Digital Identity Guide for Tax Administration

MINISTERIO
DE ASUNTOS EXTERIORES, UNIÓN EUROPEA
Y COOPERACIÓN

aecid

cooperación
española

Digital Identity Guide for Tax Administration

Digital Identity Guide for Tax Administration

ISBN: 978-9962-750-07-9 (PDF)
ISBN: 978-9962-750-08-6 (ePub)

Cite as follows:
Inter-American Center of Tax Administrations (2026). *Digital Identity Guide for Tax Administration.*

Authors

- Alejandra Carratú
- Jimena Hernández
- Juan Pablo García

Reviewed by:

Raul Zambrano
Fransheska López
Elizabeth Rodríguez

Content

Acknowledgments

This work was made possible thanks to the valuable contributions of key natural persons from various Tax Administrations in the region. We express our special gratitude to the technical teams, management, and institutional correspondents of the Tax Administrations of Brazil, Chile, Costa Rica, Ecuador, Spain, Guatemala, Honduras, Mexico, Panama, Peru, and Uruguay.

We especially thank the CIAT technical team for their constant support, methodological guidance, and strategic vision in guiding us through this research.

Introduction

Within the framework of the international cooperation agreement between the Spanish Agency for International Development Cooperation (AECID) and the Inter-American Center of Tax Administrations (CIAT), the aim is to provide professionals in Latin American tax administrations with specialized training in the integration of digitalization and new technologies. In this regard, the purpose of this Guide is to serve as a reference for tax administrations, especially those in Latin America, in the implementation and management of digital identity mechanisms, considering the specific characteristics and needs of the tax sector, both for the administration and for taxpayers.

The digital transformation of tax administrations requires technological, regulatory, and operational frameworks that guarantee the efficiency, transparency, and accessibility of the digital services provided. In this context, digital identity emerges as an essential component for enabling reliable and seamless interactions between taxpayers, public agencies, and automated systems. Its importance lies in the fact that it allows for the **secure, unique, and remote** identification of citizens, companies, and third parties interacting with the administration.

Digital identity is not merely a technological resource: it is an **enabling institutional capability**. Its adoption is strategic, given that its proper implementation transforms the relationship with taxpayers, improves tax administration, and moves toward smarter, more people-centered models.

Below are some of its most relevant benefits, which explain why it constitutes a strategic component in the modernization processes of Tax Administrations:

- **Facilitates access to digital tax services:** digital identity is the gateway to procedures, tax returns, payments, and inquiries without the need for physical presence.
- **Reduces costs and operating times:** by automating identity verification, it reduces the administrative burden for both the Tax Administration and the taxpayer.
- **Increases legal certainty and security:** it ensures that digital interactions are protected against impersonation and/or fraud.
- **Improves conditions to facilitate compliance with tax obligations:** a more agile and reliable digital experience promotes a more transparent relationship between the taxpayer and the administration.

- **It enables interoperability between public systems:** a standardized digital identity facilitates data exchange with other institutions, improves traceability, the integration of government services, and the public value offered to citizens.

In relation to international recommendations, both the Organisation for Economic Co-operation and Development (OECD) and the Inter-American Development Bank (IDB) recognize digital identity as a key component in their respective strategic frameworks. The Tax Administration 3.0 model (OECD, 2020) includes digital identity as one of its "core components," enabling the secure, unique, and integrated identification of taxpayers. Furthermore, the IDB's digital maturity model (Inter-American Development Bank, 2023) considers it a critical cross-cutting capability that enables user-centered digital services.

However, according to the OECD report (2024), while it highlights that most tax administrations already offer authenticated digital access, it also recognizes that the degree of progress varies significantly between jurisdictions, reflecting regional asymmetries in terms of technological capabilities, infrastructure, and level of digitization.

Given the diverse realities of Latin American countries, this Guide aims to provide a practical approach to the strategic, technical, and legal aspects of digital identity in tax contexts, using clear and accessible language.

Chapter 1 covers key concepts related to digital identity and identification, including their evolution toward more reliable, interoperable models aligned with best practices. It also identifies the technical and regulatory challenges that must be addressed to consolidate an inclusive, secure, and regionally integrated digital ecosystem. Concrete examples illustrating progress in cross-border identification are presented, and the strategic role of tax administrations in driving this transformation is discussed.

Chapter 2 provides an overview of the current state of digital identity within tax administrations in Latin America, considering regulatory and technological aspects, as well as the level of implementation and development in each jurisdiction. This survey was conducted using a structured questionnaire and supplementary research on digital government portals, with the aim of understanding the challenges and problems that limit the effective deployment of digital services in different administrations and their relationship to digital identity.

Chapter 3 analyzes cutting-edge trends and makes strategic recommendations for the evolution of digital identification in tax administrations, considering emerging approaches and current dynamics, while acknowledging the different starting points in each country. It also delves into key components such as authorization and auditing, pillars of the AAA model, whose implementation is essential to guarantee traceability, control, and trust in digital identity systems.

