increasing use of online social and professional networks, e-commerce platforms, online financial services, and connected devices that can track an individual's geolocation, personal usage features related to health, daily activity, shopping habits, family composition, age, and more enable new possibilities for identifying individuals. While there are no standards on the minimum or type of data attributes to be captured to generate digital identity, figure 6 summarizes the most common types of information included in digital identification systems and used later for authentication. To improve KYC processes, identity analytics is being used with social media data or other data, such as online searches and public data gathered through the internet.

Recent developments also show the adoption of digital identification systems completely delinked from any type of foundational identification systems that also serve as a gateway for the provision of additional services based on authentication of ID. The Aadhaar system in India, which is completely based on biometrics and capturing additional personal information in the form of building blocks, enabled the enrollment of 1.1 billion individuals through its non-reliance on legacy systems and lax requirements regarding evidence documents. The 12-digit unique ID number is linked to biometric readings of the individual. This serves as the first block in the India Stack, which consists of a combination of APIs that allow government and the private sector to deploy remote products and services, such as Aadhaar-enabled payment systems, the Unified Payment Interface, e-sign,

BOX 5

SMART CARD: SOUTH AFRICA

South Africa, with a population of more than 51 million people and international borders with six different countries, is a multiethnic nation. Citizens and permanent residents aged over 16 are required to have a green barcoded identity book that is used as proof of identification for many official uses, such as applying for a driver's license or passport, registering to vote, and opening a bank account. However, fraud and theft have made the paper book system increasingly insecure for individuals and the state, and there is a large number of duplications (that is, one person with multiple IDs and the same ID shared by multiple persons). As part of a major national investment in technology modernization, the Department of Home Affairs, which is the custodian of the National ID System or the National Population Register, decided to put in place a smart ID card system.

The department opted for an eID system—for its high level of security and advanced data-protection mechanisms. In South Africa, two means of authentication will be used—biometric fingerprint verification and a PIN known only to the user. An embedded secure software with its microprocessor securely contains identification details and ensures that only authorized authorities can read and verify the card's data using contactless machine-readable scanners. The inclusion of this biometric identification makes it virtually impossible to duplicate the card and ensures, for the first time, that citizens can be securely authenticated to their eID document.

This new smart card-based infrastructure offers the opportunity to facilitate additional e-government services as part of South Africa's modernization ambition. The Sealys eID supports public key infrastructure and match-on-card authentication techniques to enable easy verification of identification and a future-proof platform capable of providing a broad range of secure online services, such as online and in-person authentication, as well as legally binding digital signatures. Government departments of transport, health, and social development are looking at how to exploit the e-ID functionality.

Source: Gemalto, 2017

FIGURE 6: Summary of Data Items Used for Remote Identity Proofing

Credential	Biographic	Account	Biometric	Behavior	Geolocation
ID document	Name	Password	Facial	Transaction details	IP
Access badge	Last name	Passphrase	Iris	Purchases	Mobile number
Smart card	Date of birth	Pin number	Voice	SMS	Address
Mobile phone		Sequence	Fingerprints		
Security token		Secret facts			

Source: Authors' elaboration

and DigiLocker. All these services linked to the unique ID number is called the India Stack. To verify the identity, the bank or any other institution captures biometrics and launches a query to the centralized Aadhaar database. The verification is made through the use of fuzzy-logic algorithms to match the received information with the existing one in the centralized database. The response to the query is a yes/no response. This verification can be used for payment transactions and digital onboarding. The unique number is linked to a number of documents that live in the locker, and the data subject can choose to share such information or not. The Reserve Bank of India approved the use of Aadhaar as proof of identity to meet the regulatory KYC requirements of Jan-Dhan basic savings accounts.[21] Approximately 200 million bank accounts have now been opened using Aadhaar.

Blockchain based on distributed ledger technology (DLT) is viewed as an emerging technology that can be applied to IMS. At present, the primary use cases for DLT have come in the form of new ways of performing fund transfers, payment settlement, and regulatory oversight, due to its decentralized, replicated, and transparent nature. At the heart of DLT is the idea of repli-

cating transaction data and codes across individuals and organizations in such a way that dispute resolution is embedded and enforced by computer protocol. The key value-added characteristic of DLT is an unchangeable transaction history that is backed by a transaction-executing protocol that is universally available across parties. DLT results in what is commonly called a blockchain or "shared ledger," where all the parties have access to the same transaction histories hosted on servers across peer-to-peer infrastructure. Public blockchains can provide decentralized registration and discovery of the public keys needed to provide digital signatures. For digital identities, this technology might require a single trusted third party. This technology is currently being tested in Dubai and Hong-Kong. In the United States, a consortium of credit unions in partnership with Evernym is using DLT to develop a digital identity system.[22] There are also several initiatives aiming at providing KYC utilities based on DLT. For instance, the start-up KYCK uses IBM Blockchain and Bluemix to enhance the customer-onboarding process in financial institutions.

FIGURE 7: Dubai ID System

In the United Arab Emirates (UAE), the Federal Authority for Identity and Citizenship issued a new unified digital identity for UAE citizens, bridging gaps between the national SmartPass service with the local Dubai ID system. MyID has been linked to the UAE national ID database issuing 5.4 million credentials by 2017. This joint effort has been led by the federal government's Telecommunications Regulatory Authority and the Smart Dubai initiative and using DLT technology.

Source: Federal Authority for Identification and Citizenship

Open ID Connect enables providers to build functional authentication systems for mobile use. This technology builds on a token-based standard protocol for delegated authorization over the internet (0Auth 2.0) without the need to share user's credentials. Only a username and password are stored on their own server for authentication purposes. Open ID Connect includes additional information on the user related to users' authentication, and its services can be used by mobile devices through APIs. This technology has been adopted for log-ins by many large organizations (for example, Google, Microsoft, and Facebook).

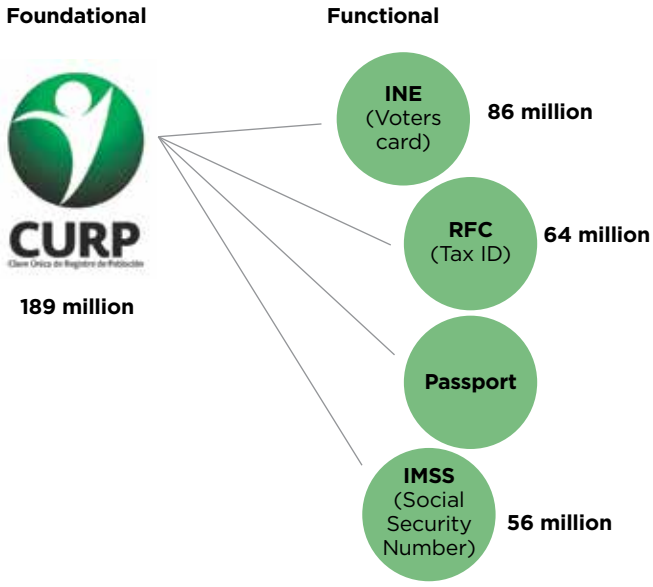
There are also projects led by banks offering digital identification solutions in several countries. In the United Kingdom, GOV.UK was launched by the Government Digital Service in May 2016 to use government services online. The program allows users to select and register with an identity provider of their choice, and then use their "assured" identity to access digital services. Some of these providers are certified companies, and this certification is required to access certain government services. In the United Kingdom, Barclays is a certified company offering identification services and allows non-Barclays clients to access the service via API or web service. In Canada, the government launched the program Secure Key Concierge, which resembles the United Kingdom's approach, whereby leading financial institutions in Canada manage identification verification services to access government services. The system stores more than four million individuals, linking them to more than 80 government services through their banking log-in. In Germany, a cross-industry (banking, insurance, manufacture, postal, telecom) registration system aims at providing digital identification services. It should be noted though that in the European Union, the antitrust authorities need to approve this initiative.

V. Overview of IMS Environment in Mexico

IDENTIFICATION OF INDIVIDUALS

In Mexico, several identification documents are used to prove an individual's legal identity. Figure 8 illustrates the types of foundational and functional identification systems available in Mexico that are frequently used in the financial sector. In addition to the CURP, INE credential, RFC card, passport, and IMSS card, the following credentials also serve to identify individuals and are widely accepted in the financial sector: the military service card, covering 19 million people and issued by the Ministry of National Defense; the school credential, which includes 28 million students and is issued by the Ministry of Education; the *Prospera*,[23] covering 29 million individuals and issued by the Ministry of Social Development; and, finally, the *Seguro Popular*, which covers 57 million people and is issued by the Ministry of Health and state government. Some of these credentials will be discussed to the extent that they cover beneficiaries of cash transfers and other government subsidies that could be delivered though government payment platforms.

FIGURE 8: Key Individual Credentials in Mexico



Source: World Bank Mission, 2017

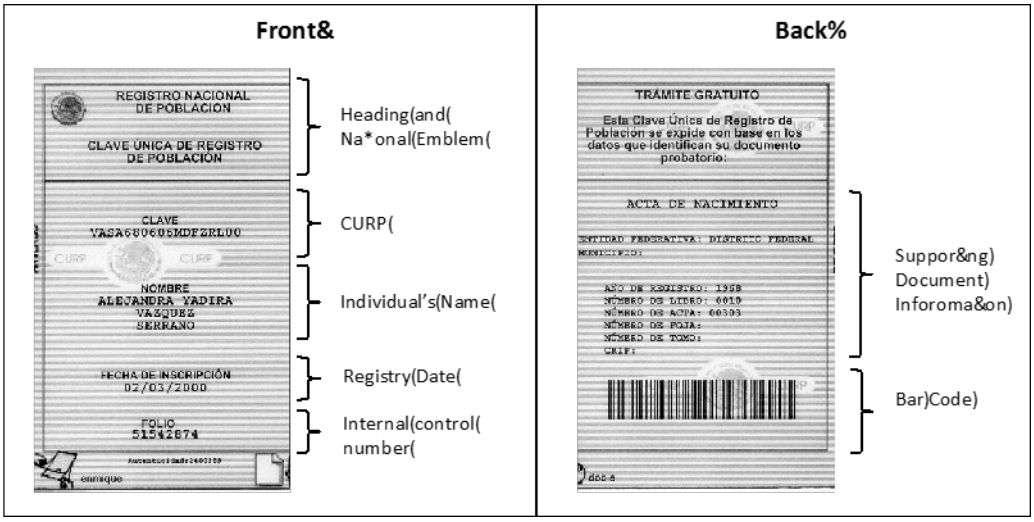
Unique Population Registry Code

The two foundational identification systems for individuals in Mexico are the civil registries and RENAPO. RENAPO is responsible for issuing the unique identity number CURP. Each of Mexico's 32 states has a civil registry, and each of these is regulated by state laws; has different registration and record-management systems, supporting software, and hardware; and varies significantly in terms of performance, capacity, and coverage. RENAPO is responsible for the civil registries and, through the civil registers council (CONAFREC), coordinates the civil registries. CONAFREC has been working on the standardization and convergence of practices and methodologies throughout the registries in the country, but the administrative responsibilities for aspects of the registration reside at the state level, presenting challenges to harmonization objectives. As illustrated in figure 9, the CURP credential is a simple document that contains the CURP code, a name, the registry date, and an internal control number.

The CURP (see figure 10) consists of 18 alphanumeric characters and is verifiable and universal. It is generated using four basic individual data components: (i) a complete name, (ii) gender, (iii) a date of birth, and (iv) place of birth. In addition, the following are accepted as proof documents: (i) a birth certificate, (ii) a migration form issued by the National Migration Institute, (iii) a naturalization letter issued by the Ministry of Foreign Relations, (iv) a Mexican Nationality certificate, issued by the Ministry of Foreign Relations, and (v) a refugee document.

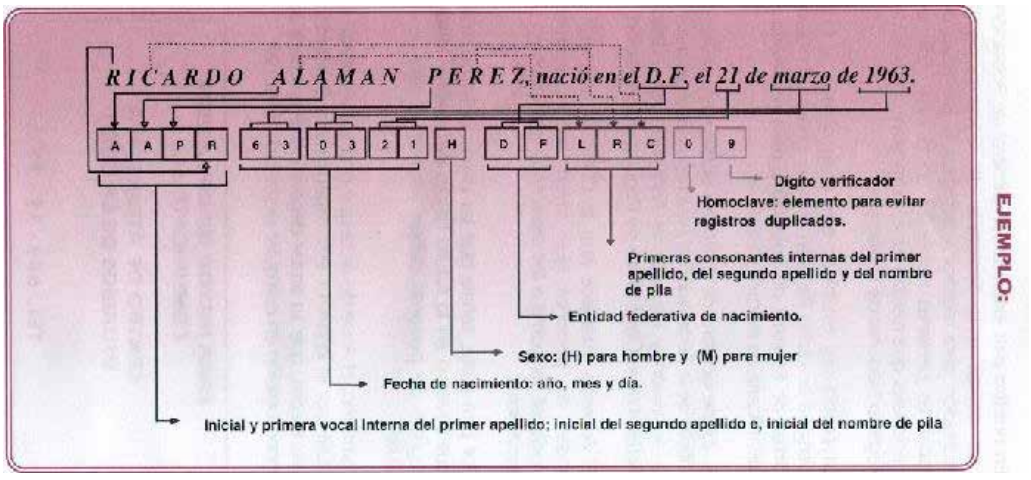
The RENAPO databases were initially decentralized, which led to duplications. Since 2004, a centralization process has been conducted, and the database has been

FIGURE 9: Clave Única de Registro de Población (CURP)



Source: RENAPO

FIGURE 10: Sample of a CURP



Source: RENAPO, 2017

cleaned up by matching it against birth and death registrations. RENAPO information relies now on a management information system called the National Database for the Unique Population Registry Number. This centralized database, which runs in Java, enables the creation, modification, or erasure of information, as well as enquiries and the issuance of CURP certificates to certified RENAPO agents. The e-CURP initiative contributed to reducing significantly the number of duplicates, but duplicates remain, and some registries have not been able to digitize all birth certificates and associate the CURP to birth certificates. This situation translates into weaknesses of the CURP—namely, a lack of uniqueness and appropriate verification processes. Finally, as part of the program, the registries will be connected and include biometric attributes, but this process has not yet started. This situation also impedes the interoperability of the IMS with other registries and the authentication of credentials.

