ID4D
IDENTIFICATION FOR DEVELOPMENT

PRACTITIONER'S NOTE

IDENTITY AUTHENTICATION AND VERIFICATION FEES: OVERVIEW OF CURRENT PRACTICES

April 2019

Summary

This note was prepared by the World Bank's ID4D Initiative to summarize country experiences and practices related to fees charged by ID authorities to public and private sector third parties for identity authentication and verification services.[1] It contains information from Argentina, Chile, Colombia, Ecuador, India, Kenya, Malaysia, Pakistan, Panama, Peru, Tanzania and Thailand.[2]

This note is not intended to provide recommendations or endorse a particular model or approach; it merely aims to highlight existing practices and key considerations related to the provision and pricing of identity verification services. Each country or identity provider considering the introduction of fees for identity verification is encouraged to carry out its own analysis, and decide whether to charge fees, what services to charge fees for, and which types of entities or individuals might be exempted. The need or opportunity to generate revenue should be balanced against the importance of not creating barriers to obtaining identity documents and accessing services that require identity verification or authentication. The Principles on Identification for Development can provide further guidance on how to design and implement an ID system in a manner that helps maximize its benefits for development while mitigating the risks.

This note provides insights into the institutional arrangements and verification fee structures for the private and public sectors in twelve countries. The private sector usually includes banks and other financial institutions, telecom companies and mobile network operators; while public sector service users often include Ministries of Health, Ministries of Education, Ministries of Internal Affairs and transportation agencies that need to verify personal information in order to deliver services effectively.

[1] Although authentication and verification are related and often used interchangeably, they can be distinguished by whether the process involves determining the veracity of particular attributes or credentials (verification) or ensuring that a person is who they claim to be (authentication). To facilitate the reader's understanding, this note will used both terms interchangeably.

[2] This note is primarily based on information gathered from current and past staff members and websites of RENAPER (Argentina), *Servicio de Registro Civil e Identificacion* (Chile), *Registraduria del* Estado Civil (Colombia), Dirección General de Registro Civil, Identificación y Cedulación (DIGERCIC), UIDAI (India), JPN (Malaysia), *Tribunal Electoral* (Panama), NADRA (Pakistan), and RENIEC (Peru), and BORA (Thailand).

WORLD BANK GROUP
ID4D.WORLDBANK.ORG

Contents

About ID4D

The World Bank Group's Identification for Development (ID4D) Initiative uses global knowledge and expertise across sectors to help countries realize the transformational potential of digital identification systems to achieve the Sustainable Development Goals. It operates across the World Bank Group with global practices and units working on digital development, social protection, health, financial inclusion, governance, gender, legal, and among others.

The mission of ID4D is to enable all people to access services and exercise their rights by increasing the number of people who have an official form of identification. ID4D makes this happen through its three pillars of work: thought leadership and analytics to generate evidence and fill knowledge gaps; global platforms and convening to amplify good practices, collaborate, and raise awareness; and country and regional engagement to provide financial and technical assistance for the implementation of robust, inclusive, and responsible digital identification systems that are integrated with civil registration.

The work of ID4D is made possible with support from the World Bank Group, Bill & Melinda Gates Foundation, Omidyar Network, and the Australian Government.

To learn more about ID4D, visit id4d.worldbank.org.

Acknowledgments

This note was prepared by Julia Clark, Jonathan Marskell, and Julian Najles as part of the Identification for Development (ID4D) Initiative, the World Bank Group's cross-sectoral effort to support progress toward identification systems using 21st century solutions. It was made possible through the generous support of the partners of the ID4D Multi-Donor Trust Fund.

This note benefited greatly from the inputs and reviews of World Bank Group staff including Robert Palacios, Luda Bujoreanu, and Anna Metz, and was prepared under the supervision of Vyjayanti Desai.

In addition, this report would not have been possible without the insights and feedback provided by Flavio Brocca and Estefania Casadei (RENAPER, Argentina), Gloria Larenas and Daniela Rodriguez (DIGERCIC, Ecuador), Sharon Sinclair de Dumanoir and Boris Corcho (Tribunal Electoral, Panama), Arianna Espinosa (RNEC, Colombia), Claudia Araya (*Registro Civil, Chile*), Patricia Mongkhonvanit (Revenue Department, Thailand), Felix Ortega (RENIEC, Peru), and Rehman Qamar (NADRA, Pakistan).

Introduction

A growing number of identity providers (e.g., national ID agencies) around the world now offer reliable remote identity authentication and verification services to a variety of third parties, including public and private service providers such as government agencies, banks, and mobile network operators.