The aim is for this Guide to be a tool designed to support organizations beginning this process, while also reinforcing existing models. It also seeks to promote best practices and facilitate informed decision-making on public policy related to this topic, contributing to strengthening the digital transformation of tax administrations in the region.

1. Evolution and Trends in Digital Identification

1.1. Identity and Digital Identification

Digital Identity

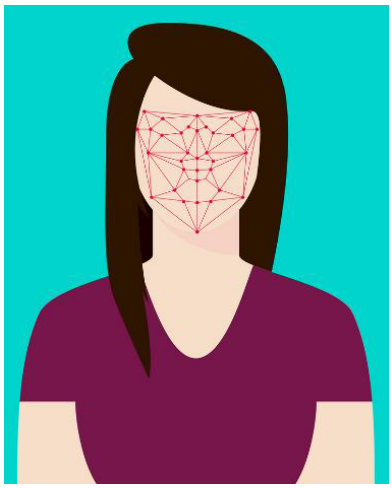
Digital identity is information about a person that exists in the digital world. This information is composed of various types of data, including structured data such as names and surnames, identification numbers, as well as information related to their habits, images, and videos, among other things. This data is generated by each person based on specific information entered into different systems but also includes information that some applications and devices infer about us, such as behaviors, tastes, opinions or ways of thinking, preferences, places we visit, videos, and even each "like" we register through **our** interactions on social media. Much of this information is generated without our knowledge or, at least, without our awareness.

All this trail of information about each person that is left on the internet is known as a digital footprint. It is not the purpose of this publication to delve deeply into this topic, but it is important to keep in mind that a digital footprint represents who we are, what we like and dislike, what we think, our habits, our relationships, our interests, and our values. It is important to be aware of this issue and to know techniques and tools to protect it. An active digital footprint is the one we create with our conscious actions, such as posting on social media or filling out electronic forms, among others. A passive digital footprint is the one that is created without us being fully aware of it, such as the IP addresses we use, geolocation data, the time spent on websites, and the articles or news we read, among others.

Identity is made up of many different types of data that are part of our footprint and can be used for different purposes, either by their owner (person) or by a third party (algorithm, software, person, or organization). Some search engines use it to personalize user searches or to offer personalized advertising. The information

that makes up a person's digital identity includes personal data such as names, document numbers, date of birth, address, email, credentials, personal documents, etc.

On the other hand, approaching the topic from a more philosophical perspective, we can conclude that, in the digital world, our identity no longer depends solely on our physical presence or our physical bodies. As we have seen, it is formed from the information we share online, how we interact on social media, and the profiles we create. Every action, every expressed preference, every connection forged contributes to shaping a version of us that exists and evolves within the digital ecosystem. From this perspective, digital identity is not just a collection of data: it is a way of showing who we are in this information age.



Digital Identification (Authentication)

Digital identification is the process by which a person, entity, software, or object is recognized and validated by another (person, entity, software, or object) in a digital environment. In the physical world, to be recognized, we present ourselves by showing an identification document (national ID card, passport, etc.), and the verification of our identity occurs implicitly since we are physically present. In contrast, in the digital world, a person must identify themselves using data linked to their digital identity—such as username, document number, or credentials—and must also provide evidence that proves they are indeed who they claim to be, since there is no physical presence to verify it. This process of identification and verification is known, in technical terms, as the authentication process.

In the digital world, when two computer systems interoperate, they must also digitally identify each other to ensure the proper handling of data and reduce risks related to information leaks or unauthorized access.

Operational Foundations of Digital Identity

After reviewing different approaches to the concept of digital identity and digital identification, it is important to establish that, in the context of this publication, a definition of digital identity will be adopted that focuses on its role as an identification mechanism and is considered equivalent. In this sense, ***Digital Identity is understood as the set of attributes and credentials that allow for the secure and unique recognition of citizens in their interaction with digital services,*** functioning as a tool to validate that the person accessing an online service is indeed who they claim to be.

Identity is used to validate a person or entity during the digital identification process, using different techniques or technologies.

AAA model (Authentication, Authorization, Auditing)

In the context of cybersecurity, Authentication, Authorization, and Auditing are known by the acronym AAA and are important concepts associated with and determined by digital identification. The importance and reliability of identification are crucial for determining authorization and subsequently conducting a proper audit.

Depending on how it is implemented, Authentication and Authorization, especially in computer systems using outdated standards and models, are often viewed as a single issue, but this is no longer the case. As will be discussed later, there is an increasing separation between Authentication and Authorization. With the emergence of digital identification systems or ecosystems, where natural persons use a single digital ID across multiple digital services, it is necessary for each service to focus on developing a proper authorization and role management scheme.