In terms of inclusion, 189 million CURPs are currently included in the National Database for the Unique Population Registry Number, 76 percent of which are assigned through the civil registries, but there are approximately 50 million duplicates.[24] The main piece of proof to enable individuals to issue a CURP is the birth certificate, which, for some individuals, particularly those located in rural areas, might be challenging. Birth certificates are issued by civil registries, and from 1930 until 2016, 143,103,700 birth certificates were issued throughout the 37 civil registries, which have recently been connected and are undergoing a digitized process. In July 2017, six million birth certificates were digitized, capturing the image of the certificate and data included in the certificates. However, the main problem still remains that mandates and laws applicable to each registry differ significantly.

The CURP cannot be electronically authenticated, as it does not have critical aspects that enable authentication, such as biometrics. In addition, although the CURP can be enquired electronically, the supporting documents (birth and death certificates) are not yet digitally available. In addition, the CURP is not supported by an interoperable platform that enables access by different users. One of the major challenges of the CURP is its design, which makes it vulnerable to duplication and forgery.

The INE Voter Card

The voter card is issued by the INE, and it enables citizens to participate in elections. It is valid for 10 years, after which a new credential should be issued. The INE credential was developed in 1992. Before 1992, the voter's credential was issued on paper and through a decentralized scheme that prompted low levels of trust. Since 2001, it has incorporated some biometrics (both index fingerprints), and in 2006, the database was cleaned up, ensuring that the biometrics were also captured in a centralized database. In 2007, a system of inconsistencies were included in the validation process. In 2008, the INE started to incorporate the CURP and cleaned the INE database, aiming to reduce duplicates of the credential. Currently 85 percent of the INE credentials include a CURP. Since 2012, prints from all 10 fingers have been captured, and the quality of the photograph was improved when facial recognition software was introduced in 2016. A total of six generations (types) of INE credentials are currently in circulation. The number of INE-registered voters was 86,296,040 by December 2016.

The database currently holds 91 million fingerprints and 95 million facial images and carries out 60,000 queries daily. The database responds to each enquiry in less than one minute. The INE lacks the potential accessibility for minors, as it was designed to serve as an ID number to vote and was therefore limited to the adult population. However, in the context of financial services, this limitation is not critical, as the majority of services are directed to the adult population. In terms of duplicates, the number of duplicates in the database has been reduced from 442,605 in 2004, representing 4 percent of the database, to 3,567 in 2016, which represents 0.02 percent of the database.

Due to the inclusion of biometric attributes, the INE credential presents higher potential to include fewer duplicates than RENAPO. The fact that the information is digitized and included in a centralized database increases the robustness of this IMS. Also, the INE has developed a

FIGURE 11: Illustration of the Voters Roll Credential (INE)

Source: INE

fee-based verification service that is available to the following institutions:

i. National Commission on Savings and Retirement (*Comisión Nacional de Sistemas de Ahorro para el Retiro*, CONSAR): For enrollment of consumers in retirement plans and changes to retirement funds managed by Retirement Funds Administrators (*Administradoras de Fondos para el Retiro*, AFOREs).

ii. Banks Association of Mexico (*Asociación de Bancos de Mexico*, ABM): Their constituents use this service to verify clients during onboarding and consumer relations.

iii. Public notaries: They use this service to verify the identity of parties in legal documents.

iv. National Banking and Security Commission (*Comisión Nacional de Banca y Valores*, CNBV): It uses the service to formulate and ensure compliance of regulations on KYC.

The INE has signed memorandums of understanding with *Instituto de Ciencias Forenses, Instituto de Servicios Medicos Forenses, Comision Nacional de Tribunales Superiores de Justicia, Fiscalias Generales del Estado, and Procuraduria General* to verify the vital status of deceased and unknown individuals. However, the INE is not a neutral platform, as its operation is managed by the electoral council and its primary objective is enabling citizens to participate in elections. However, the INE credential was established as an official credential by the 1992 Decree on Reforms to the General Population Law (Transitorio 4). Moreover, since 2016, the INE has been authorized to provide verification services to public and private organizations subject to privacy rules established under the Transparency Law and the Data Protection Law, which requires the the following: (i) adopting measures to avoid data loss, data corruption, data abuse, and unauthorized data access, and (ii) enabling consumer consent to access their data.

Social Security Number

In 1943, the IMSS was created with 60 members and currently covers 56 million, including workers, insureds, and beneficiaries. Although information on all these individuals is captured electronically and organized in a systematic manner, the database suffers from anomalies in the data captured and normalization problems (for example, Maria Guadalupe, M. Guadalupe), leading to duplicates. From 1997 until 2007, the registration of workers required only the social security number. In 2007, the law establishing the Institute for Social Security and Services for State Workers (*Instituto de Seguridad y Servicios Sociales de los Trabajadores del Estado*, ISSTE) was introduced.

FIGURE 12: Sample of IMSS Card

Source: IMSS

The CURP was a precondition to issue the social security number in Mexico for workers listed under ISSTE and in 2010 also for those listed at IMSS. Since 2012, the IMSS has been enhancing and cleaning up the database through a cross-check against CURP and RFC, and, more recently, IMSS has been capturing information on new members from existing files at RENAPO and SAT.

To issue a IMSS card, the following evidence documents are required: (i) a nationality credential; (ii) a birth certificate or adoption certificate; and (iii) a letter of migration for foreigners or a certificate of nationality for Mexicans living abroad. The required ID credentials include (i) the INE credential, (ii) passport, (iii) military service card, (iv) and unique identity number CURP.

The IMSS has already existing agreements and protocols to validate certain details of information with other existing identification databases. The IMSS currently accesses information for validation and cross-check from RENAPO (CURP) and SAT (RFC card) and shares information with INFONAVIT, FONACOT, Seguro Popular, SAT, Procesar, CONSAR, and AFOREs through reciprocity agreements between institutions.

Tax Registration Number (RFC)

The tax authority SAT issues the RFC code, which is composed of 13 characters. The first four letters are generated from the first two letters of the first last name, the first letter of the second last name, and the first letter of the first name. The second block consists of six digits that represent the date of birth, organized as YY-MM-DD. The third block is automatically generated by the SAT and consists of a three-digit alphanumeric code. The third block is what makes the RFC code more robust than the CURP. In sum,

FIGURE 13: Layout of the RFC for Individuals

Karen Sánche Ocaña				May 30 1979						Control Code		
S	A	O	K	7	9	0	5	3	0	Q	Z	2

Source: SAT, 2017

the RFC is composed of the CURP plus the SAT code. Figure 13 illustrates the composition of the RFC code.

A total of 67 million on RFC cards have been issued, of which 57.7 million are active, and 56.8 million represent RFC codes of individuals. The RFC card also suffers from duplication, as it can be created by the employer as well as by the employee. It is also subject to errors related to spelling (for example, Maria Karen or Karen) or individuals with same name and date of birth. The registration process is available both online and directly at the Local Administration for Taxpayer Assistance (*Administración Desconcentrada de Servicios al Contribuyente*) of the SAT.

The following documents are required to obtain the registration for individuals:

(1) Birth certificate and CURP

(2) Proof of address

(3) Government-issued identification

(4) Online preregistration number (if applicable)

In case of individuals, such obligation is mandatory for those who are required to file tax returns or to issue electronic tax invoices regarding the acts or activities they carry out, or for the income they earn, as well as for individuals who open a financial account in an institution of the Mexican financial system or in savings and loan cooperatives where they receive deposits or perform transactions liable to tax.

FIGURE 14: Sample of an RFC


gob mx

FOLIO: RF201675492766

CEDULA DE IDENTIFICACION FISCAL

SHCP SAT

Registro Federal de Contribuyentes

IdCIF: 16070124671
VALIDA TU INFORMACION FISCAL

SHCP SAT

ACUSE ÚNICO DE INSCRIPCIÓN AL REGISTRO FEDERAL DE CONTRIBUYENTES

Lugar y Fecha de Emisión
TORREON, COAHUILA, a 07 de Julio de 2016

Se ha procesado con éxito tu inscripción en el RFC
Tipo de movimiento: Inscripción de persona moral

Datos del Contribuyente:

RFC:	-
Denominación/Razón Social:	
Régimen Capital:	
Nombre Comercial:	

Datos de Ubicación:

Tipo de Domicilio:	Código Postal:
Tipo de Vialidad: L	Nombre de Vialidad:
Número Exterior:	Número Interior:
Nombre de la Colonia: ANNA	Nombre de la Localidad:
Nombre del Municipio o Demarcación Territorial:	Nombre de la Entidad Federativa:
Entre Calle: L.	Y Calle:
Características del Domicilio:	Referencias Adicionales:

Página [1] de [3]

MÉXICO COMER

Contacto

IDENTIFICATION SYSTEMS FOR LEGAL ENTITIES

Ideally, the identifying characteristics of an entity should be as closely connected as feasible to the legal, regulatory, or other administrative construction that specifies the existence and extent of the entity. An entity may change fundamental composition over time via corporate actions, such as mergers and spin-offs, or undertake basic changes of internal structure or function, leading to complex questions about what it means to be the "same entity" at various points in time. Moreover, in some jurisdictions, a simple change of ownership of an entity—that remains otherwise exactly the same—is treated legally as a new entity, thus further calling into question the connection between even the physical reality of an entity and its legal embodiment. In some jurisdictions or situations, an entry in a business registry may serve this function. In other situations, such information may be unavailable or unreliable, and other identifying information would be required.

Globally, the LEI is becoming a recurrent way of uniquely identifying legal entities. The organizational structure of the Global Legal Entity Identifier System consists of a federated group of registrars, LOUs; a central operational body, the Global LEI Foundation; and a regulatory body charged with oversight of the Global Legal Entity Identifier System, the Regulatory Oversight Committee. The

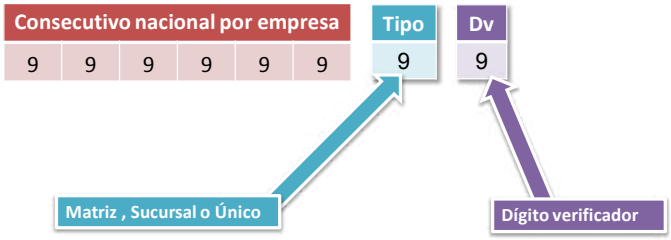
Global LEI Foundation is a Swiss foundation inaugurated in June 2014 and founded by the Financial Stability Board. It is overseen by 70 global regulators on the Regulatory Oversight Committee. According to the US Treasury, 2,133 LEIs have been issued in Mexico.[25]

Statistics Code for Legal Entities (*Clave Estadística Empresarial,* CLEE)

Since 2012, INEGI has assigned a code to each business registered under the National Statistical Directory of Economic Units, created in 2010. This code is called the Business Statistics Code (CLEE) and is composed of eight characters, six of which are consecutive, one represents the type of establishment (headquarters or branch), and the last one is assigned by INEGI based on a predefined criteria. Two additional numbers represent the type of activity and the municipality of the establishment.

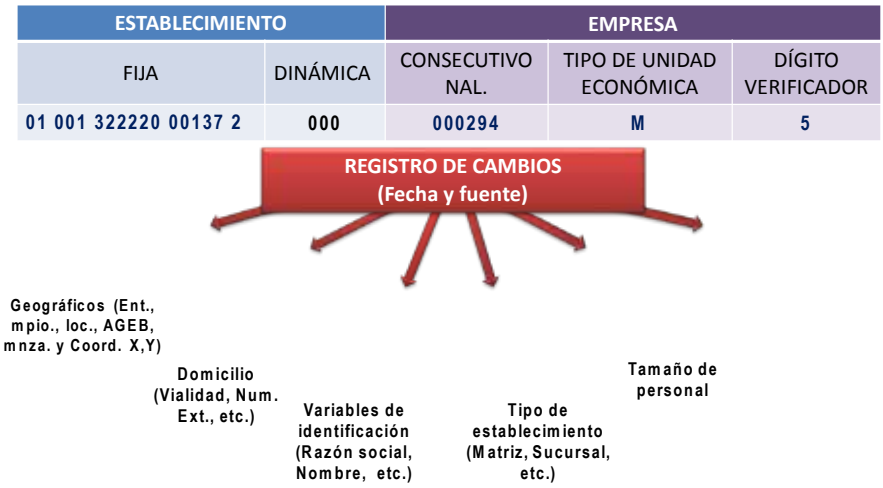
INEGI currently includes five million legal entities based on census data—last one dated 2014—including many that are not registered with the SAT and have no RFC code. The system is based on identification information and the geographical location of the activity. In addition, INEGI captures information from other sources, including the IMSS, SAT, INFONAVIT, and Federal Electricity Commission. Information is stored in a database where all the changes are captured based on the dynamics of the legal entity. This database could be considered a directory more than an identification-management system for legal entities.

FIGURE 15: Composition of CLEE



Source: INEGI

FIGURE 16: CLEE—Historic Database



Source: INEGI, 2017

Public Registry of Commerce

Legal entities are registered at the Public Registry of Commerce (Registro Público de Comercio), which captures core information about legal entities but assigns a registration number, not a unique code, to each one. The main role of the Public Registry of Commerce is to provide legal certainty to legal acts. Legal entities are registered with the commerce registry, generating an entry number and capturing all the relevant events of such legal entity to the entry registration number. Although the system is now centralized through the Registry Management Integral System (*Sistema Integral de Gestión Registral,* SIGER) at the country level, online searches are not yet available. Although information on legal entities is available for public consultation, the number issued by the SIGER is not considered a valid number to identify legal entities. The main objective of the SIGER is to facilitate the use of the Advanced Electronic Signature.