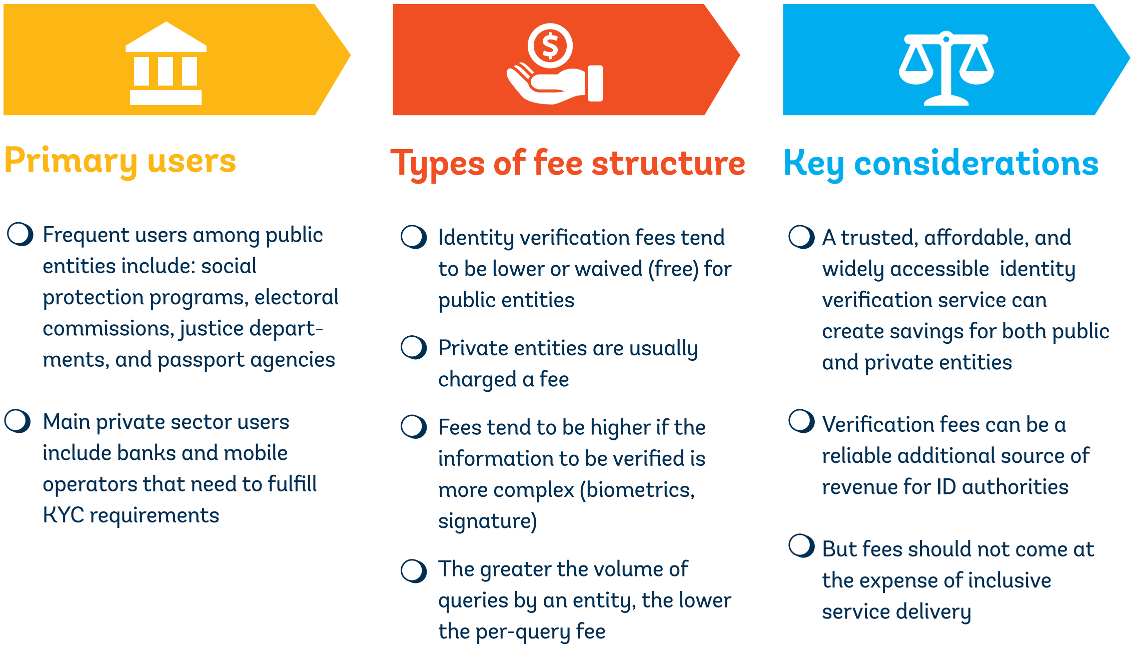
In several countries, third parties can query ID provider databases in order to verify an individual's identity, as needed for service delivery or administrative purposes. In some cases, identity verification might be a legal requirement. Banks and mobile network operators, for instance, are often obligated to verify their customers' identity in the context of "know-your-customer" (KYC) and/or anti-money laundering (AML) regulations when opening a new account or providing certain services. Making identity verification services available to certain third parties—particularly in the case of on-demand, online services—can therefore create efficiencies for both the public and private sector and improve the reach, efficiency, and transparency of myriad services and transactions.[3]

In addition, charging fees for identity verification services can be an important revenue source for identity providers. An additional revenue flow can help identity providers invest in modernizing their systems and reduce dependence on government budgets. At the same time, there is also a risk that such fees can place a burden on third parties by driving up their operating costs and may create financial barriers to people when accessing services if these extra costs are passed onto end-users.

Verification fees should therefore be set using great care, balancing the potential benefits from earning greater revenues against the potential exclusion risks. Reliable identity verification services can create savings for third parties and the people they serve as long as the fees charged for verification are lower than what the service users' own verification costs would have been in its absence. Strong regulatory frameworks can help mitigate exclusions risks and offering varying fees for different users or types of services can also help ensure that critical services remain accessible for all.

[3] *See*, for example, the World Bank reports on public- and private-sector savings from ID systems, available at http://id4d.worldbank.org/research.

Figure 1. Main findings on verification services



Primary users

- Frequent users among public entities include: social protection programs, electoral commissions, justice departments, and passport agencies
- Main private sector users include banks and mobile operators that need to fulfill KYC requirements

Types of fee structure

- Identity verification fees tend to be lower or waived (free) for public entities
- Private entities are usually charged a fee
- Fees tend to be higher if the information to be verified is more complex (biometrics, signature)
- The greater the volume of queries by an entity, the lower the per-query fee

Key considerations

- A trusted, affordable, and widely accessible identity verification service can create savings for both public and private entities
- Verification fees can be a reliable additional source of revenue for ID authorities
- But fees should not come at the expense of inclusive service delivery

Country Experiences

The countries examined in this note differ in terms of which third parties have access to verification services and the fee structures used, as shown in Table 1 below. For eight of the twelve countries included in Table 1, the note also provides more detailed information. In general, the primary users of verification services are government programs and agencies—e.g., social protection programs, electoral commissions, justice departments, passport agencies, etc.—as well as banks and mobile operators that need to fulfill KYC requirements. In some cases, these third parties have dedicated secure connections to the central server which hosts the ID data and make queries in real time, on an ongoing basis; in others, verification is done via web-based portals or APIs. Furthermore, some identity providers conduct large batches of verifications for specific purposes within a set time frame (e.g., periodic deduplication of a voter list before elections). Fees typically vary based on whether the third party is a public or private entity, the type of data or query, and/or the volume of transactions.