Furthermore, in a world where cyber threats have increased exponentially, auditing has become a key element for building trust in computer systems. A proper audit implementation on an information management system allows for determining what happened, when it happened, who the actors involved were (what each actor did), and from where they acted, among other things. All these elements allow for reconstructing the events and, consequently, ensuring the integrity of the information. They also provide reliable information as evidence in cases of criminal activity.

While the focus of this work is on digital identification (authentication) in tax administrations, authorization and auditing are defined as follows:

- **Authorization:** Once a person is authenticated by the system, it authorizes them to access certain information and perform specific actions. This process depends on the user's profile, the reliability of the authentication methods used, and the system's specific rules. It is beyond the scope of this Guide to delve into this topic in detail, but it is important to keep in mind since authorization depends, first and foremost, on digital identification. As will be discussed later, in systems where authentication is handled elsewhere, the authorization process must still be managed by the system itself.
- **Auditing:** This involves tracking and recording all actions that each user performs on a system. It is an important aspect today for several reasons, such as the ability to determine what happened in the event of an incident and answer questions like which users accessed and/or modified which information, among others.

Chapter 3 will delve deeper into these two topics, given that, according to current trends, they are aspects that will become increasingly relevant in Tax Administrations.

1.2. Evolution of Digital Identification

The Beginnings of Digital Identification

During the 1970s, with the emergence of the first computer systems, digital identification was reduced to a unique code that the user entered into a system to identify themselves and thus access their information and the operations the system offered based on their profile. This code fulfilled both functions: it identified the person and simultaneously validated their identity, so it was considered a secret between the system and the person. It was generally created within the system and then communicated to the user, in a world completely different from today's.

Classic Digital Identification

Shortly thereafter, systems were developed that separated the "user" entity (identifier) from the verification process, giving rise to the concept of **authentication**. The act of authenticating, also known as "login," is the process of identifying oneself and verifying that identification. In this scenario, a person enters data that uniquely identifies them into the system, such as a national identification number, a unique username, or an email address. They must then verify their identity so that the other party (the computer system) can confirm that the person is indeed the one who identified themselves. To validate the identity, a predefined factor must be used between the system and the user. These factors can be of three types:

- Something I know: something that only the computer system and the person know, i.e., a shared secret like a password or PIN.
- Something I have: something that the user possesses and that the computer system knows only that person has. This could be, for example, a coordinate, a unique number, or a one-time password (OTP).
- Something I am: This is where biometric technologies come into play, obtaining information such as fingerprints, iris scans, or facial recognition.

A few decades ago, many systems allowed users to choose their identifier, requiring them to enter a word that identified them, if such word hadn't already been chosen by someone else. This word was unique within the system, thus allowing for the unambiguous identification of the user. Since the beginning of this century, this

has evolved toward more universal identifiers, such as email addresses. An email address, according to its RFC 5322 standard (Resnick, 2008), consists of a username, the special symbol "@," a subdomain (optional), a domain, and the mail server extension (example: juan.perez@gmail.com, juan_perez@correo.universidad.edu.pa, etc.).

Note that an email address is a universal identifier. An identifier composed of a country code, a document type, and a document number is also universal (example: Uruguay – National Identity Card – National Identity Card Number). This trend toward using universal, or at least broader, identifiers deepened in the early years of this century. This approach will be discussed in more detail later.

This authentication system, based on an identifier and a method for validating identification, has had to evolve by strengthening various aspects, given technological advancements, the widespread adoption of the internet, the increase in computing power, and the risks that all these advances entail from a cybersecurity perspective, particularly regarding identity theft.

One of the first actions to strengthen it was the emergence of "password policies" which, through proper implementation in different systems, ensure that people choose strong passwords. That is, a combination of characters long and complex enough that, from a statistical perspective, it would take a system decades to decipher them using brute force techniques or dictionaries of possible text combinations.

Policies also became more complex due to the increasing level of cybersecurity risk, requiring passwords to be changed periodically and prohibiting the use of old passwords. Furthermore, best practices and recommendations advise choosing different passwords for all systems used.

Other security precautions were also implemented, particularly regarding how user passwords are stored in databases. For many years, best practices have indicated that passwords should not be stored in cleartext, because if an unauthorized third-party gains access to the database, they could easily access user credentials. The most recommended and widely used practice is based on cryptography, specifically hash functions that transform the password into an unrecognizable and irreversible sequence.

This Guide does not aim to delve deeply into this topic, but it does highlight that storing passwords in cleartext has been considered a significant vulnerability for decades. If an attacker manages to extract a database of user credentials, even if they are encrypted, there is a risk of a brute-force attack attempting to decrypt the passwords. This is one of the reasons why password policies require strong passwords and the need to change them periodically.

However, that scenario—with strong, encrypted passwords—is no longer sufficient on its own. In recent years, attack methods have intensified and become more sophisticated, such as phishing or the use of malware

designed to intercept user activity. For example, keyloggers, capable of recording every keystroke, allow attackers to capture passwords even before they reach the system and are encrypted. Given this situation, password strength remains necessary, but not sufficient, and additional mechanisms are required.