Mexican Business Information System

It is mandatory for all legal entities with commercial activity to be registered[26] at the Mexican Business Information System (*Sistema de Información Empresarial Mexicano*, SIEM), although few registrations are effectively taking place. The number is assigned by the Secretariat of Finance and Public Credit (*Secretaría de Hacienda y Crédito Público*, SHCP), but it is not necessarily linked to an existing legal ID number (for example, the RFC code). The annual fee ranges between 150 and 600 pesos, and information, though captured, is not centralized at the national level. The objective of the SIEM was to connect suppliers and vendors and create a business network. There are 225 chambers of commerce throughout the country that issue SIEM certificates through CAM, CANACO, and CANACOPE networks.

Tax Registration Number (RFC)

The SAT manages the RFC that issues a number to all tax-paying individuals and legal entities subject to the tax code (*Código Fiscal de la Federación*). Information to generate the registration is facilitated by the taxpayer, and the registration request is made either by the taxpayer or the taxpayer's employer. Currently, 67.4 million taxpayers are registered under the SAT (including individuals and legal entities). In July 2017, there were 3.3 million active legal entities with RFC. The SAT has seven different channels to assist taxpayers through 67 administrative offices.

The RFC code for legal entities is 12 characters long. The first three characters represent the business name. The next six characters represent the company's registration date (YYMMDD). The last three characters are assigned randomly by the tax authority.[27]

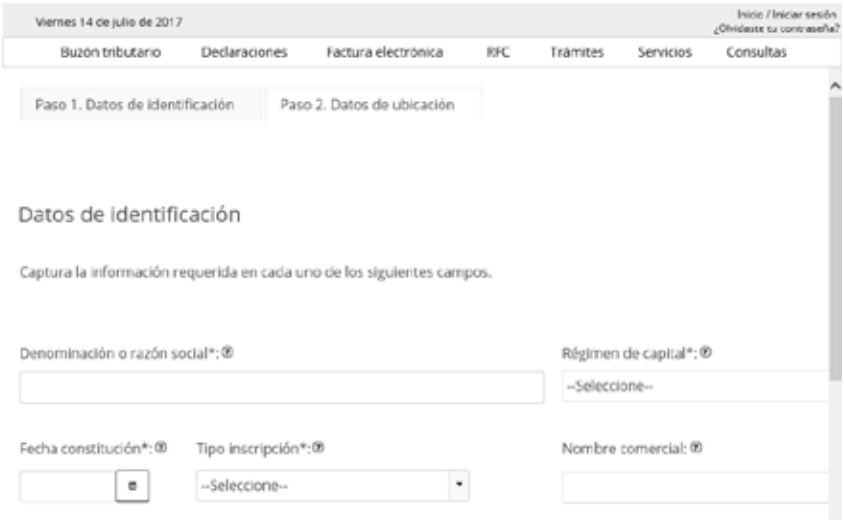
The RFC code is associated with the CURP through a verification process provided by RENAPO. Then information included in the location section is verified against the INEGI street directory, but there are still duplications. To issue an RFC code, a number of documents are required: (1) the certificate of incorporation, (2) a proof of address, (3) a power of attorney and identification of the authorized representative of the legal person, and (4) the online preregistration number (if applicable).

The RFC code is used in the following environments: (i) banking and financial services, such as opening an account or a credit card, and (ii) buying or selling property. The SAT currently offers identity-verification services to Banco de México, CNVB, ABM, and savings banks (*cajas de ahorro*), and notaries are able to make queries to the database through the SAT platform. The SAT exchanges the full content of its database with the INE.

FIGURE 17: RFC Identification Data Captured

Source: SAT

FIGURE 18: RFC Location Data Capture



Source: SAT

Advanced Electronic Signature (FEA)

Digital signatures and electronic signatures (e-signatures) are an electronic sound, symbol, or process attached to or logically associated with a contract or other record and executed or adopted by a person with the intent to sign the record. The signed record itself can produce evidence of each participant's signature. During the signing process, the signer's certificate is bound to the document using the private key uniquely held by the signer. During the validation process, the reciprocal public key is extracted from the signature and used both to authenticate the signer's identity through the trusted Certification Authority and to confirm that no changes were made to the document since it was signed.

For the financial sector, it is also relevant that the FEA is composed of a private and public key that authenticates the signee of a legal act through the verification of the keys. In Mexico, the FEA is issued by the SAT. Figure 19 presents an illustration of the FEA. The first attempts at the FEA were in 2005, when several amendments were introduced to the federal fiscal code, and the SAT created the Confidential Electronic

identification Key (*Código de Identificación Electrónica Confidencial*, CIEC). At the same time, Banco de México also started to authorize private-sector companies to provide this service, although the final mandate was charged to the public authorities until 2009, when the Law on Electronic Signatures was issued.[28] While other agencies under the authorization of the *Secretaría de Economía* can also issue e-signature certificates, the resulting codes should be notified to the SAT. Four companies are currently authorized to provide such services in Mexico.

The adoption of e-signatures in Mexico is still low due in part to a lack of clear guidelines on the implications, acceptance, and legality of e-signatures. In the financial sector, the most common uses of the FEA are (i) consent to access the credit bureau, (ii) credit accounts, (iii) factoring accounts, and (iv) promissory notes. The FEA is also used in formalizing contracts though legal service providers or for employment-related contracts and association membership.

Legal Entity Identifier (LEI)

The LEI is a unique code that is assigned by the LOU at the request of a legal entity. In June 2012, the G20 adopted the establishment of a global LEI system for parties to financial transactions with a global governance framework representing the public interest. This resolution was adopted to solve the problem that financial service organizations face regarding the lack of an effective process to understand their counterparty exposures or the exposures of their counterparties' counterpart. While legal entities are not prohibited from requesting an LEI, this one is subject to cost[29] and needs to be renewed on an annual basis. Certain legal entities, based on the type of cross-border operations they perform, are required to issue an LEI. The LOUs are responsible for the issuance of LEI accreditation. The LOU needs to be accredited to start providing services of LEI registration to legal entities in Mexico. The accreditation process also requires no objection from the Banco de México. In Mexico, the only LOU currently accredited to provide such services is the GS1.

FIGURE 19: Electronic Signature

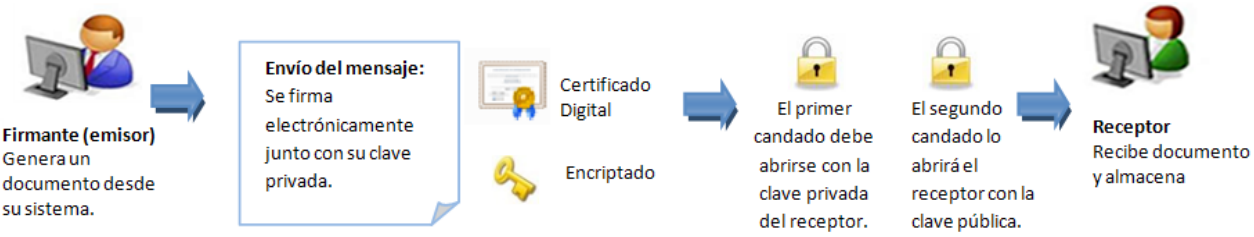
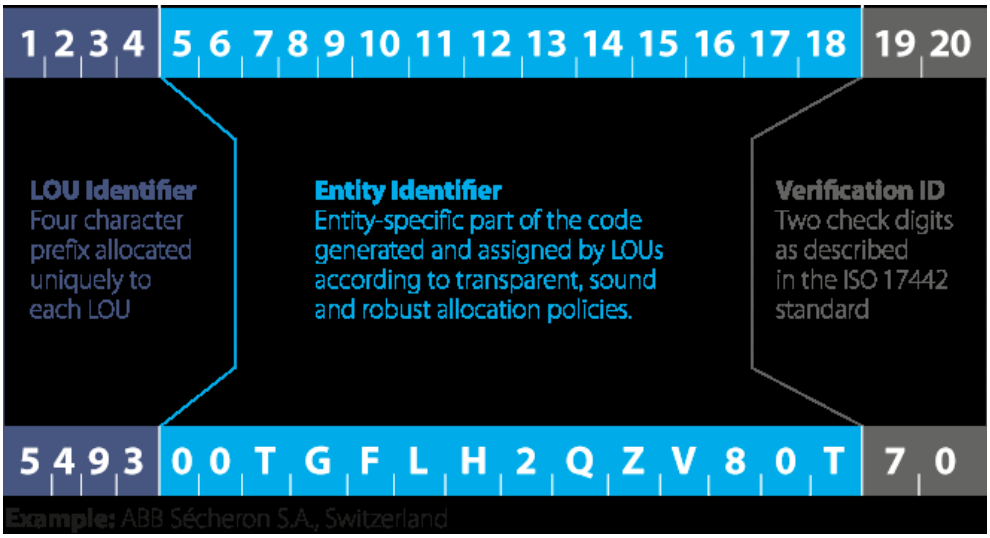


FIGURE 20: Legal Entity Identifier Standard



Source: GLEIF, 2017

The standard ISO 17442 developed in this process was adopted as the core identification framework for the LEI. The standard specifies the high-level definition of the identifier code, an indication of the scope of coverage, and the information required for identification. ISO 17442 defines the LEI as a 20-digit alphanumeric code. The Bank of Mexico modified the rules for identification of legal (moral) entities and escrows to reflect the introduction of the LEI in December 2017.[30]

The LEI is intended to ease the efforts of supervisors and regulated entities when authenticating legal entities in compliance with KYC and similar regulatory requirements. The legal entities request the LEI from the LOUs through the website, and then the LOUs perform the validation using authoritative public sources, such as company registries. In the event the existing company registry is not robust enough or the validation process is cumbersome and unreliable, then the LOUs can use private sources, such as an official certificate of incorporation or a fund prospectus.

VI. Digital Identity in Mexico

RATIONALE FOR DIGITAL AUTHENTICATION SYSTEMS

The commitments of Mexican authorities to financial-inclusion objectives include enabling 75 percent of the population to access financial services. According to the Global Findex, only 39 percent of Mexicans hold bank accounts. Also, the federal government channels government payroll and subsidies to individuals.

The identification and authentication of consumers and legal entities are critical aspects for banks and financial institutions in Mexico, as it represents their entry point to manage relations with them. Effectively identifying them also allows to reduce the risks of erroneously allocating or collecting funds. Banks and financial institutions in Mexico use mostly these four types of credentials to identify their consumers: the CURP, the INE credential, a passport, and, to a lesser extent, the military credential. However, they could legally also accept a large list of other credentials, including (i) a consular certificate, (ii) the senior credential issued by the National Institute of Senior Citizens (*Instituto Nacional para las Personas Adultas Mayores*, INAPAM), (iii) the social security card issued by the IMSS, (iv) the credential from ISSTE, and (v) the driver's license.[31] The main reason for the extensive use of the INE credential and passport is the inclusion of biometric information, such as facial and fingerprint scans.

Identification of individuals and legal entities is also a key objective of authorities for several reasons, including meeting financial-inclusion objectives and measures to control financial stability. In a country in which only 44 percent[32] of adults hold an account at a financial institution, financial inclusion is one of the policy objectives of the government and particularly relevant to the objectives of the Ministry of Finance and the Banco de México. Mexico's financial-inclusion strategy includes a series of measures based on business initiatives and novel products that will allow financial intermediaries to supply services to satisfy the needs of an important segment of the population that still lacks access to the formal financial system. These initiatives require innovative mechanisms to identify individuals, such as the following:

i. Developing savings and payment products and services that adequately suit the needs of the underserved population (low-value, low-volume transactional and mobile accounts)

ii. Facilitating the sending and receiving of international remittances as well as decreasing their costs

iii. Increasing the availability of points of access to financial services (introducing banking agents). In 2015, 3.2 million adults held a mobile banking account. For mobile accounts, depending on transactional limits and the associated risks implied by the account, different opening requirements were established, allowing for the possibility of flexible, low-value accounts (monthly deposits of $600) to be opened without having to go to a bank branch, and with minimal ID requirements (name, address, and date of birth).

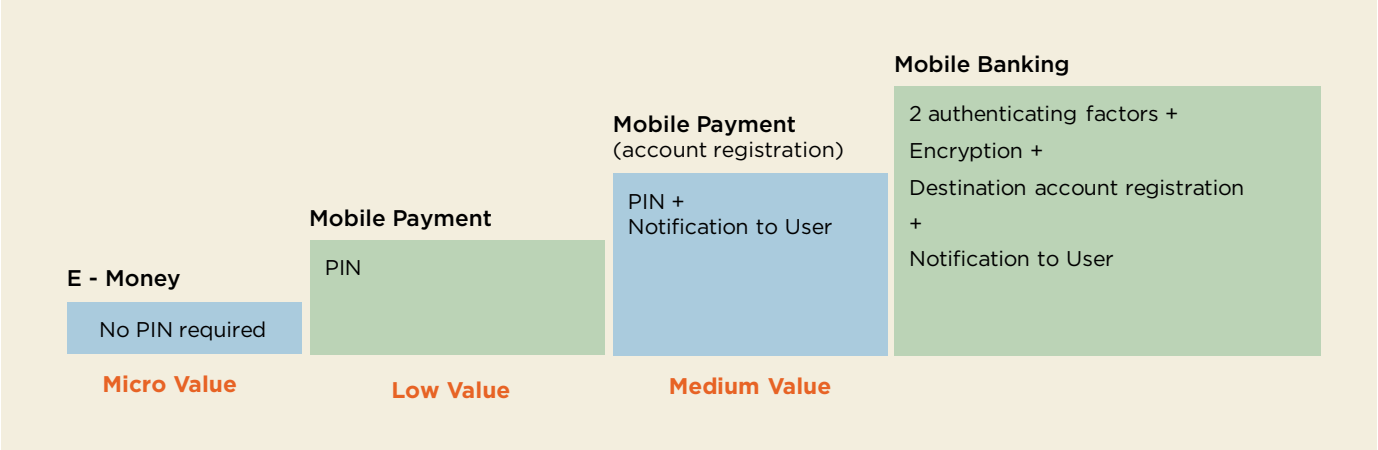
Since the establishment in 2004 of the Financial Intelligence Unit (FIU) to prevent money laundering and counter the financing of terrorism, interest has been growing in addressing the need to identify individuals and legal entities unambiguously. In Mexico, various organizations regulate AML controls, depending on the type of financial institution. The FIU[33] at the SHCP[34] is the main institution regulating AML-related aspects. In addition, CNBV[35] regulates transactions related to (a) commercial banks, (b) development banking institutions, (c) limited-purpose financial societies (*sociedades financieras de objeto limitado*, SOFOL), (d) brokerage houses, (e) societies managing mutual funds (*sociedades operadoras de sociedades de inversión*), (f) distribution societies of mutual fund shares, (g) financial lessors, (h) financial factoring companies, (i) general deposit warehouses, (j) credit unions, (k) societies for savings and loans, (l) foreign exchange houses, (m) multiple-purpose financial societies (*sociedades financieras de objeto múltiple*, SOFOM), (n) entities of saving and popular credits, (o) foreign exchange centers, and (p) money-transfer operators. The Comisión Nacional de Seguros y Fianzas (CNSF)[36] regulates (a) insurance and (b) securities. CONSAR[37] issues regulations for managers of retirement funds. Finally, the SAT issues regulations related to vulnerable activities of nonfinancial legal entities.