Across the twelve countries analyzed, third parties rely on both biometric and biographic information to verify end-user information. Biometric data usually includes fingerprints and photo which need to comply with certain standards when captured in order to be “understood” by other systems. Biographic information usually includes names, sex, and address. Third parties can verify an identity using one type of data or a combination of both.

The type of data that need to be provided by (or about) an individual for verification (e.g. name, ID number, photo, etc.) and the response returned by the ID authority (e.g. yes/no or more detailed information) differs based on the type of transaction or service for which the identity verification is performed and based on the model that each country has chosen. For example, in Argentina, to verify an ID number, third parties need to introduce the ID number and the person’s sex and the system will return a yes or no answer. In Ecuador, third parties request to end users the ID number and a fingerprint code stated on the back of the ID card and the system returns a certificate with biographic and biometric data.

Table 1. Verification Services for Third Parties in Select Countries

Country	Population -millions- (World Bank, 2017)	GDP/ Capita - USD. (World Bank, 2017)	Fees[4]	Data Protection and Privacy law (UNCTAD, 2019)
Argentina	43.8	14,398	Public sector: **free** Private sector: Per query fee - USD 0.125 (basic) - USD 0.375 (fingerprint) - USD 2.5 (biometrics+)	Yes
Chile	18.2	15,346	Public sector: **free** Private sector: Per query fee[5] - USD 0.040 (basic) - USD 0.054 (photo) - USD 0.040 (signature) - USD 0.135 (biometric)	Yes
Colombia	49.9	6,408	Public sector: **free** Private sector: Price depends on volume of queries, e.g.,: - USD 0.095/per query for up to 100k queries (biometric) - USD 0.014/per query for up to 12m queries	No
India	1,339.2	1,942	Public sector: **free** Private sector: - USD 0.007 for Aadhaar authentication with a yes/no response - USD 0.3 for e-KYC transactions	Yes
Ecuador	16.2	6,273	Public sector: **free** Private sector: Per query fee - Web page based: Demographic USD 0.15 Biometric USD 0.30 - Web service based: Demographic USD 0.08 Biometric USD 0.30 - CD or DVD based Demographic USD 0.12	No

[4] Fees were converted from local currencies to USD using the applicable currency exchange rate on December 29, 2019 and are be subject to change.

[5] These per query rates assume a monthly volume of verification requests between 50,001 and 600,000 UBI. Please see the section on Chile for more details.

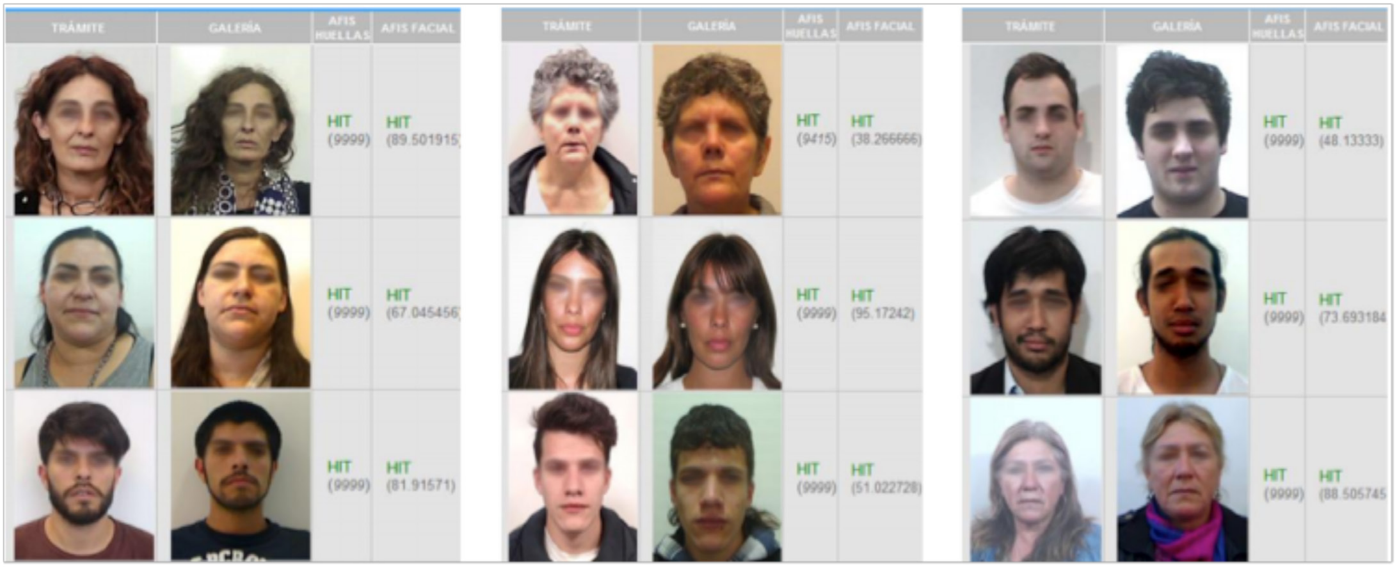
Country	Population -millions- (World Bank, 2017)	GDP/ Capita - USD. (World Bank, 2017)	Fees[4]	Data Protection and Privacy law (UNCTAD, 2019)
Kenya	48.5	1,595	All: **free** verification of a demographic record and national ID card number as it is considered a citizen service[6]	No
Malaysia	31.2	9,952	All: - USD 0.13 to verify a demographic record - USD 0.25 to verify a demographic and biometric record	Yes
Pakistan	193.2	1,548	Public sector: USD 0.09 per query Private sector: USD 0.29 per query	No
Panama	4.1	15,196	Public sector: **free** Private sector: - USD 1 for 1-10,000 queries - USD 0.75 for 10,001-30,000 - USD 0.50 for 30,001-60,000 - USD 0.10 for 60,001-more	No
Peru	31.8	6,572	Public sector: **free** Private sector: There are various ways to verify an identity. Wired connection, used by banks, has the following fees: - USD 0.026/per query for up to 200k queries - USD 0.06/per query for 800k or more	Yes
Tanzania	55.6	936	Citizens: USD 0.22 for any query or authentication by any government or private sector user Legal residents and refugees: USD 1 for any query or authentication	No
Thailand	68.9	6,595	Public Sector: **free** verification of a demographic record and the national ID card (it is considered a citizen service)	No