Multi-Factor Authentication (MFA) Systems

The implementation of Multi-Factor Authentication has become one of the most effective strategies for reducing risk, especially in environments where sensitive information, such as financial or tax data, requires high levels of protection. This led to the emergence of systems that use two-factor authentication (2FA).

These mechanisms work as follows: once the person (user) is identified, they must use "something I know" followed by "something I have" or "something I am." A commonly used combination is a strong password (something I know) and a one-time password (OTP, something I have). An OTP is a code, usually six digits, generated by a mathematical algorithm that is unpredictable. This makes it impossible to know what the next code will be, so if the user enters the correct code, their identity is validated.

An OTP can be managed in three ways:

- After the user enters the password, if it is correct, the system generates the code and sends it to the user via another previously agreed-upon method, for example, through SMS or WhatsApp to the user's mobile device or email. This requires a device with a battery, internet connectivity, and/or email access.
- The user downloads a mobile application for this purpose, such as Google Authenticator or Microsoft Authenticator, and synchronizes it with the system beforehand. This ensures that both use the same mathematical algorithm, the same timings, and begin generating numbers from the same seed, so both should always have the same valid OTPs. This requires the user to have their mobile device available for digital authentication.
- The organization responsible for the system provides the user with a physical token. This is a piece of hardware that has the mathematical algorithm configured, as is the case with the mobile application, and a small screen that shows the user the number generated. In this case, it is necessary to deliver the device to the user in person (or in a secure manner), and the user must have the device when they wish to identify themselves digitally.

For the last two cases, there is a widely used international standard called Time-based One-Time Password (TOTP), which is a time-based one-time password defined by the Internet Engineering Task Force (IETF). For it to work correctly, in addition to defining a common seed, the clocks of both devices—phone or token and server—must be synchronized (M'Raihi, Machani, Pei, & Rydell, 2011).

There are some significant security differences when implementing an OTP mechanism. Sending an OTP via SMS is more vulnerable than via WhatsApp because the SMS channel is less secure. In turn, synchronous OTP generation using an authentication application or token, especially if it's not linked to the mobile phone, is more secure than any transmission method (even via WhatsApp or email). In this case, the code isn't transmitted through any channel but is generated simultaneously on the user's device and the verification system, reducing the risk of interception.

According to best practices and recommendations, each OTP should last between 30 and 60 seconds, but for critical systems with highly sensitive information, this duration could be reduced to 20 seconds for greater security. A limited number of attempts are also generally allowed. After a certain number of failed attempts, the OTP mechanism becomes invalid, or the system directly blocks the user. For mobile or web applications, where it is necessary to connect via the Internet, slightly longer times are generally allowed due to possible connection latency.

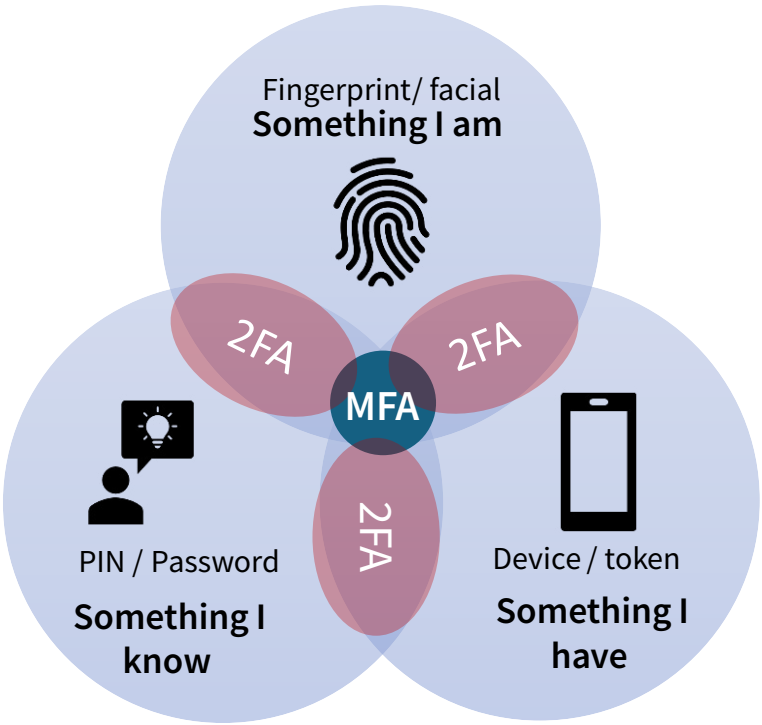
In all cases, there are some disadvantages and limitations. Sending the code to the mobile device involves messaging costs, which represent considerable expenses for mass services. The OTP generated in a mobile application is often not a simple tool for inexperienced users, and in the case of hardware OTPs, the device must be delivered to the user personally (or securely), which generates logistical and operational costs. Furthermore, the user must carry the device with them whenever they need to digitally identify themselves.