Strict KYC requirements and credit risk management can hinder financial-inclusion efforts. The adoption of a layered KYC approach to accounts allows more lenient requirements for the authentication of simplified accounts linked to mobile phones by the Banco de México aimed at facilitating financial inclusion through mobile service providers.

Mexico's payments infrastructure involves several types of participants, including deposit-taking non-bank financial institutions (that is, SOCAPs and SOFIPOs), private payment system operators, and third-party payment service providers/payment aggregators, payment-initiation service providers, payment network operators, and remittance service providers. In terms of infrastructure, the Interbank Electronic Payment System (*Sistema de Pagos Electrónicos Interbancari*os, SPEI) is the main system supporting the national payment system, and the largest user of SPEI is the National Treasury (*Tesorería de la Federación*, TESOFE) to channel government-to-person payments directly to the accounts of the beneficiaries. Initiatives are ongoing to foster the agile payments between merchants and similar ones by the private sector to incentivize person-to-person digital payments.

Most remittances to Mexico are handled by money-transfer operators that provide money-transfer services worldwide. These companies receive foreign currency from remitters primarily in the United States and deliver Mexican pesos to beneficiaries in Mexico through a Mexican agent, usually a bank or retailer with an extensive branch network. Some retail stores and banks also offer

FIGURE 21: Layered Authentication Requirements Approach



Source: CNBV and Banco de México,2010

domestic remittance services; consumers pay for a cash transfer in one of the stores, and the consumer notifies the beneficiary. Ultimately, the beneficiary can withdraw the money from any store or branch using an ID card.

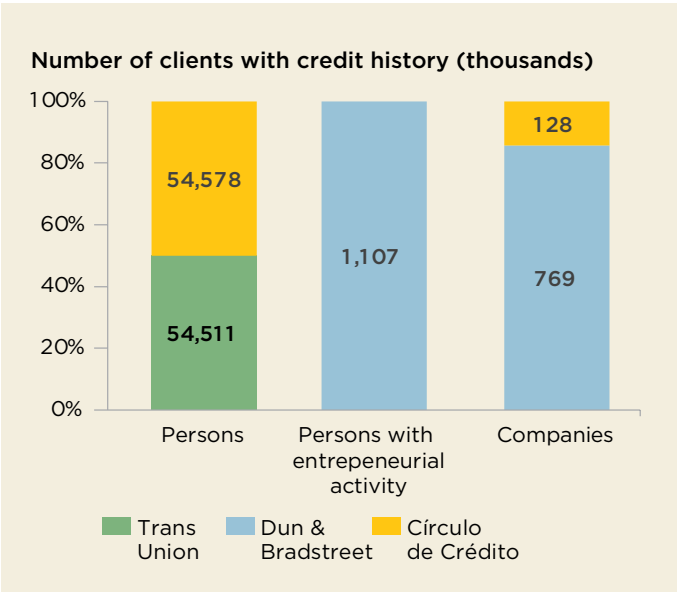
Through correspondent banking relationships, banks can access financial services in different jurisdictions and provide cross-border payment services to their customers, supporting international trade and financial inclusion. Banks cite rising costs and uncertainty about how far customer due diligence should go ensure regulatory compliance (that is, to what extent banks need to know their customers' customers—the so-called KYCC) as main reasons for cutting back their correspondent relationships. The Working Group on Correspondent Banking of the Committee on Payments and Market Infrastructures recommends that relevant stakeholders should use the LEI for all banks involved in correspondent banking as a means of identification. The LEI should be provided in KYC utilities and information-sharing arrangements. Customer due diligence requires that correspondent banks identify and understand their respondents' banking activities and whether the respondents maintain additional correspondent banking relationships.

Innovation has opened the path to new inclusion opportunities for underserved and unserved populations, reduced costs and increased efficiencies for traditional financial service providers, and allowed the entry of new players in the financial sector. Several technology companies offer financial-related services that need to identify consumers effectively. Currently, 158 fintech platforms are operating in Mexico, of which 30 percent are focused on payments and virtual currencies; 28 percent on crowdfunding and online loans; 13 percent on financial management for companies; 4 percent on royalty-based crowdfunding; and 25 percent dedicated to other activities. Identifying the parties involved in these transactions might be complex. Innovation has also resulted in payment transactions that involve card-not-present transactions, and globalization has contributed to a larger presence of cross-border transactions involving individual consumers and legal entities. In this context, several measures have been conducted that call for innovative and simplified yet effective mechanisms for KYC compliance.

The opening of platforms and APIs enable new applications to be built on existing services. Digitally collected data can complement or replace traditional methods of consumer identification, and biometrics allow providers to meet due diligence requirements. However, since no fintech law is in place in Mexico yet, this information is not widely used by the different institutions. Other challenges include a lack of harmonization of standards between different platforms and service providers, including the key identification enabler, as well as the absence of a clear legal framework on the use of personal identifiable information for different purposes.

The credit reporting systems in Mexico collect information on individual's and legal entities' credit history. In 2015, 154,242,881 individuals and 3,764,454 firms were included in the country's credit reporting system. Credit bureaus serve as a key tool to support financial-inclusion objectives by allowing creditors access to consumer behavior information and therefore enabling institutions to extend loans and credit-based products that conform to the consumers' repayment risk profile. Figure 22 illustrates that the coverage of individuals in their database is high. Information is captured at the account level, and each account needs to be linked effectively to a consumer (that is, an individual or a legal entity). Also, credit bureaus collect a section of information composed by identification information. Such data items typically include (i) the name and last name, (ii) previous names, (iii) an address, including the street, number, code, city, and municipality, and (iv) a previous address. In addition to this information, other types of information are captured, including (i) the date of birth, (ii) gender, (iii) employer, (iv) spouse's name, (v) mother's name, and (vi) father's name. This information has proved to be helpful to reduce duplications and detect fraud. The credential used in the credit bureau is the CURP and the RFC card, but there is no legal requirement to capture the RFC card or CURP in the credit bureau. The bureaus

FIGURE 22: Credit Histories Captured in Credit Bureaus



Source: Banco de México, 2015

have been incorporating the CURP into files and now cover 70 million individuals.

The Banco de México has developed a gradual approach toward the adoption of the LEI as a main identifier of financial counterparties. This approach stems from the 2008 financial crisis as a need to identify cross-border exposures at the entity level, instead of the conglomerate aggregated level. At this moment, the Banco de México has not explored the potential for the future use of the LEI by banks and financial institutions to issue loans or by large corporations to identify suppliers and sellers or extend commercial credit, as the bank is currently focused on over-the-counter cross-border counterparties only.[38]

Because identification theft has become a serious concern in Mexico, the authorities have taken several initiatives to reduce it. The Commission for the Protection and Defense of Users of Financial Services (*Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros*, CONDUSEF) reported that in 2016 it had received 4,082 claims involving potential identification theft. Identity theft is a growing concern in this age of digital technology and applications. Credit bureau databases are constantly updated and used. This fact enables the detection of errors but also of potential fraud, even when monitoring techniques employing data learning from patterns are adopted for identification. For example, credit bureaus commonly address credit card fraud and ID theft by identifying mismatches in some of the geodemographic variables included in the application by the credit applicant, patterns related to different addresses in short periods of time, and so on. Traditional authentication methods, such as passwords, passphrases, identity documents, and so forth, are insufficient to combat this threat.

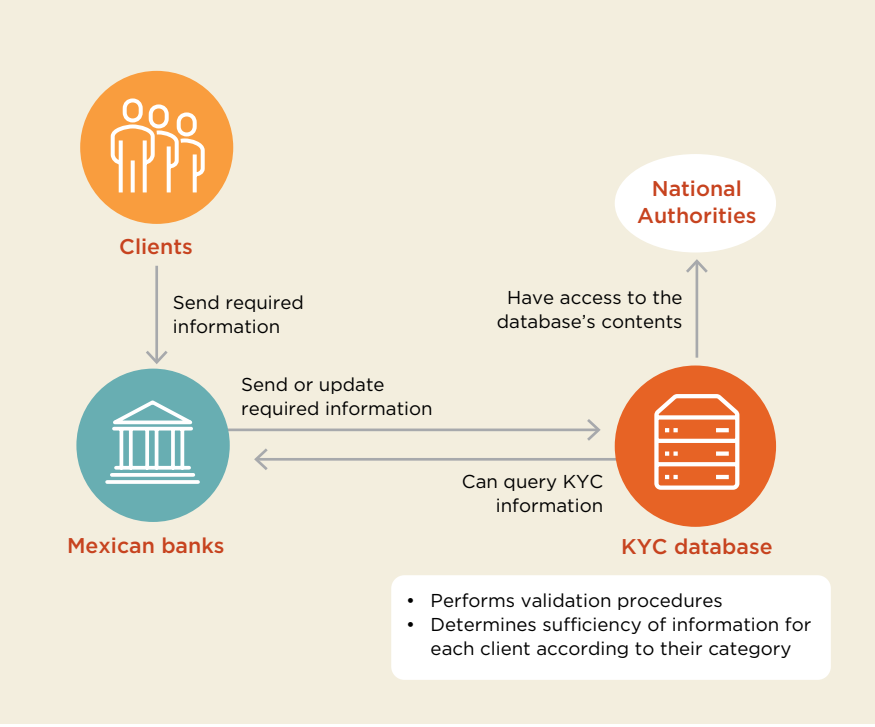
The implementation of the fintech law and financial-inclusion objectives also calls for digital financial services that entail the remote provision of financial services. The G20 High-Level Principles for Digital Financial Inclusion suggest that an interoperable national database system linked to civil registration and identity systems could be a key enabler to financial inclusion. An interoperable, technology-neutral national database system, where appropriate, that links relevant civil registration and identity systems and is appropriately and securely accessible to authorized parties, such as financial service providers, subject to client consent where required by data-protection laws, should be considered as a key action to enable digital financial inclusion.

INITIATIVES TO ENHANCE CURRENT IDENTIFICATION IN THE FINANCIAL SECTOR

An array of new initiatives is being deployed to reduce costs and increase efficiencies in identifying individuals and legal entities. While traditional financial services have relied on identification credentials such as the CURP, passport, military service card, and RFC card, financial-inclusion objectives and innovative financial services, coupled with the unintended consequences of strong enforcement of AML/CFT regulations, have prompted different institutions, both private and public, to mount initiatives aimed at leading the digital identity stewardship. The following paragraphs summarize the most relevant activities and initiatives conducted in the financial sector that require the identification of individuals or legal entities.

The Banco de México and SHCP are developing a transaction database and KYC database for cross-border transactions.[39] The goal of the database is to maintain an updated and complete file on each client. It would allow banks and authorities to make enquiries that are

FIGURE 23: KYC Database



Source: Banco de México, 2017

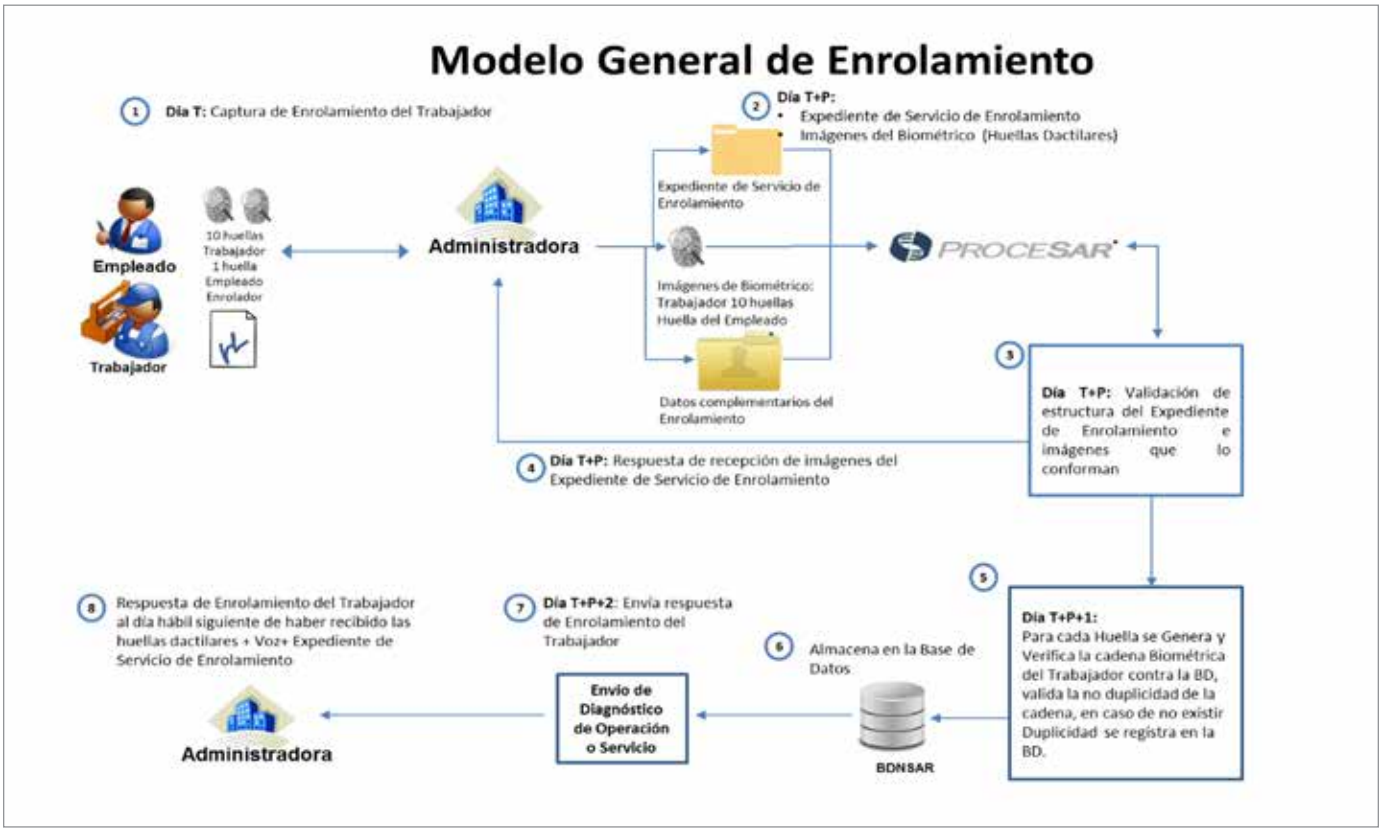
suitable to their needs, with previous authorization from the consumer. In addition, a database on KYC, including identification information on individuals and legal entities, combined with other pieces of information, is also under development. Banco de México intends to address the FATF requirement for "sufficient controls and monitoring systems for timely detection and reporting of suspicious activity" with transaction-monitoring solutions that, through careful optimization, allow for rules-based analysis across all clients and accounts.