[6] Kenya's IPRS system also offers a free online service to banks, telecoms, and other entities to verify thlient ID cards are genuine, conducting some 1.5 million ID card queries per day. However, it currently does not have the capability to verify individuals using online biometric authentication.

Argentina

Argentina's *National Registry of Persons* (RENAPER by its initials in Spanish) provides a variety of online identity verification services for different types of public institutions and private entities. Verification services are free of charge for all public institutions including the Ministry of Health, Ministry of Security, provincial governments and agencies, National Social Security Administration (ANSES by its initials in Spanish) and the National Directorate of Migration. For private entities, the amount charged depends on the types of services provided. RENAPER provides four types of services based on the type of information to be verified: verification using names AR$ 5 each (USD 0.125), verification using finger prints AR$ 15 each (USD 0.375), verification using a personal photo AR$ 5 each (USD 0.125) and verification using a combination of photo and the bar codes on the front and the back of the ID card AR$ 100 each (USD 2.5). In all cases, service providers need to submit information depending on the type of inquiry. For example, to verify a name, requesting entities are required to submit the ID number and the sex of the person in question. For photo verification, a digital photo (ICAO standard) is required, and for fingerprint verification, third parties need to send an image in WSQ format. RENAPER will return a HIT or NO HIT answer depending on the accuracy of the match as shown in photo number 1. (Argentine Official Bulletin, 2018).

Photo 1. Examples of HIT or No HIT on Verification Services



TRÁMITE	GALERÍA	AFIS HUELLAS	AFIS FACIAL
		HIT (9999)	HIT (89.501915
		HIT (9999)	HIT (67.045456
		HIT (9999)	HIT (81.91571)

TRÁMITE	GALERÍA	AFIS HUELLAS	AFIS FACIAL
		HIT (9415)	HIT (38.266666)
		HIT (9999)	HIT (95.17242)
		HIT (9999)	HIT (51.022728)

TRÁMITE	GALERÍA	AFIS HUELLAS	AFIS FACIAL
		HIT (9999)	HIT (48.13333)
		HIT (9999)	HIT (73.693184
		HIT (9999)	HIT (88.505745

In order to be able to use identity verification services, private companies must sign a Memorandum of Understanding with RENAPER requesting a specific type of service and committing to comply with the country's Data Protection Law. As of the end of 2018, RENAPER provides verification services to 93 private companies including banks, financial entities, private medical institutions, notaries (RENAPER, 2018).

Chile

The *Civil Registry and Identification Service* (Civil Registry) of Chile has been providing biometric identity verification services for public institutions and private entities since 2005. For public institutions, the Civil Registry does not charge any fees. In 2018, more than 16 million queries were verified at the request of public institutions, including the National Service of Employment, the National Police (*Carabineros*), the Ministry of Health and the Office of the Public Prosecutor (Civil Registry, 2018).

For private entities, the Civil Registry has established a fee scale based on the type of data queried, where each query costs a certain number of pre-purchased "credits" called *basic units of infrastructure* (BUI). For example, a verification query with photo costs 2 BUI; a verification with signature costs 1.5 BUI; a verification of identity with one fingerprint costs 1.5 BUI; a verification with ten fingerprints costs 20 BUI; a verification based on information stated on the ID card consumes 1.5 BUI; a verification via AFIS 1:1 using WSQ image or NEC consumes 5 BUI.