It is also possible to use biometric factors, that is, "something I am." Nowadays, all mobile devices have cameras and the ability to take a photo of the user; some also have fingerprint readers. In the case of photos, the system must also implement a tool known as liveness detection. This is software that takes a video or sequence of images, which is then analyzed with Artificial Intelligence to ensure that the image obtained belongs to a living person and not merely a previous photograph. If this condition is met, the photograph taken of the person must be biometrically compared with another photograph available in the system, previously uploaded. While there are variations on this topic, it is a useful method but generates significant costs for the entire system and requires the user to have devices such as cameras and a suitable location in terms of lighting, position, saturation, etc., to capture the images.

Currently, the use of digital IDs with strong passwords and multi-factor authentication mechanisms has become essential; however, these methods have vulnerabilities. Unfortunately, in the last decade, the evolution of cyber threats has been rapid. There are now multiple variations of phishing methods—such as smishing (via SMS), vishing (via voice), and quishing (through fraudulent QR codes)—which, combined with artificial intelligence tools, advanced social engineering, sophisticated attack techniques, and certain types of malwares, have weakened the reliability of two-factor authentication (2FA).

In recent years, the term Multi-Factor Authentication (MFA) has emerged. This involves adding more factors, combining “something I know” with “something I have” and “something I am.” The following image illustrates the concepts of 2FA and MFA:

Figure 1. 2FA and MFA.



***Source**:* Prepared by the author

While this trend in MFA helps protect digital IDs, it still involves strengthening a mechanism designed decades ago in a completely different reality. Using multiple factors generates significant costs, considerably hinders usability, and does not guarantee against identity theft.

Under this traditional digital identification model, recommendations suggest using different and complex passwords for each system, changing them periodically, and employing other authentication methods that require a specific physical device and/or a mobile phone and a pre-configured application. Although well-intentioned, all these recommendations are not foolproof and, moreover, make it extremely complex for people to manage their digital IDs, which introduces potential vulnerabilities (often “human”) that ultimately lead to increased risks, as well as considerable costs.

These methods, historically based on the username-password combination and later reinforced with various additional measures, are reaching the end of their useful life. With the aim of meeting this need, for some years now, new methods and technologies of digital identification have been promoted, as well as the concept of “Continuous Authentication,” which seeks to rethink digital security.

Passwordless

Another key concept in evolution and main recommendations for digital identification is passwordless authentication. This is a security approach where a user can digitally identify themselves (authenticate) without needing to remember, enter, or manage passwords. As seen previously, password-based methods for verifying identity were designed for a world entirely different from today’s. Having to manage multiple, strong, and distinct passwords for each system daily, in addition to updating them periodically, represents a complex and far from trivial task for most people. This situation brings risks and difficulties.

Instead of using “something I know,” as described earlier, this approach promotes using more secure and easier factors such as:

- Something I have: a device (cell phone, cryptographic token, physical key also known as passkeys) or cryptographic keys also known as FIDO2 (Fast IDentity Online).
- Something I am: facial biometrics, fingerprint, or iris.

In this case, the credentials to verify identity are held by the user, but, in addition, in the case of a device or cryptographic keys, a digital signature is used as a means of verifying identity, and the private key resides on a cryptographic device in a protected and secure manner. These digital signature-based methods will be explored in more detail in section “3.1 Trends in Digital Identification” in Chapter 3. This same chapter also presents a summary of the most relevant digital identification models worldwide, highlighting them as the strongest and most reliable methods of digital identification in all cases.

Continuous Authentication

Continuous authentication is a security approach that dynamically and transparently verifies the user’s identity continuously while they interact with the system, rather than only upon login.

To achieve this, a series of actions and controls are implemented that constantly monitor user activity to detect potential anomalies or fraud attempts. In other words, the system adjusts the required authentication

level based on the risk profile of each action performed. It can also take actions such as requesting digital identification again or sending an OTP (One-Time Password) to a device or email address.

Some of the types of controls implemented under this approach include:

- **Biometric data:** This includes elements such as mouse movement patterns or keyboard typing speed. People tend to have patterns that the system learns as it is used, allowing it to detect anomalous behavior. Another biometric factor used, provided it is explicitly stated in the "terms of use" and accepted by the user, is access to the device's camera continuously or intermittently, to carry out facial recognition, seeking to reinforce the validation of identity in real time.
- **Behavioral data:** Like the previous control mechanism, but related to usage patterns, navigation, reading speed, usage time, schedules, days of the week, etc.
- **Environmental data:** Includes data related to geographic location (obtained via GPS and/or IP address), networks used, type of device used, etc. Regarding the device, people tend to always use the same equipment, such as laptops, mobile phones, or tablets. The system can record a fingerprint that identifies them and associates them with their user, so that each time the user uses their frequently used devices, the risk level can be considered lower.