The key credentials to be used for identifying consumers in the KYC database are the CURP and RFC card. As the LEI evolves, the system is designed to allow the storage of the LEI in addition to the RFC code. The objective of the KYC database is to standardize the quality of information about each client in the financial system, aiming at making a bank's KYC processes more efficient and reducing the regulatory enforcement burden on authorities. Ultimately, these two databases will also cross-reference each other.

The ABM, a private organization that represents commercial banks, has been working on a standardized technology for all banks to identify financial consumers through biometrics to comply with the CNBV regulation on article 51 bis of the Credit Institutions Law *(Ley de Instituciones de Crédito)*. The industry has already made an initial Mex$1 billion investment ($56.2 million) in fingerprint technology to comply with legal requirements on identification—two pieces of consumer identification—to open a Level 3 or 4 account with more than Mex$17,000 ($955) or any amount of credit applications. In 2012, Bank of Mexico issued a regulation establishing that banks in Mexico need to allow their deposit account holders to associate their cell phone numbers with their accounts to facilitate electronic transfers of funds across bank accounts.[40] In addition, for transactions above 1,500 UDIs (investment units, *unidades de inversión*), banks should verify fingerprints against the INE database. This requirement also applies to digital onboarding for deposit accounts and credit accounts above 60,000 UDIs.

CNBV has implemented a new initiative that will install biometric fingerprint readers in banks across the country in an effort to curb the growing frequency of identity theft. CNBV said that within the next 12 months, all banking institutions throughout Mexico will require an on-site fingerprint reader to verify the identity of clients. The biometric identification method will be used for all banking

FIGURE 24: Registration of AFOREs Accounts

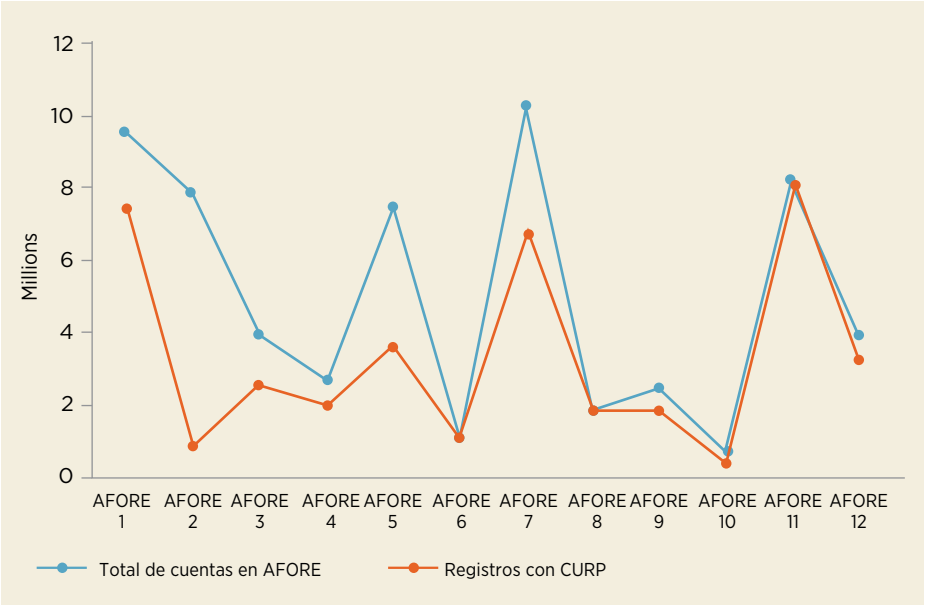


Source: Procesar, July 2017

clients who request services, including applying for credit cards and payroll, as well as a range of loans (personal, group, home and auto, and micro-credit loans).

Procesar has developed the Savings for Retirement System[41] database, which includes all AFOREs accounts and the operations between such accounts. The Mexican pension fund system is composed of individual accounts created through mandatory contributions of 8.5 percent of workers' wages. Workers can choose their pension manager fund (AFORE), and they can also switch AFORE if they find a cheaper option. Eleven AFOREs include 41 million members, and 3.5 million of them participate through the ISSTE[42] or are independent employees. During the enrollment process, biometrics from both employees and employers are captured and stored, and data is verified against existing data in the system.

FIGURE 25: Number of AFOREs Accounts Linked to curp



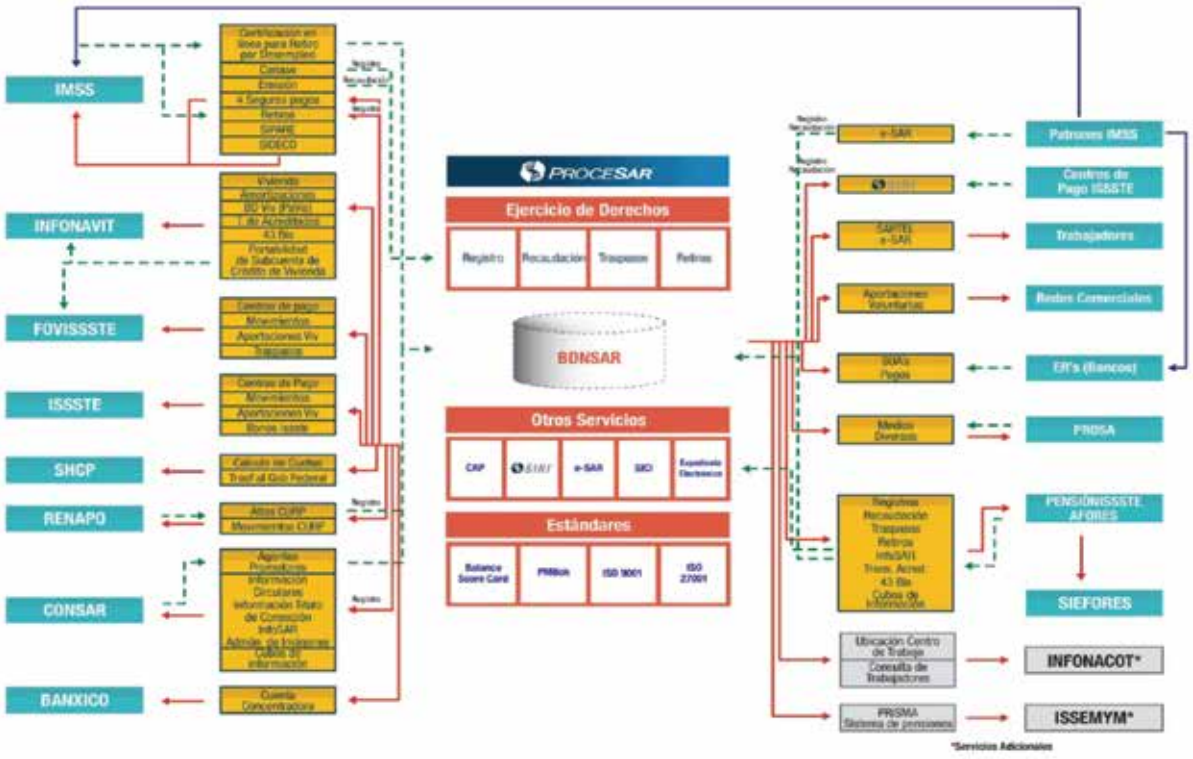
Source: Procesar, July 2017

Different credentials have been used through the years to identify workers prior to their enrollment on the Savings for Retirement System database. From 1997 to 2007, the most common credential was the social security number issued by the IMSS. In 2007, the ISSTE law mandated that the CURP should be the main credential used by all workers registered at ISSTE, and since 2010, the CURP has been the key identification credential for ISSTE employees. In 2016, the CURP also became the key identification credential of all members.

The Savings for Retirement System database is also connected to other government agencies to enable verification processes linked to the management of AFOREs accounts. The automated and centralized services provided by a third party (Procesar) registers all individuals, AFOREs, and ISSTE and enables the identification of employees from different government agencies or who are listed through AFOREs through the database. The private pension supervisor, CONSAR, has recently developed a plan to biometrically identify members of the AFOREs. Beginning in mid-2016, these firms will be responsible for capturing biometric data (10 fingerprints and digital quality photos) for their members when they interact for the purpose of changing funds or applying for different services. There is also a central automated fingerprint identification system that will be used to deduplicate these individuals. The mandate was motivated by the false registration of pension fund members by some agents (at a financial cost to members for each switch), as well as the desire to minimize duplicate pension accounts. In July 2017, 59,863,340 accounts were registered, and 39,889,875 are linked to the CURP.

Based on this, and for all the reasons mentioned in the paragraphs above, it is of paramount importance for the financial sector to adopt a suitable yet reliable manner to identify and authenticate individuals and legal entities through digital platforms. The adoption of a digital identity could serve as a convenient solution for the financial sector and government to provide digital services.

FIGURE 26: Information Flows of sar Database (BDNSAR)



Source: Procesar, June 2017

VII. Legal and Regulatory Framework

Mature ID systems are supported by a strong backbone of data-privacy and e-transaction laws as well as policies mandating participation in the country's civil registries. Identity is recognized under article 14 of the Mexican Constitution. The legal framework described in this section is divided into three main sections: (i) issuers of IMS (foundational and functional), (ii) users of IMS, and (iii) aspects related to consumer protection, including privacy and data protection.

Legal Aspects of the Mandate to Issue Credentials/Digital Identity

Article 4 of the Mexican Constitution recognizes the right to identity. This article was included under the Decree of June 17, 2014.

According to article 85 of this law, the Ministry of the Interior (*Secretaría de Gobernación*) is responsible for registering and certifying the identity of all residents in the country and all nationals living abroad.[43] RENAPO is the government agency in charge of issuing a unique legal identifier for every individual and incorporating it into a National Population Registry as established under the article 91 of the Law on General Population. In addition, RENAPO has the mandate to issue regulations, methodologies, and protocols for the National Population Registry and to coordinate with all agencies and institutions within the federal structure in relation to those matters. In 2006, a protocol[44] for registering and sharing information between Mexico's foundational and functional IDs was issued, further developing articles 92 and 94 of the General Population Law.

In December 2005, the Intersecretarial Commission instructed RENAPO to develop and publish a technical protocol for registering and sharing information. This protocol was published in 2006 and updated in 2009. The 2009 Protocol for Registering and Sharing of Information is the basis for current institutional arrangements between Mexico's foundational and functional IDs. The protocol and its implementation are based on articles 92 and 94 of the General Population Law. The first refers to the Ministry of the Interior's responsibility of establishing the norms, methods, and technical protocols for the integration of the National Population Registry and for the identification and registry of individuals in federal institutions. The latter refers to the responsibility of the public sector (federal, state, and municipal) to contribute to the consolidation of the National Population Registry.

The Protocol for Registering and Sharing Information between foundational and functional IDs accepts the following identity documents for official use:

a. Military service card
b. Passport
c. Professional card
d. Student card with picture
e. IMSS card
f. ISSTE card
g. INE credential
h. Certification of residence issued by local authority
i. Testimonial by an indigenous and municipal authority

The protocol also enables RENAPO to provide certain services to third parties (that is, functional ID issuers), including (i) removal from the registry in the case of deceased individuals, (ii) CURP data requests, and (iii) validation of the CURP based on geodemographic data.

RENAPO establishes the guidelines for assigning and using the CURP in birth certificates and other vital status documents. Additionally, it designs and implements the systems interconnecting the civil registries and the National Population Registry and acts as the regulating and sanctioning body for all civil registration activities. In addition, it establishes the norms, methods, and technical protocols of the National Population Registry and coordinates the registry and identification methods of all agencies and institutions within the federal structure.

The INE issues the Mexican voter card and is subject to (i) the Federal Law on Transparency and Access to Public Information, and (ii) the Federal Law on Personal Data Protection. Article 30 of the General Law on Electoral Institutions and Procedures (*Ley General de Instituciones y Procedimientos Electorales)* establishes the responsibility of the electoral board (*junta electoral*) to develop and maintain a voter roll. In addition, a transitional provision (article 4) was included in the General Population Law in 1992 that enabled the INE to be used as de facto foundational identification credential. The provision established that "*in the meantime, while the citizen identity card is not issued, this card INE can function as a mean of personal identification for administrative transactions, in accordance to the agreements that the electoral authority subscribes to this effect.*"

Article 20 of the Code of Commerce establishes that the Public Registry of Commerce is responsible for developing and maintaining the electronic system under the Secretariat of Economy (*Secretaría de Economía*) to capture, store, and secure information related to business registrations.[45] The system should enable enquiries as well as the issuing of certificates, verification services, and the exchange of information.