Third parties verifying information need to enter into the system the unique ID number of the end user (called Single National Roll number – RUN by its initials in Spanish), RUN's check digit, and the image of the fingerprint in order to obtain a response. The system will return a HIT or NO HIT depending on whether the probability of a match is above or below a certain threshold.

The Civil Registry uses a nomenclature based on BUIs (which refers to the incremental capacity of infrastructure required to respond to the queries) and the *unidad de fomento*, which is a unit of account equivalent to USD 39.54. The *unidad de fomento* is constantly adjusted for inflation so that its value remains almost constant over time. Under this scale, the Chilean authority charges private companies a monthly fix amount of 70 *unidades de fomento* equal to ~USD 2,771 for up to a monthly request of 50,000 basic units of infrastructure. If the private company needs more than 50,000 BUI, the cost of each BUI decreases: to a per unit cost of USD 0.027 for 50,001-600,000 BUI and a per unit cost of USD 0.008 for more than 600,000 BUI (Library of Congress (Chile), 2006).

To be able to verify personal information, public institutions and private companies must sign a MoU with the Civil Registry that states how the information would be verified, the conditions under which the information must be submitted, as well as the terms of compliance with the Data Protection Law.

Colombia

Since 2012 the *Registraduria Nacional del Estado Civil* (subsequently referred to as *Registraduria*) allows public institutions to verify information against its database for no fee, facilitating the efficient delivery of services in areas such as education (Ministry of Education, universities and high schools), justice and security (Ministry of Defense, Interior, Justice and the judiciary branch), social protection (Ministry of Social Protection, family welfare funds, etc.), transportation (Ministry of Transportation and Secretariat of Transit), and notaries.

For private entities, the *Registraduria* has various fixed fees depending on the number of verification queries. For example, for 1 to 100,000 queries, it charges COL $15,203,385 (~USD 4,751); for 100,001 to 200,000 it charges COL $ 30,406,770,80 (~USD 9,502); for 200,001 to 300,000 it charges COL $45,610,156 (~USD 14,253) and so on, until the range between 11,000,001 and 12,000,000 queries, where it charges COL $ 519,742,188,00 (~USD 162,419).[7]

Thus, depending on the volume of the queries, the per-query fee can range from about USD 0.1 to USD 0.01.

[7] *Registraduría Nacional del Estado Civil.* Resolution 515 from 2018 Available at: https://www.cancilleria.gov.co/sites/default/files/FOTOS2018/resolucion_515_tarifas_vigencia_2018.pdf

Third parties that opt to verify information against the national registry must sign a MoU with the *Registraduria* and perform a technical test that costs COL $ 10,276,250 (~USD 3,190), in order to ensure that the third party has the capacity and resources to responsibly manage information verification requests. Currently, the *Registraduria* provides verification services to 69 private companies (Registraduria, 2018).

Ecuador

The General Directorate for Civil Registration, Identification and Certification (DIGERCIC by its initials in Spanish) began providing identity verification services in 2013. Five years on, DIGERCIC provides verification services to 28 public institutions including the Ministry of Health, Ministry of Education, Secretariat of Migration and the National Electoral Council; and to 1,224 private entities. For public institutions, verification services are free. The private sector is charged a fee, which depends on whether the query includes demographic or biometric information. In 2018 alone, DIGERCIC processed more than 100 million queries from both the public and private sector in a single year, accounting for more than USD 4,5 million of revenue (DIGERCIC, 2019).

DIGERCIC has made available three systems to verify or share information: a) a web page-based service, b) a web service-based solution c) a CD or DVD-based service called “validation of registers”:

a) For the web page service[8], the third party, using a username and a password provided by DIGERCIC, introduces a special number located on the back of the ID card (called fingerprint code) in order to receive a signed electronic certificate that displays the most up-to-date personal information. DIGERCIC charges a fee of USD 0.15 per query for demographic data and USD 0.30 per query for biometric data.

b) For the web service option, DIGERCIC provides direct access to private companies or public institutions to its database through a software that enables data exchange between the third parties’ and DIGERCIC’s systems. DIGERCIC charges private institutions a fee of USD 0.08 for demographic queries and USD 0.30 for biometric queries.

c) For the CD or DVD-based service, DIGERCIC validates and provides additional data (e.g., date of birth, nationality, address) for third party databases. For example, a private entity would send a query with the ID number and the name of a person and DIGERCIC would complete it with the address, which is considered public information. DIGERCIC charges a fee of USD 0.12 per demographic query.