Proper risk management should be the basis for addressing continuous authentication mechanisms. All the controls implemented generate a dynamic risk level in each work session, which must be considered based on the criticality of the information and the actions the user is performing. Furthermore, this approach requires a learning and training phase since much information is generated from the user's own historical usage. Tools based on the use of Artificial Intelligence are very useful for making better use of information and improving the efficiency of continuous authentication.

Continuous authentication represents a strategic line of evolution for computer systems today, and its adoption should be framed within a philosophy of continuous improvement.

Main References and Security Levels in Digital Identification

Currently, there are three main frameworks in digital identification that are used as references regarding security levels:

- **ISO/IEC 29115, Entity Authentication Assurance Framework:** an international standard that establishes four assurance levels for authentication (International Organization for Standardization, 2013).

- **eIDAS, Electronic Identification and Trust Services:** a European Union regulatory framework where digital identification is framed within a group of trust services with a strong focus on interoperability. eIDAS incorporates concepts from ISO/IEC 29115 but is not formally based on this standard (European Union, 2014).
- **U.S. National Institute of Standards and Technology (NIST) Guidelines:** Guidelines and recommendations issued by NIST, an agency of the U.S. Department of Commerce, that define the requirements that U.S. federal agencies must meet in their digital identification systems (National Institute of Standards and Technology, 2017).

The following table shows a high-level comparison of the main issues relating to digital identification for each standard:

ISO/IEC 29115	eIDAS	NIST SP 800-63-3
Level 1 – IAL1: Low or no trust in identity. Simple authentication methods such as username/password. **Level 2 – IAL2:** Low trust in identity based on official documents and basic controls. Two-factor authentication (strong password and OTP or app). **Level 3 – IAL3:** High confidence in identity, verification based on official documents and strong biometrics. Multi-factor authentication methods (password + physical token, cryptography, or FIDO2). **Level 4 – IAL4:** Very high confidence in identity, verified in person with multiple elements. Robust multi-factor authentication methods with cryptographic devices (hardware) with cross-checks against trusted sources.	**Level 1 - Low:** Minimal confidence in identity. Self-declared data with simple verifications. Simple authentication (username/password) with optional second factor. **Level 2 – Substantial:** High confidence, verification through official documents and/or biometrics. At least one second authentication factor. Formal procedures for revocation, audits, monitoring, etc. **Level 3 - High:** Very high confidence, in-person or biometric verification with liveness detection. Authentication with cryptographic chips according to FIDO2.	**ID Verification:** **IAL1:** Self-declared, no identity verification. **IAL2:** Remote or in-person verification based on official documents and automated biometric controls. **IAL3:** On-site verification with physical controls and strong biometrics. **Authentication:** **AAL1:** Single factor. **AAL2:** Two distinct and strong authentication factors. **AAL3:** Authentication with cryptographic hardware, protection, and multiple factors.

The three cases offer slight suggestions, but agree on the most critical issues, such as the need to use strong biometrics and official documents for identity verification and decentralized cryptographic hardware-based authentication methods (digital signatures).

Regulatory Equivalencies

In the same way that technical frameworks are created for the standardization of digital identification and its security levels, regulatory frameworks have also been incorporated that seek to provide legal certainty to transactions carried out in the digital world and based on an identification process.

Legal certainty in digital environments encompasses everything that contributes to achieving security, including specifically technological or digital tools and instruments, as well as the normative and institutional factors or elements that support them.

When discussing these instruments, two highly relevant concepts form the basis for the afore-mentioned regulatory framework: the principle of functional equivalence and the recognition of the legal validity and evidentiary admissibility of digital identification instruments.

Regarding the principle of **functional equivalence**, it refers to the need, in the electronic world, in cyberspace, for elements that perform the same function as in the material, tangible world. The prime example has been the establishment of the electronic document as the functional equivalent of the paper document and the electronic signature as equivalent to the handwritten signature. They are not the same thing, but rather “something” that has the same functionality. This same criterion can be applied to establish equivalence between in-person and digital identification.

Following the same line of thought as the previous section, and based on the principle of functional equivalence, some ideas regarding the **admissibility** and **evidentiary value** of digital media should be introduced. In this case, the aim is to establish the validity of digital identifications as an essential element for recognizing the validity of the acts that will result from these processes.

A regulatory framework for digital identification must establish legal, technical, and operational foundations to ensure that electronic identification systems are secure, interoperable, reliable, and respectful of natural person rights.

Some key aspects that these regulatory frameworks should include are:

- **Key Definitions:** When establishing regulations on technological matters, it is often necessary to define the scope of some of the technical terms used to facilitate their application and interpretation. It is important to define, for example: digital identity, registration and authentication levels, electronic signature, and digital identification service provider.
- **Scope of the Regulatory Framework or Subjective Scope of Application**: Natural persons, legal entitys, domestic or foreign, public and/or private sector.