Article 17D of the Federal Fiscal Code establishes the need to provide documents in an electronic format subject to the advanced electronic signature. For such a signature, it is necessary to have in place a certificate ensuring the link between the data and the signee. Such a certificate should be obtained from the SAT or an authorized certifier approved by Banco de México. An advanced electronic signature has an effect equal to that of a handwritten signature. The federal code also establishes that, when the certificate has been obtained from an entity different than the SAT, the person should physically verify its identity at the SAT. The SAT should be informed about the code issued by the approved certified entity.

Legal Aspects Related to the Use of Identification Mechanisms in the Financial Sector

Compliance and risk prevention are two key factors that compel banks and financial institutions to seek effective ways to identify their clients, including individuals and legal entities. A number of financial-sector laws and regulations require the identification of individuals and legal entities, but so do potential fraud and ID theft. These factors create incentives for banks and financial institutions to use existing IMS to verify the credentials provided against official records. Other emerging trends to authenticate and identify individuals could also mitigate the risk of fraudulent payments, illegal transactions, and identification theft.

A set of different laws and regulations have been amended to reflect the considerations brought up by the FIU to comply with the FAFT recommendations and articles 139, 148 and 400 of the criminal code. While it is not the object of this report to discuss the AML/CFT regulation, it is worth mentioning that to meet AML/CFT requirements included under a number of laws related to the financial sector,[46] a standardized and possibly digital approach to unique identification systems would largely benefit the financial sector.

Article 115 of the Credit Institutions Law mandates the SHCP to establish KYC rules that also call for the collection of information sufficient to enable the adequate identification of clients. This article also includes the creation of a blocked persons list that will be created by the SHCP, and credit institutions would not be allowed to provide services to these persons. This article was amended in February 2017 to include additional credentials to identify individuals and legal entities, such as (i) the INE credential, (ii) a passport, (iii) a professional credential, (iv) a military credential, (v) a seniors credential from the

National Institute of Older Persons (*Instituto Nacional de Personas Adultas Mayores*), (vi) an IMSS credential, (vii) an ISSTE credential, (viii) a driver's license, and any other approved by CNBV.

In 2010, CNBV, Banco de México, and the SHCP developed a harmonized framework for simplified accounts that allowed a flexible scheme for open financial services while linking these products with mobile phones. These rules, established by the SHCP, allowed banks to open different types of accounts depending on the transactions performed within the account. Requirements increase, and transactions and channels are eased, based on the type of information collected from the consumers: (i) Low transaction average accounts required only a name, date of birth, and address, but transactions in these accounts are limited to 2,000 UDIs per month ($370). (ii) Low-risk accounts required the name, date of birth, country of origin, nationality, occupation, type of business, address, and telephone number of the consumer. (iii) Medium-risk accounts required face-to-face account opening, transactions were limited to $3,700 per month, and channels included any electronic means (mobile, card, and bank transfers). For these accounts, full KYC is required. The final type of account is the traditional bank account, which requires complete KYC and allows for no limit on transactions, which can be made through any electronic means plus checks.[47]

Regulations issued in 2017 to enhance mechanisms to identify consumers deployed by credit institutions include several provisions related to identification that are worth mentioning. In particular, article 51 bis establishes that, for all services except for Level 1 and 2 accounts, credit institutions should require the following credentials: (i) the INE credential, which should be verified by the financial institutions based on the verification process established under article 51 bis 4, (ii) the CURP, or (iii) migratory documents. Article 51 bis 1 establishes measures for Level 3 and 4 accounts with different degrees of flexibility depending on the amount of the transaction or the credit, but they require the INE credential and a verification process against the INE credential, including matching the credential identification code, full last names, and biometric matching of at least 98 percent using existing reading machines.

For the remote identification of clients, article 51 bis 5 establishes that, for Level 3 bank accounts and consumer credit below 3,000 UDIs, the following data should be collected: (i) full last names, (ii) a date of birth, (iii) gender, (iv) nationality, (v) the CURP, (vi) a mobile number, and (vii) an address, including street, number, municipality, province, postal code, and country. In addition, the submission of such data is considered consumer "consent." Finally, a picture of the customer's INE credential should be sent together with the form. Financial institutions should also verify the INE credential and can accept information sent though the Advanced Electronic Signature. Table 1 summarizes the identification requirements for Level 3 and 4 remote accounts.

In 2015, the Banco de México issued regulations establishing rules to identify legal entities through the LEI. Circular 14/2015, on credit institutions related to rules applicable to LEI code, establishes that each credit institution and its counterpart should have an LEI issued by the LOU. In addition, credit institutions should verify annually the status of the LEI of those counterparties with whom they would be conducting business. Additional operational rules are established under this regulation to ensure the validity of the LEIs, including the following: (i) LOUs should follow rules established under the manual; (ii) LOUs should have a website available providing information related to the provision, maintenance, and renewal of LEIs; (iii) LOUs should verify information of any new applicant for an LEI and its counterparts; and (iv) LOUs should share LEI codes with the Banco de México. Finally, this regulation establishes conditions for establishing LOUs.

TABLE 1: Summary of Identification Requirements for Remote Accounts

Identification of Individuals Remmore Presence		
Type of account	L3 L4 >3,000 UDIs	L3 L4 >5,000 UDIs
Credential	INE (passport, consulate certificate) CURP	INE (passport, consulate certificate) CURP
Personal Data	Full last names Date of birth Gender Nationalliy Address Mobile phone Picture of credential	Full last names Date of birth Gender Nationalliy Address Mobile phone Picture if INE credential Migratory document (through FEA)
Consent	Yes. By sending the form	Yes. By sending the form
Verification	Against existing data in the Institution files against INE	Against existing data in the Institution files against INE

In Regulation 39/2010, Banco de México requires that credit bureaus obtain verification through the CURP or RFC card to provide consent to access credit information. To provide effective consent to access credit reports from credit bureaus in Mexico, the consent could be provided verbally or by electronic means. In these cases, the consent provision requires the identification of the consumer through the CURP or RFC card.

The Fintech Law also required effective identification of consumers. Article 58.II of the Fintech Law of 2018 allows the SCHP to develop regulations regarding the documents and information that fintech institutions (*instituciones de tecnología financiera*) will collect to identify their consumers. Such information should be kept for 10 years and vested with adequate security measures to protect identification information. In addition, the SHCP would also share the list of blocked persons with the fintech institutions, when appropriate, and request that they cease providing services to such persons.

Data Protection and Privacy Aspects

As technological advances make it easier to collate data, government agencies and corporate firms seek to collect personal information about people either from the individuals themselves or by accessing data from other organizations. When dealing with government-issued ID numbers from credentials for individuals, conflicts around efficiency and privacy arise. While it is true that identity reduced to a number eases cross-referencing between databases, simplifies the verification processes, and increases government flexibility, it also increases the risks of function creep and the fraudulent use of an individual's identity. A structure for information management, access, and control that restores individual autonomy would allow individuals to dictate how their personal information will be used and disseminated—to the extent possible—aligning public policy with international privacy standards

ID systems should be supported by a legal framework for the protection of personal data. The assumption is that participants' private information will be available to multiple stakeholders and that any compromise of this data would reduce public faith in the system significantly. Data is protected when stored (and only for the duration disclosed) and while in transit and is accessible only to those with appropriate credentials. Only relevant basic biographic information should be collected, and it should not include data that could other be used to profile and possibly discriminate against a target population. Article 6 of the Mexican Constitution recognizes privacy as a human right, but article 16 of the constitution also recognizes the right to personal data protection.

Privacy aspects of the use of personal information for IMS are included under the Law on Transparency and Access to Public Information and the Law on Protection of Personal Data Law. The Law on Transparency and Access to Public Information in Mexico covers aspects related to information held by government agencies. This law calls for enabling access to information included in their databases as well as the protection of personal information. It covers information included in the RENAPO databases, including the CURP, and civil registries, the INE, the IMSS, and databases operate by Procesar on behalf of CONSAR, among others. Under article 68.II, the law establishes that the processing of data is to be limited to those data sets that are adequate, relevant, and non-excessive according to the permissible purposes for data collection. Authorities should also ensure data security and prevent data from any misuse, corruption, loss, unauthorized transfer, or access as established under article 68 VI. Moreover, personal information included in government-held databases should not be further distributed, disclosed, or commercially exploited unless the individual gives express consent.

Information on identification is considered confidential according to the transparency law. Article 116 of the law establishes that personal information that enables the identification of an individual is considered confidential and that such information may be accessed only by data subjects, their representatives, and the public agencies authorized to access such information and any other person prior to obtaining the data subjects' consent. (See article 119.) Article 120 includes exceptions to the prohibition of transferring data to third parties in the following circumstances: (i) when the information is already available in public registries, (ii) when the information is considered public information by law, (iii) when, to protect third parties' rights, such a transfer or access is necessary, and (iv) when such a transfer takes place between authorities subject to memorandums of understanding or international agreements in the context of fulfilling their duties.

Article 23 of the General Law on Transparency and Access to Public Information covers all personal data held by public authorities. This article also includes those persons who perform any activity in relation to using public funds or on behalf of any of the authorities included in article 23. In this context, private-sector actors that are developing digital identity services, or authentication-related services on behalf of authorities, are also subject to the provisions of the transparency law. Article 24 establishes that authorities should protect classified and confidential information.

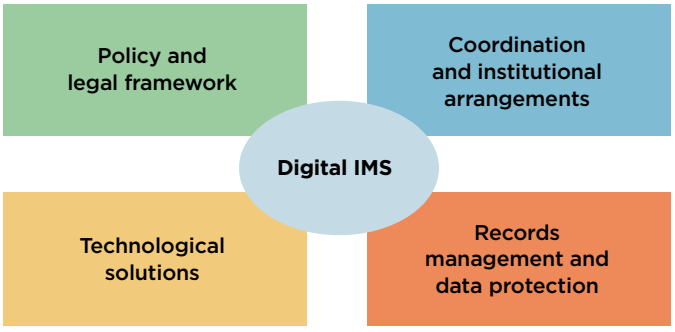
It should be noted that the INE requested a formal opinion from the National Institute for Access to Information (*Instituto Nacional de Transparencia*, INAI) about providing verification services in compliance with the data protection and the transparency laws. The INAI issued a formal opinion on May 2015[48] in which it supported the provision of such services and considered them of public interest due to the benefits that they could bring to data subjects, public entities, and credit institutions, as well as those that provide services or goods. However, the information included in the INE database is considered confidential and subject to the data subject's consent. In addition, in providing the verification services, the INE should also implement adequate security measures based on the data protection law and transparency law. Finally, the provision of such service is subject to contractual arrangements between the parties and will not involve the transfer of any personal information.

Mexico's data protection law covers information held by private data controllers. In this context, if a private-sector data controller collects information about individuals that includes personal data, the controller is subject to the provisions of the law that include principles related to data quality, purpose limitation and specification, proportionality, lawfulness of data collection, consent, and accountability. This law, therefore, would not apply to government-held databases but would apply to all financial institutions, banks, and other financial-sector participants, including the new institutions under the fintech law. The data protection law establishes that personal information is subject to consent unless it is included under the provisions outlined under article 22 of the data protection law (for example, compatible purposes between data collection and data access, when specifically established by the law, when subject to a court order, when such data is publicly available, or when personal data is anonymized). In addition, if personal information is held by private entities, the rights to access, rectify, cancel, and oppose (ARCO), security measures, and data portability also apply.

VIII. Potential Actions to Establish a Digital Identity IIIin Mexico

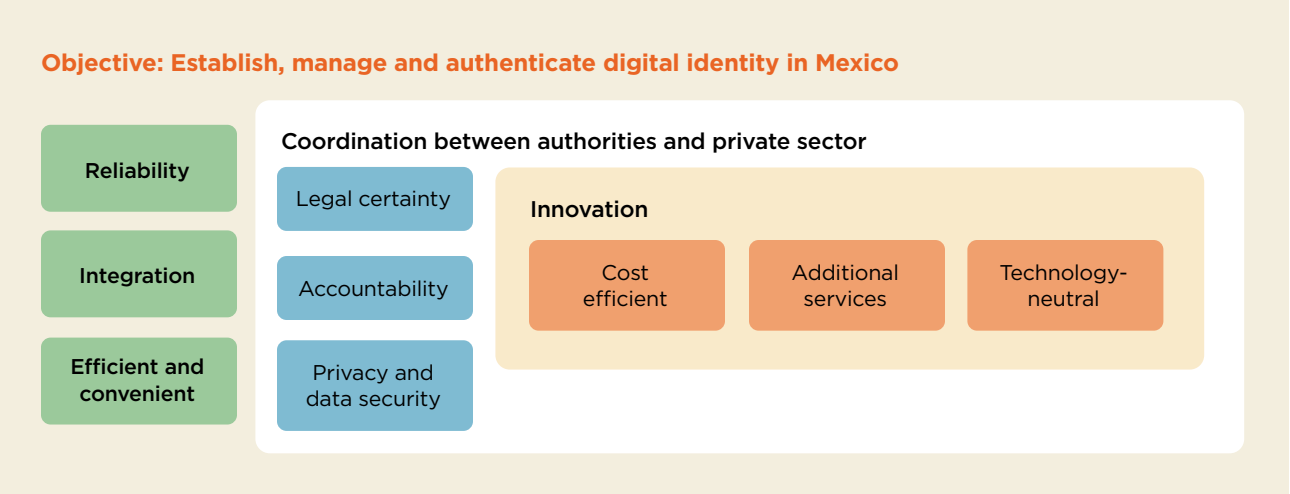
This section aims at providing some guidance to government and issuers, as well as users, to facilitate the adoption of a digital identity system for individuals and legal entities in Mexico. The section focuses on policy aspects and suggests some pilots to test potential solutions under controlled environments.