Third parties can opt to use one or more services by submitting an application that includes a letter of expression of interest, a form with standards of interoperability, Web Service technical operational documents, and ID cards and tax documents of the entity’s representatives; and the signing of a MoU that includes confidentiality clauses and conditions under which the agreement can be revoked such a misuse of information or inadequate security measures.

[8] *See* the webpage in https://servicios.registrocivil.gob.ec/identidad/#no-back-button

India

India’s Aadhaar system allows for online demographic and biometric authentication against the Unique Identification Authority of India (UIDAI) database by third parties that comply with its requirements. Following a screening process, UIDAI has established physical, secure connections with a number of large organizations known as “authentication service agencies” or ASAs. These entities—e.g., banks, telecom agencies, state and central government agencies, etc.—may verify an individual’s identity for their own purposes or provide identity verification services to third party “authentication user agencies” (AUAs). These AUAs, as well as sub-AUAs that are vetted by the AUAs, are entities such as bank branches and smaller companies that interface directly with individual customers. Identity queries involve directly pinging UIDAI’s database using a person’s Aadhaar number and biometric (e.g., fingerprint or iris scan), demographic data, or one-time-password through a secure internet connection from AUAs and sub-AUAs via the ASAs, allowing for real-time authentication. No physical token (e.g., a smart card) is used in this process.

Government entities and the Department of Posts are exempt from authentication fees. As of March 2019, private entities are charged Rs. 0.5 (USD 0.007) for Aadhaar authentications where only a yes/no response is provided, and Rs. 20 (USD 0.3) for e-KYC transactions, where UIDAI shares a limited number of biographic fields about the individual being verified. Commercial banks that also provide Aadhaar enrollment and updating services are, in most cases, exempt from these charges. As of 2019, UIDAI had processed around 27 billion authentication requests associated with approximately 1.2 billion Aadhaar numbers and has the capacity to process 100 million queries per day.

Pakistan

The National Database and Registration Authority of Pakistan (NADRA) provides authentication and verification services to a number of public agencies, including the election commission, social protection agencies (including the Benazir Income Support program or BISP, the disaster management authority, and the Zakat and Bait-ul-Mal departments), the Federal Bureau of Revenue, the courts, provincial and local governments, and for passport and immigration services. It also facilitates authentication for private firms, including banks, microfinance institutions, other financial service providers, and telecom companies. Some of these transactions are done online in real time, while others are performed in batches for specific needs.

In general, public sector agencies are charged PKR 15 (USD 0.09) per transaction, while private firms are charged PKR 35 (USD 0.29) per transaction. These charges provide a solid revenue stream for NADRA that is used for daily operations (e.g., staff salaries) as well as upgrades to technology and improvements to service delivery. For example, NADRA verified the identities of 100 million SIM card holders for the Pakistan Telecom Authority in 2014, which at a per-unit fee of USD 0.09 would have netted NADRA approximately USD 9 million. Using biometric verification for the quarterly cash disbursements to the approximately 5.4 million beneficiaries of the government’s Benazir Income Support Program (BISP) would provide over USD 1.9 million in revenue annually.

Panama

The National Civil Registry, which is part of the Electoral Tribunal of Panama, has been providing verification services to public and private institutions, including the e-government agency, the Ministry of Health, the Ministry of Foreign Affairs, and the consumer protection office since 2005. Verification and data sharing services are provided free of charge to public institutions and some private entities. For example, in 2014, the National Civil Registry signed an MoU with the Superintendence of the Banks of Panama to provide free verification services to banks in order to facilitate greater financial access and prevent identity fraud and impersonation (Tribunal Electoral, 2019).

Public institutions can connect to the National Civil Registry database through a webservice or via the National Civil Registry webpage using a username and password. Depending on the information required and authorizations granted, third parties can access names, place and date of birth, issuance and expiration date of the ID card, photo, signature and fingerprints. Private institutions only have access to the webpage service and are provided a username and password following the signing of a MoU. In both cases, data use and access permissions, including the type of information that can be accessed, is stated in the MoU.

The National Civil Registry charges a monthly base 'subscription' fee of USD 100 to third parties using verification services and has established a pricing structure where additional fees depend on the number of queries required. In 2018 alone, the National Civil Registry responded to 6,111,221 queries from 51 public institutions and 88,081 queries from private entities. The following chart shows the fees being charged (Tribunal Electoral, 2017):

Scale of queries	Cost per query in USD
1 -10,000	1.00
10,001 - 30,000	0.75
30,001 - 60001	0.50
60001 - or more	0.10

Peru

Peru's *Registro Nacional de Identificacion y Estado Civil* (RENIEC) has been providing online identity verification services using biometrics since 2009. Initially, the service was provided to allow notaries to verify the identity of individuals for transactions such as property sales. Since then, it has been expanded to cover many public and private entities, including social welfare agencies, the justice department, police, banks, commercial centers, and telecom companies. Verification requests are free of charge for government agencies. Private entities are required to pay a fee for verification or authentication services, however, in certain cases—such as government-mandated biometric authentication checks for the onboarding of mobile customers—private- sector third parties may also be exempt from certain fees (RENIEC 2018).