- **Guiding Principles:** Functional equivalence, security, confidentiality and protection of personal data, interoperability, international compatibility, technological neutrality or non-discrimination, among others.
- **Identification Security Levels:** Based on standards and according to the risk associated with the transaction. This could also include the minimum technical requirements for each level (e.g., two-factor authentication for a high level), as well as the types of identification methods accepted (e.g., biometrics, digital certificates, mobile credentials).
- **Interoperability and Technical Standards:** Adoption of national and international standards.
- **Institutional framework and roles:** supervisory and regulatory authority. Responsibilities of identification and authentication service providers. Obligations of public and private bodies that implement or use digital identification services. Penalties regime for misuse, negligence, data breaches, fraud, and identity theft.
- Mechanisms for **auditing, controlling, and monitoring** the data used for identification.
- **Legal recognition of digital identification methods:** legal equivalence with physical identity. Where applicable, the validity of digital identity may be expressly defined in administrative, notarial, financial, and other processes.
- Mechanisms for **cross-border** recognition of digital identity systems.

The construction of these regulatory frameworks is fundamental for any digital trust service, as they represent not only a technological solution but also a profound transformation in how legal certainty, authenticity, and proof are built in the digital environment. Their construction and consolidation require a multidimensional approach: legal, technical, and institutional.

Current State of Digital Identification

Currently, we are in a transitional phase, where methods used and reinforced for decades are reaching the end of their lifespan, even though authentication factors (something I know, something I am, something I have) remain valid. Threats and technologies evolve very rapidly, so digital identification must evolve to ensure methods remain secure and easy to use.

Digital transformation and the widespread use of ICTs have introduced numerous opportunities, but also new and challenging risks. Information security threats have increased dramatically over the last decade, and this trend is unlikely to stop in the future.

There are numerous studies by recognized organizations on this topic. For example, the World Economic Forum, in its Global Risks Report 2025, highlights cybersecurity as an essential component of national and corporate resilience. Specifically, the World Economic Forum's *Global Cybersecurity Outlook 2025* estimates a global cybersecurity cost of between $10.5 and $12 trillion by 2025. This figure is equivalent to the world's third-largest economy, after the United States and China. (World Economic Forum, 2025).

Digital identification is a critical component in the digital world, as it protects our private information from the public sphere, establishing a fundamental boundary. Many cyberattacks, frauds, and crimes begin by compromising some form of digital identification. Currently, with advancements in Artificial Intelligence tools, sophisticated social engineering techniques, and our heavy reliance on ICT, threats are becoming increasingly complex.

In recent years, innovative, more secure, and easier-to-use digital identification methods have emerged; some even function similarly to traditional in-person identification.

1.3. Digital Identification Systems and Ecosystems

National Digital Identification System

In the digital environment, a specific identification is used for each digital system, portal, or service, generally through a username and password combination. However, for some time now, there has been a trend toward digital identifications behaving similarly to traditional in-person models.

Citizens typically obtain their national identification in person (national identity card, passport, etc.) from a recognized and competent organization, and it is used in many public and private places. The same is true for passports, which are used at all borders. Thus, there is a small set of (standardized) identifications issued by recognized organizations, which are trusted by an entire ecosystem composed of multiple public and private organizations, as applicable.

In the digital world, various computer systems and digital services have begun to integrate identification providers, and similarly, large user credential aggregators have begun to position themselves as digital identification providers. Today, it's possible to access Spotify, Booking.com, and many other digital portals and services using an account (identification) from Google, Apple, LinkedIn, or Facebook, among others.

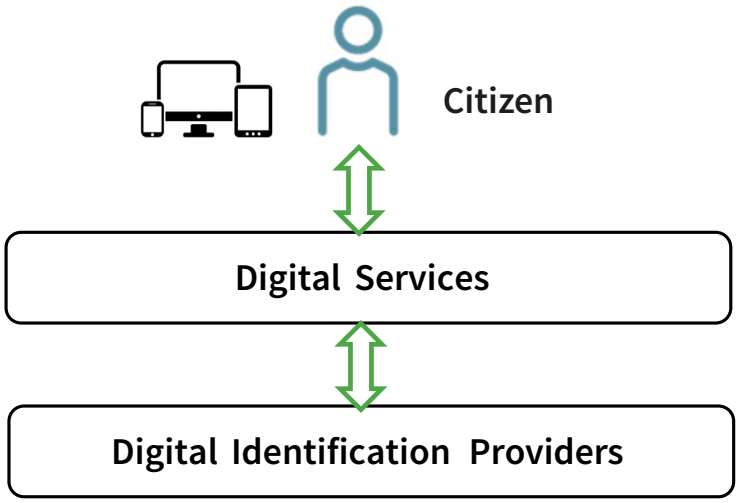
This trend, where digital identifications are becoming more like traditional identifications, simplifies and reduces risks in the digital environment. You can have a smaller number of more secure identifications and use them across multiple digital services.