Authorities should develop a national strategy for digital IMS for financial inclusion.



The adoption of a digital IMS is a multilayered process that requires political consensus, a unified strategy, and agreement on common goals. In Mexico, the enhancement of identification systems should take into consideration the benefits of adopting new technologies that could bring convenience and efficiency while also reconciling the existing legacy of siloed databases that respond to different standards, legal mandates, and user needs. To achieve optimal results, coordination between authorities is key, but collaboration between the private and public sector could also contribute toward achieving the overall objectives, establishing clear roles for each participant through the creation of a formal coordination forum. This forum could be led by the National Council for Financial Inclusion (*Consejo Nacional de Inclusion Financiera*, CONAIF) as the key interested party in achieving identity solutions for the financial sector. The solutions could also be coordinated with other relevant agencies, given their broader implications, including the secretary of the interior (*secretaria de la gobernacion*) and the secretary of the economy (*secretaria de economia*).

FIGURE 27: National Strategy Key Features



Enhance the digitization of proofing registries (birth and death certificates).

Efforts led by RENAPO to introduce the CURP from birth and enhance civil registration at the state level should be strengthen and supported. Vital registration systems in Mexico are the responsibility of the municipalities, and each municipality has its own laws, rules, and regulations that govern the registration processes and functions. The availability of robust, electronic, and affordable birth- and death-registration systems helps reduce duplications in all existing foundational or functional identification systems, contributes to improved delivery of social and financial services, and mitigates fraud. To achieve an automated civil registration system, the following aspects are to be considered: (i) the harmonization of laws, procedures, and administrative responsibilities to the greatest extent possible, (ii) the development of electronic registration processes (recording, storing, and indexing), (iii) continuing to work toward interoperability of registries and universality of the CURP by creating the necessary architecture and interoperability platforms, and (iv) enhanced coordination through the National Council of Civil Registry Officials (*Consejo Nacional de Funcionarios del Registro Civil*, CONAFREC). Mobile technologies could be considered to support these efforts in close collaboration with CONAFREC and RENAPO.

Authorities should develop a strategy to clean up existing databases and identify a key database to serve as the primary source. This source should have biometrics (for example, INE).

Consider upgrading the CURP as the key unique identity number for the identification and authentication of individuals. One of the major problems of the CURP lies in its design, which makes it vulnerable to forgery and changes as vital changes of the person take place. The CURP is based on an alphanumeric code linked to a first and last name. If a person changes his or her name, the CURP changes. This is a major concern for the robustness of a foundational identification system.

a. Upgrading the CURP might require amending the existing legal framework.

b. RENAPO needs a road map for deduplication and the possibility of confronting other existing databases to identity unique individuals in the national population database.

c. The INE database could be an option to serve as the main database for individuals' official credential. Understanding that INE has already been recognized as an official credential,[49] it would be relevant to clarify the role that RENAPO has regarding the INE database. In this context, it is relevant to mention that also the additional verification services provided by INE to both the public and the private sector are also[50] considered of public interest and beneficial for data subjects, public entities, and private-sector service providers.

d. INE also need to consolidate the voter credential, since six generations are in circulation. It is also relevant to consider that the INE credential expires every 10 years and that there is always a need to keep the database updated. This requirement provides incentives to introduce additional features to improve the integrity of the database.

Developing standardized guidelines regarding data normalization could help improve data integrity and minimize data redundancy in existing databases. By restructuring a

relational database in accordance with a series of formal standardized methods for separating data and input, data information could be substantially improved. In adopting new technologies, standardized guidelines for collecting supporting relevant information would also be relevant. This practice would also enable APIs to access reliable information, when appropriate, based on implementation of article 76 of the fintech law.

To the extent possible, consider the adoption of a digital IMS that is technology neutral, allowing a minimum degree of interoperability and for authentication of individuals and legal entities operating in the digital environment.

Promote the use of alternative technology to authenticate individuals for digital transactions. While authorities work toward the enhancement of the national ID management system, the financial sector could start working on the adoption of a digital formats to authenticate individuals through an interoperable, technology-neutral, national database system that links relevant registration and identity systems and is appropriately and securely accessible by authorized parties, such as financial service providers, and authorities, subject to client consent. The legacy situation present in Mexico calls for coordinated measures that bring convenience to users by adopting new technologies and recognize the need to transform the existent legacy systems.

In this context, a potential solution could be to pilot the adoption of mobile ID solutions through agreements with mobile network operators to develop digital ID authentication mechanisms in selected geographical areas and controlled environments. Article 51 bis 8 of the CNBV Regulation on Identification Requirements for individuals and legal entities, issued in 2017, allows CNBV to approve additional identity mechanisms for remote accounts, provided that such technology proves to be reliable and could verify the official credentials (the CURP and INE card). Mobile phones represent a potential channel for promoting financial inclusion, given their extensive penetration in the population and the feasibility of interconnecting data securely and economically. According to GSMA, 53 million smartphone users were in Mexico in 2016, and mobile phone users make up 69 percent of the population. If this could be an option, the following factors would need to be considered:

a. Technological neutrality requires agreements between all mobile network operators.

b. Interoperability of the system is necessary.

c. Create a trusted framework that addresses transparency, control, accountability, and privacy.

Work toward the adoption of the LEI and Advanced Electronic Signature.[51]

Identifying legal entities participating in the financial sector, particularly those that are micro and small in size, is still a challenge, but this is also true for those that operate across borders, regardless of their size. There is a unified identifier for legal entities at neither the global level not even the domestic level. The most common number used is the tax number, although not all legal entities have a tax ID number for different reasons, or such a number is not always recorded in the databases in a manner than can be shared or accessed by different parties. While LEI has not been fully implemented in Mexico yet, and while the RFC does not capture all the informal legal entities, it would be useful to devote additional efforts to the adoption of LEI beyond entities that operate on cross-border basis. The adoption of an LEI requires (i) adequate certification of additional LOUs, (ii) further awareness of the role that an LEI can play in the financial sector, (iii) incentives for financial institutions to encourage the adoption of the LEI, (iv) incentives to small and medium-sized enterprises to request an LEI, and (v) a review of the current costs to issue and renew an LEI.

Work toward the broad adoption of the FEA by all potential users, including notaries, financial institutions, and consumers. The use of e-signature has simplified the processing and use of documents and contracts, as transaction fulfillment can occur fast, effectively, and securely. The banking industry in particular is using e-signatures to transform its agreement processes and provide an additional layer of reliability, security, and enhanced customer experience to every signed electronic form and document. However, many financial institutions still have not yet adopted the FEA for financial contracts.

To enable privacy, systems should build on the principle of privacy by design.

Enable privacy tools to comply with existing privacy and data-protection laws in Mexico. Both the right to identity and the right to privacy are fundamental human rights that relate to individual autonomy, but they protect different interests in different ways, and both should be balanced. The current legal framework under the Transparency and Access to Public Information Law and the Law on Protection of Personal Data establishes imposes obligations on all public agencies holding personal information in their databases and requires the receipt of explicit consent to transfer and access such data. In this context, at a minimum, the following data-protection principles should be considered.

a. ***Purpose limitation:*** the data controller (a government entity or private company) uses or collects data only for a specific purpose, predefined to the user. Data may not be used, shared, or stored for any reason beyond the specific purpose unless the individual´s consent is obtained.

b. ***Data security:*** Identification databases should be considered critical infrastructure and protected by cybersecurity measures against data loss, data corruption, data abuse, and unauthorized access from third parties. The data controller is responsible for embedding the appropriate technology and taking adequate measures against cyber incidents, including procedures and protocols to identify threats, prevent incidents, and respond to incidents, minimizing as much as possible the negative consequences to individuals.

c. ***Consent to data collection and processing:*** The data controller is responsible for embedding the appropriate technology and taking adequate measures to prevent unauthorized persons from accessing the data or to prevent data from being accessed for unauthorized purposes.

d. ***Allow individuals access their own data:*** Data controllers should have in place a transparency unit from which individuals could request access to their data. In case of linked databases, the National Transparency Platform (*Plataforma Nacional de Transparencia*) could play a relevant role and serve as the unit for individuals to exercise this right.

Consider legal aspects to enable the reform.

Clarify the role of the INE database as the primary source of data for identity purposes. Although the temporary provision is still active, there is a need to clarify the role of INE database going forward. Clarifying the role of RENAPO over INE, as well as defining it as the "primary source of official credential for individuals" would benefit the standardization process and minimize additional siloed efforts while adding value to existing infrastructure—in particular, the role that the INE plays as a functional credential that has de facto become a foundational one.

The legal framework should establish a minimum set of unique identity attributes. This set is essential to enable standardization across different databases, but it is also essential to establish digital identity. As an example, the European Union's eIDAS regulation 2015/1501 establishes the following for individuals: (i) current first name and last name(s), (ii) date of birth, and (iii) a unique identifier that is as persistent as possible. Then, additional attributes may include (i) first and last name(s) at birth, (ii) place of birth, (iii) current address, and (iv) gender. This should be followed by technical specifications and standards for data entry (for example, normalization) that should be standard across public and private entities developing/maintaining the digital IMS. In this sense, only those credentials that meet the minimum attributes and normalization standards should be considered official and the basis of the digital identity.

For online authentication services—based on existing data-protection and transparency laws—only those attributes that are adequate, relevant, and non-excessive should be required to grant the service. In this context, it might be relevant to define what is considered relevant and non-excessive in the context of digital identity. It might be necessary to issue guidelines regarding the authentication process, including the prohibition to transfer data from different databases without obtaining the data subject's consent. Also, implications of data anonymization and security measures around authentication protocols should be considered.

The legal framework should also ensure that validating digital identity constitutes completing identity verification under prevailing AML/CFT requirements.

As regards the use of digital signatures, there should be equivalence between physical and digital signatures. While the fintech law recognizes this concept, it might be necessary to review the current process, which requires certification to be obtained through the SAT to enable a more agile and cost-efficient use of digital signatures.

a. Third-party authentication services that are managed by the private sector are recognized as legally equivalent to a bank doing the authentication itself.

A close collaboration between authorities is key to enable the reform. This collaboration could be vested with memorandums of understanding to ensure that the accountability and liability of each agency is not undermined.

Collaborate with stakeholders outside government that can facilitate identification programs for excluded groups for financial inclusion and other purposes. Authorities should consider partnerships with the private sector to deploy technology that meets policy objectives (for example, underserved and unserved populations, including women, populations in rural areas, or mircro entrepreneurs). To this end, to understand the opportunities, risks, and consequences for consumers and the overall economy, close collaboration between parties is critical.

By giving an overarching agency jurisdiction over the national ID system, a country can ensure that the system is developed independent of individual department interests. It is also important to establish a government mandate encouraging all departments to contribute (if necessary) and to cooperate to ensure that the national ID program operates at intended. The SHCP, secretary of the interior, and secretary of the economy are key players to activate coordinated actions.

The role of the INAI in providing guidance for the effective implementation of a privacy-by-design approach in digital identity and authentication technology should be considered. Understanding the nature of the INAI, which serves as the enforcement agency for both the transparency law and the data protection law, dialogue between authorities and implementing partners in developing such technologies is encouraged.

APPENDIX A

Principles of Identification for Sustainable Development, 2017

Principles of Identification for Sustainable Development	
INCLUSION **Universal coverage and accessibility**	1. Ensuring universal coverage for individuals from birth to death, free from discrimination
	2. Removing barriers to access and usage and disparities in the availability of information and technology
DESIGN **Robust, secure, responsive, and sustainable**	3. Establishing a robust—unique, secure, and accurate—identity
	4. Creating a platform that is interoperable and responsive to the needs of various users
	5. Using open standards and ensuring vendor and technology neutrality
	6. Protecting user privacy and control through system design
	7. Planning for financial and operational sustainability without compromising accessibility.
GOVERNANCE **Building trust by protecting privacy and user rights**	8. Safeguarding data privacy, security, and user rights through a comprehensive legal and regulatory framework
	9. Establishing clear institutional mandates and accountability
	10. Enforcing legal and trust frameworks through independent oversight and the adjudication of grievances

APPENDIX B

G20 High-Level Principles on Digital Financial Inclusion, 2016

High-Level Principles on Digital Financial Inclusion	
PRINCIPLE 7 **Facilitate customer identification for digital financial services**	Ensure birth registration and other foundational identity systems are universal and affordable. Amend laws and regulations that inhibit or deny digital identification registration to underserved groups such as married women.
	Ensure that government identity databases—birth registration and tax IDs, for example—are made appropriately and securely available to other parts of government, subject to client consent when required by data-protection laws
	Establish an interoperable, technology-neutral national database system, where appropriate, that links relevant civil registration and identity systems and is appropriately and securely accessible to authorized parties, such as financial service providers, subject to client consent where required by data-protection laws
	Establish and promote, as necessary, new and innovative forms of identity registration and verification such as digital biometric identification products and online identity verification services, particularly for those currently lacking any form of identification. Establish acceptable open standards to manage identity, transaction and account risks
	Implement risk-based customer identification and verification requirements to facilitate uptake of low-risk digital financial services for financial inclusion purposes, for example through tiered frameworks for customer due diligence. Such requirements should authorize identification from one or multiple state-validated sources and clearly specify the data sources that can be used for identity verification while meeting the requirements of the Financial Action Task Force for *"reliable, independent source documents, data or information*
	Establish a legal framework that protects the privacy and security of identity data and requires informed consent to use and disclose such data. This framework should also require robust recourse frameworks to allow individuals to seek redress when consent, rights or privacy have been violated.
	Collaborate with stakeholders outside government that can facilitate identification programs for excluded groups for financial inclusion and other purposes. One example would be humanitarian relief organizations and other relevant nongovernmental organizations.
	Establish clear accountability and transparency around the roles and responsibility of the public and private agencies in charge of identity management
	Encourage development of safe and secure digital signature systems that can help facilitate authentication and validation, especially for underserved consumers

APPENDIX C

Glossary

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

Authentication (b): (a) The process of establishing confidence in the truth of a claim, which could be any declarative statement; (b) the process by which a user conveys data into a system in order to be recognized and to be able to interact with the system; and, (c) in biometrics, sometimes used as a generic synonym for certification.[52]

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

Biometrics: Physical or behavioral attributes of an individual, including fingerprints, irises, facial images, gait, signatures, keystrokes, and so forth.