Fees for private entities are based on (a) the type of information requested, (b) the number of queries, and (c) whether verification relies on wired connections or the agency's website. For non- biometric attributes, a variety of authorized users—e.g., small banks, commercial centers, etc.—can query the RENIEC database via the website at a per-transaction cost of PEN 0.9 (USD 0.28) for basic information such as name or date of birth; PEN 1.2 (USD 0.37) for additional information such as photo or address, and PEN 1.6 (USD 0.49) for higher-level data such as a signature. For third parties such as banks that have a wired connection to the RENIEC database, similar non-biometric queries are priced by bulk and cost between PEN 0.6 (USD 0.18) for 0–400,000 queries to PEN 0.11 (USD 0.03) for 1,600,000+ queries. Biometric queries that match individuals' fingerprints against the RENIEC database in order to authenticate a person are mainly used by notaries, telecoms, the police, and social programs. These queries return a "yes/no" response from RENIEC and are priced between PEN 1.5 (USD 0.46) for 0–30,000 queries to PEN 0.14 (USD 0.04) for 1,200,000 or more queries (RENIEC 2017a).[9]

RENIEC processes around 250 million verification queries per year. Of these, approximately 70 percent are performed free of charge for public agencies, while 30 percent are for private entities. In total, this yields approximately USD 45 million in revenue annually (RENIEC 2017b, 2018).

1. Biometric verification (ABIS) - Notaries, telephone companies, police(free), social program (free)

Scale	Cost/query (USD)
0-30,000	0.56
30,001-120,000	0.39
120,001-240,000	0.25
240,001-360,000	0.15
360,001 +	0.09

2. Wired connection query – Banks, commercial centers and government agencies (free)

Range	Cost/query (USD)
0-200,000	0.26
200,001-400,000	0.20
400,001-600,000	0.14
600,001-800,000	0.09
800,001 +	0.06

3. Internet query - Primarily used by small Banks, small Commercial centers, small or government agencies (free), etc.

Unit	Cost/query (USD)
Level 1	0.47
Level 2	0.59
Level 3	0.74

[9] An updated list of services and fees can be found on the RENIEC website at: http://www.reniec.gob.pe/portal/Tinstitucional.htm.

Key Considerations

Balancing Revenue, Demand and Inclusivity

Charging fees for identity verification services can be an important revenue stream for ID agencies, offering fiscal sustainability and greater autonomy. These services can also generate savings for third-party users if the fee levels are less than the cost and liability associated with other methods of identity verification. Setting fees too high, however, may suppress demand from potential public and private-sector users and drive up consumer costs to the point where many people, and often those the most in need, can no longer afford services. Fees should be set in a manner that fosters inclusion and ensures the affordability of identity verification services, both for large organizations and for smaller ones that serve poor, rural and other marginalized groups.[10] Moreover, ID agencies should be able to provide basic services and to cover operational costs regardless of their revenues from verification fees. For example, in Argentina, by law, the revenues obtained from verification services will be only allocated to cover costs regarding the "modernization and institutional strengthening in the identification of persons."[11] Since identity verification services are a public good and pre-requisite for delivering certain services, including to the poor, there may be use cases where identity verification services will need to be provided free of charge or highly subsidized in order to remain inclusive.

Independent Oversight and Consultation

Continuous consultation with a diverse array of potential users can help avoid excessive fees that can result in exclusion or the use of less accurate data for service provision. In addition, where identity providers have a monopoly on identity verification, a strong regulatory and oversight framework is necessary to help ensure that rates remain affordable and transparent, and that the ability to generate revenues does not create perverse incentives for the identity providers. In Ecuador, Peru and Pakistan, for example, independent regulatory bodies approve fee schedules. In the Peruvian case, identity verification fees are approved and endorsed by the Council of Ministers after a consultation process, that includes a calculation of fees, which have to be equal to their administrative cost, based on a "Single text of administrative procedures"[12] created by the Peruvian Government. In Ecuador, changes in verification fees must be approved by the Ministry of Finance (DIGERCIC, 2019).

Fee Structures

One way to promote affordability and inclusivity is through price differentiation, as fees for verification services need not be uniform across third-party users, types of transactions, or over time. For example, based on the information provided, nine of the twelve countries analyzed do not charge verification fees to other public institutions. When it comes to the method used for charging fees, five countries (Argentina, Ecuador, Malaysia, Pakistan, and Tanzania) opt to charge a fixed amount per query, while four countries (Chile, Colombia, Panama and Peru) have a scaled fee structure, whereby higher volumes of verification requests by the same entity cost less on a per-request basis. In Pakistan, NADRA charges fees to public-sector users, but they are lower than those for private users. In India, UIDAI initially opted to keep all authentication services free in order to ensure rapid uptake among a variety of third parties; it has now introduced charges for certain private sector users. In Panama, the National Civil Registry does not charge public institutions nor some private entities in order to help prevent identity fraud and impersonation.