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

Credential (b): A document or token that establishes the identity and proves the condition of a person and his or her competence or authority to perform a certain activity or function

Digital identity (a): A collection of electronically captured and stored identity attributes that uniquely describe a person within a given context and are used for electronic transactions. It specifically provides remote assurance that the person is who he or she purports to be. A **digital identification system** refers to the systems and processes that manage the life cycle of individual digital identities

Digital identity (b): The unique representation of a subject engaged in an online transaction. A digital identity is always unique in the context of a digital service but does not necessarily need to uniquely identify the subject in all contexts. In other words, accessing a digital service may not mean that the subject's real-life identity is known.[53]

Identification: The determination of identity and recognition of who a person is; the action or process of determining what a thing is; or the recognition of what it is.

Identification 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 unique set of features and characteristics that individualize a person, including the name and other biographical data of the individual.[54]

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

Legal entity identifier (LEI): A 20-character alphanumeric code to identify legally distinct entities that engage in financial transactions. The organizational structure of the LEI consists of a federated group of registrars, local operating units (LOUs); a central operational body, the Global LEI Foundation; and a regulatory body charged with oversight of the LEIs, the Regulatory Oversight Committee. The Global LEI Foundation is a Swiss foundation inaugurated in June 2014 and founded by the Financial Stability Board. It is overseen by 70 global regulators in the Regulatory Oversight Committee.

Unique identity number: An attribute in the form of a unique number used to identify individuals upon their inscription in the civil register or civil identification system.

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

Verification (b): (a) A method of identity verification based on knowledge of private information associated with the claimed identity. This is often referred to as knowledge-based authentication (KBA) or knowledge-based proofing (KBP).[54] (b) Confirmation of a claim through the provision of objective evidence when specified requirements have been fulfilled.[55]

References

AFI (Alliance for Financial Inclusion). 2017. *National Retail Payment Systems to Support Financial Inclusion, Guideline Note No. 29.*

BBVA Research. 2013. *La banca móvil en México como mecanismo de inclusión financiera: desarrollos recientes y aproximación al mercado potencial*.

CPMI (Committee on Payments and Market Infrastructures) and World Bank Group. 2016. *Payment Aspects of Financial Inclusion* (Bank for International Settlements and World Bank Group, April 2016), http://www.bis.org/cpmi/publ/d144.pdf.

Dahan, Mariana, and Alan Gelb. 2015. *The Role of Identification in the Post-2015 Development Agenda,* World Bank Working Paper 2015.

FATF (Financial Action Task Force). 2003 and 2012. FATF 40 Recommendations.

GLEIF (Global Legal Entity Identifier Foundation). 2016. "Accreditation Process" (web page). https://www.gleif.org/en/about-lei/the-lifecycle-of-a-lei-issuer/gleif-accreditation-of-lei-issuers/accreditation-process.

GPFI (Global Partnership for Financial Inclusion). 2016. *G20 High-Level Principles for Digital Financial Inclusion.*

Grassi, P. A., M. E. Garcia, and J. L. Fenton. 2017. *Digital Identity Guidelines,* NIST Special Publication 800-63-3 (National Institute of Standards and Technology).

GSMA. 2017. *Innovations in Mobile Birth Registration: Insights from Tigo Tanzania and Telenor Pakistan.*

GSMA. n.d. Mobile Connect, web page, https://www.gsma.com/identity/mobile-connect.

World Bank. 2015. *Identity Management Systems Analysis—Guidelines and Questionnaire.* Available at https://id4d.worldbank.org/guide/id4d-tools-and-research-topic.

World Bank. 2016. *Identification for Development: Strategic Roadmap.*

World Bank and Center for Global Development. 2017. *Principles on Identification for Sustainable Development: Toward the Digital Age.*

World Bank Group and Digital Impact Alliance. 2018. *Technology Landscape for Digital Identification.*

Endnotes

1. According to the Commission for the Protection and Defense of Users of Financial Services (*Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros*, CONDUSEF).
2. This situation is the result of a combination of duplicates in the system and the lack of an adequate link between death certificates and the CURP.
3. Please see http://documents.worldbank.org/curated/en/213581486378184357/pdf/112614-REVISED-English-ID4D-IdentificationPrinciples.pdf
4. http://globalfindex.worldbank.org/
5. For further reading, please see the G20 High-Level Principles for Digital Financial Inclusion (Global Partnership for Financial Inclusion, 2016) https://www.gpfi.org/sites/default/files/G20%20High%20Level%20Principles%20for%20Digital%20Financial%20Inclusion.pdf. Principle 7: "*Facilitate access to digital financial services by developing, or encouraging the development of, customer identity systems, products and services that are accessible, affordable, and verifiable and accommodate multiple needs and risk levels for a risk-based approach to customer due diligence*."
6. Payment service providers require users to prove their identity through digital channels, or they act as platforms on top of established financial institutions and rely on KYC processes.
7. To evaluate customer risk and issue loans, a consumer's identification information must be validated. Innovators gather information from users through pseudo- digital channels, such as photographing existing ID cards or gathering trusted information from an existing source (for example, credit bureaus), therefore decentralizing a central piece of the product offering.
8. FATF is an intergovernmental body that sets standards and develops and promotes policies to counter money laundering and the financing of terrorism. The task force is composed of 34 member countries and two international organizations. A list of members and observers can be found on the FATF website, www.fatf-gafi.org.
9. For the PAFI report, please see: http://documents.worldbank.org/curated/en/806481470154477031/pdf/107382-WP-REPLLACEMENT-PUBLIC-PAFI-Report-final-in-A4.pdf.
10. Please see the definition of the National Institute of Standards and Technology: "Digital identity is the unique representation of a subject engaged in an online transaction" (page 2), https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-3.pdf.
11. Joseph Atick, Mariana Dahan, Alan Gelb, and Mia Harbitz, "Digital Identity," in *Digital Dividends*, World Development Report 2016 (World Bank, 2016).
12. For further reading, please see the G20 High-Level Principles on Digital financial Inclusion, https://www.gpfi.org/publications/g20-high-level-principles-digital-financial-inclusion.
13. According to 2016 Global Findex database, approximately 375 million unbanked adults in developing countries (18 percent) are prevented from obtaining one because they lack the necessary ID documentation.
14. Please see page 30 of the PAFI report.
15. Please see page 26 of the report *General Principles for Credit Reporting* (World Bank, 2011).
16. Definition included in the 2016 discussion report on digital identity published by the World Bank, GSMA, and the Secure Identity Alliance.
17. In the context of this document, digital identity refers to the set of electronically captured and stored attributes and credentials that can uniquely identify a person (World Bank, GSMA, 2014).
18. Swedbank is another case in point. The bank has introduced online services authenticated via Smart ID for their Latvian and Lithuanian branches. Customers can download and register on the Smart ID app and perform banking transactions by authenticating themselves through their Smart ID PINs, https://www.swedbank.lv/private/campaign/smart-id.
19. The European Union's eIDAS recognizes this tool as a valid authentication tool.

20. Juniper Research, "Voice and Facial Recognition to Be Used in Over 600 Million Mobile Devices by 2021," press release November 29, 2016.
21. These accounts do not require a minimum account balance and allow for daily transactions up to a limit of Rs 10,000.
22. MyCUID operates through a person-to-person network of "distributed, private agents working in parallel with the distributed ledger."
23. Prospera, previously known as "*oportunidades*," is a conditional cash-transfer program established in 1997 consisting of giving money to a mother to encourage her to send her children to school and to the health center. Oportunidades was the first national conditional cash-transfer program targeting poor and extremely poor households that integrated three basic social rights: health, education, and nutrition.
24. Kenichi Nishikawa and Robert Palacios, "Identity System Analysis, Country Report for Mexico" (unpublished manuscript, December 2015).
25. https://www.financialresearch.gov/data/legal-entity-identifier/
26. Please see article 30 of the *Ley de Cámaras Empresariales y sus Confederaciones*, January 20, 2005.
27. http://www.sat.gob.mx/informacion_fiscal/tramites/inscripcion_rfc/Documents/Guía_preinscripción%20_PM_18072017.pdf
28. https://www.diputados.gob.mx/LeyesBiblio/ref/lfea.htm
29. The fees include an initial fee of $150 (Mex$3,000) and a renewal fee of $100 (Mex$2,000).
30. http://www.banxico.org.mx/sistema-financiero/informacion-general/codigo-lei-referencia-banco-m001.html
31. Circular 14/2015 of Banco de México.
32. Please see "Encuesta Nacional de Inclusión Financiera," 2015, http://www.cnbv.gob.mx/Inclusi%c3%b3n/Documents/Encuesta%20Nacional%20de%20IF/Cuadr%c3%adptico%202016%20%28impresi%c3%b3n%20carta%29.pdf
33. The FIU provides recommendations to different units within the SHCP, including units of Banca, Valores y Ahorro (UBVA), de Banca de Desarrollo (UBD), and Seguros, Pensiones y Seguridad Social (USPSS).
34. http://www.hacienda.gob.mx/LASHCP/MarcoJuridico/InteligenciaFinanciera/Paginas/leyes_reglamento.aspx
35. http://www.cnbv.gob.mx/PrevencionDeLavadoDeDinero/Paginas/default.aspx
36. http://www.cnsf.gob.mx/Paginas/Home.aspx
37. http://www.consar.gob.mx/
38. http://www.banxico.org.mx/sistema-financiero/informacion-general/codigo-lei-referencia-banco-m001.html
39. The cross-border transaction database will capture information about the following data items in addition to the credential related information: (i) the type of originator, (ii) the number of banks from which the client ordered wire transfers, (iii) a list of countries to which the client sends wires, (iv) the total amount of wire-transferred funds sent in a given period, (v) the number of days in the period in which the client instructed wire transfers, (vi) the number of calendar days between transfers, (vii) the number of beneficiary accounts, (viii) the percentage of the total number of transfers to the same beneficiary, (ix) the percentage of the total amount to a beneficiary versus the total amount to all beneficiaries, (x) the average amount sent by the client, (xi) the mode of amount sent, and (xii) the distribution of amounts sent by mode.
40. Please see article 17 of Circular 3/2012.
41. The National Commission on Savings and Retirement (CONSAR) regulates the Savings and Retirement System.
42. The Institute for Social Security and Services for State Workers (*Instituto de Seguridad y Servicios Sociales de los Trabajadores del Estado*, ISSSTE) is the federal government organization that administers health care and social security systems to federal workers in Mexico. Unlike the Mexican Social Security Institute (or IMSS), which covers workers in the private sector, the ISSSTE is charged with providing benefits for federal government workers only.
43. The General Population Law, published on January 7, 1974, and last revised on May 19, 2014, establishes the Ministry of the Interior as the government authority responsible for managing the national ID service. Within the Ministry of the Interior, this responsibility falls under the office of the national population registry RENAPO. RENAPO was created on August 20, 1980, through a presidential decree, and given the specific mandate to implement the National Registry System as well as develop a personal national ID number.
44. Please note that this protocol was amended in 2009 and 2014, but the latter has not been published yet.
45. This information includes all data related to the registration of new legal entities, minutes resulting from board meetings, and changes in the legal entity, legal representative, and shareholders.
46. The following laws include requirements on AML/CFT that imply the need to identify unique consumers and counterparties to financial transactions: (i) Ley de Instituciones de Crédito; Ley del Mercado de Valores; (ii) Ley de Ahorro y Crédito Popular; (iii) Ley de los Sistemas de Ahorro para el Retiro; (iv) Ley General de Instituciones y Sociedades Mutualistas de Seguros; (v) Ley de Sociedades de Inversión; (vi) Ley de Organizaciones y Actividades Auxiliares del Crédito, and (vii) y Ley Federal de Instituciones de Fianzas.
47. Banco de México Circular 2019/05 as amended by Circular 14/2011.
48. IFAI/CPDP/0022/15.
49. Article 4 of the Decree on General Population Law of 1992 establishes that information provided by the INE database and its credential will be used for RENAPO until a *Cedula Unica de Identidad Ciudadana* (CUI) is issued.
50. In 2016, an agreement by the INE General Council was approved allowing the implementation of the verification services against the INE credential based on the protection of personal data included in the voter roll. Several memorandums of understanding were signed in 2013 between INE and Banco Nacional de México (BANAMEX) to provide verification services.
51. An e-signature is generally any electronic process that indicates acceptance of an agreement or form. A range of methods can be used to authenticate the identity of participants, including email addresses, enterprise IDs, phone authentication, knowledge-based authentication, and passwords. A digital signature is a specific type of e-signature that requires the signer to authenticate their identity using a certificate-based digital ID.
52. Mia Elisabeth Harbitz, Kristo Kentala, and Iván Arcos Axt, *Dictionary for Civil Registration and Identification* (Inter-American Development Bank, 2013), https://publications.iadb.org/handle/11319/3679.
53. P. A. Grassi, M. E. Garcia, and J. L. Fenton, *Digital Identity Guidelines*, NIST Special Publication 800-63-3, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-3.pdf.
54. Mia Elisabeth Harbitz, Kristo Kentala, and Iván Arcos Axt, *Dictionary for Civil Registration and Identification* (Inter-American Development Bank, 2013), https://publications.iadb.org/handle/11319/3679.
55. P. A. Grassi, M. E. Garcia, and J. L. Fenton, *Digital Identity Guidelines*, NIST Special Publication 800-63-3, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-3.pdf.
56. ISO 9000 (2015), https://www.iso.org/obp/ui/#iso:std:iso:9000:ed-4:v1:en.

THE WORLD BANK
IBRD • IDA | WORLD BANK GROUP