Rules and Criteria for Third Party Access

In order to set conditions under which the service will be provided, ID providers can sign a memorandum of understanding (MoU) with third parties, including public institutions and private entities. MoUs usually set out the means through which third parties send queries (i.e. through wired connection; web service, etc.); how ID providers respond (i.e. RENAPER and the Chilean Civil Registry, send "hit" or "no hit" depending on whether there is a match in the data or not); the conditions of appropriate use and confidentiality of the data transmitted; and the conditions for compliance with data protection laws or other relevant regulations in a given jurisdiction.

In addition, MoUs can include payment conditions for the use of the service, which may be a fee for each verification or pricing for a set volume of queries. MoUs in some countries also indicate that a "fee connection" will be charged. For example, the *Registraduria* in Colombia charges a fee of COL $10,276,250 (~USD 3,190) for a technical test to ensure that the third party has the capacity to responsibly use the service, while the Chilean Civil Registry charges about USD 413 for each connection. Moreover, MoUs usually specify that the ID provider has the power to terminate the agreement if the recipient does not comply with certain conditions. For example, in the Chilean model, the Civil Registry can terminate the agreement if the third party does not use the services for a period of three months.

The specific models of agreement should be based on a comprehensive legal framework and relevant regulations. In order to promote transparency, it is considered good practice to publish MoU templates on the ID provider's website. For example, in Panama[13] and Argentina[14] templates and requirements are available on the institutions' websites.

Planning for the Future

The sustainability of a verification fee-based revenue stream depends, inter alia, on the system's capacity to handle large amounts of transactions as demand for these services grows over time. In India, for example, UIDAI's current capacity is 100 million transactions per eight-hour workday (see authportal.uidai.gov.in for real-time statistics on authentication). UIDAI plans to increase its processing capacity fourfold in order to handle an anticipated increase in demand for verification services due to the growing cashless economy and the uptake of Aadhaar authentication across a growing number of organizations. Advanced planning and investment in robust support infrastructure will help to ensure the long-term adaptability of a system.

[10] In Pakistan, for example, there are concerns that a focus on commercialization of identity services has led NADRA to verify more data fields than required, and that the fees are a burden on the financial sector, which could hamper financial inclusion by keeping fees high for consumers. See: https://www.theguardian.com/world/2015/mar/03/pakistan-fingerprint-mobile-phone-users

[11] Argentina 2018 National Budget Law Number 27431. Article 94. Available at: http://servicios.infoleg.gob.ar/infolegInternet/anexos/305000-309999/305347/norma.htm

[12] The "Single text of administrative procedures" was approved by the General Administrative Procedure Law. Available at: https://www.indecopi.gob.pe/documents/20795/225805/07.+Ley+del+Procedimiento+Administrativo+General+-+Ley+27444.pdf/725a60ce-7f01-4542-9e1f-82ac40dd5810

[13] https://www.tribunal-electoral.gob.pa/direccion-superior/secretaria-general/servicio-verificacion-identidad-svi/

[14] https://www.boletinoficial.gob.ar/#!DetalleNorma/192957/20180927

References

Argentine *Boletin Oficial* (2018). Resolution 430/2018. Ministry of Interior, Public Works and Housing. https://www.boletinoficial.gob.ar/#!DetalleNorma/189151/20180801.

Chilean Civil Registry "Correspondence with Chilean Civil Registry" January 4, 2019.

Chilean Library of Congress (2006). Ministry of Justice. Resolution 592, 2006. Available at: https://www.leychile.cl/Navegar?idNorma=248220&idVersion=2006-03-18

DIGERCIC "Correspondence with DIGERCIC, Ecuador" January 2019

Registraduria Nacional del Estado Civil de Colombia, "Correspondence with *Registraduria*, Colombia" December 4, 2018

RENAPER "Correspondence with RENAPER, Argentina." December 4, 2018.

RENIEC. 2017a. "Texto Único de Procesos Administrativos/TUPA 2017." Registro Nacional de Identificación.

———. 2017b. "Correspondence with RENIEC, Peru," January 11, 2017.

———. 2018. "Correspondence with RENIEC, Peru," January-March, 2018.

Tribunal Electoral (2017) *Servicio de verificación de identidad para consultas*. Retrieve from: https://www.tribunal-electoral.gob.pa/direccion-superior/secretaria-general/servicio-verificacion-identidad-svi/

Tribunal Electoral (2019). *TE suscribe convenio con la Superintendencia de Bancos para el uso del SVI*. Retrieved from: https://www.tribunal-electoral.gob.pa/te-suscribe-convenio-con-la-superintendencia-de-bancos-para-el-uso-del-svi/