Not all digital identification providers possess the necessary characteristics for use in sectors that manage sensitive information, such as healthcare, finance, or government. Some countries, primarily in the public sector, have been developing a national digital identification system for several years. This involves creating a single digital identification provider where natural persons register and obtain their credentials, which are then integrated into public digital services. As a result, each person possesses a digital identity that they use throughout the public sector, or at least a large part of it. In some cases, this also extends to the private sector; that is, the same digital identification used to access public digital services can also be used for private sector digital services.

The centralized national digital identification system is not just a software solution that manages digital identities; it must develop strategies, regulatory frameworks, standards, and requirements that ensure digital identifications are suitable for integrated digital services, just as is the case with providers of traditional or physical identification (national identity cards, passports, etc.).

The following diagram shows this situation in simplified form:

Figure 2. Schematic of a centralized national digital identification system.



Source: Prepared by the author

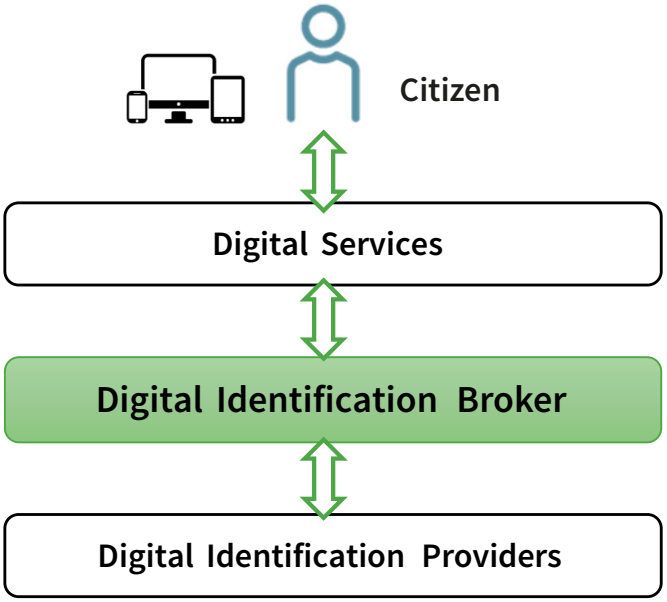
National Digital Identification Ecosystem

Some countries are moving towards a federated digital identity scheme. This involves having a regulated and standardized group of digital identity providers integrated into multiple digital services, generally in the public sector, but it could also extend to the private sector.

Natural persons possess a single digital identity. Each identity provider in an ecosystem has different methods for identification, but they all use the same identity. This means that the person is always the same, but has different methods to identify themselves digitally, which greatly facilitates access.

In this type of scheme, it is extremely important (but not essential) to include an extra piece of software, an intermediary called a digital identity broker, to facilitate integration and evolution. A digital identity broker **is a platform** that positions itself between digital systems and digital identity providers. On the one hand, it integrates digital identity providers suitable for its ecosystem, whether public or private. On the other hand, it integrates with digital services (online procedures, portals, government management systems, etc.) which, in this way, inherit the entire ecosystem of digital identifications. The following diagram illustrates this situation in a simplified way:

Figure 3. National Digital Identification Ecosystem Scheme.



***Source**:* Prepared by the author

A citizen who needs to access a digital service within the ecosystem chooses an identification provider through the broker, digitally identifies with that provider, and then returns to the service to access their personal information. The services delegate the digital identification (or authentication) of natural persons to the providers integrated into the broker. In this way, the digital identification of natural persons is unique across the entire ecosystem, like traditional in-person identification.

Access control (authorization) is specifically defined by each digital service based on the profile or role of the person who identified themselves and the level of trust in the identification they used.

Like a centralized national digital identification system, this scheme also needs to develop and evolve strategies, a regulatory framework, standards, and requirements, but it also offers some advantages:

- **Diversity of providers:** Including more than one digital identity provider (public and private) can be important for achieving greater reach and, therefore, facilitates the possibility for people to access digital identification within the ecosystem.
- **Integration of new methods:** If new providers and, above all, new digital identification methods appear, they only need to be integrated once into the broker to become available throughout the ecosystem and for users to use them in all integrated services, without needing to reconfigure each one. This maximizes the efficiency and economies of scale of the national system, since all integrated services, including the Tax Administration, automatically benefit from the advancements without individually reconfiguring each one.
- **Continuous authentication through AI:** Incorporating intelligent cybersecurity services into the broker, using artificial intelligence tools, strengthens all digital identifications throughout the ecosystem, reducing risks and increasing efficiency.
- **Statistics and transparency:** By centralizing data at a single point of access, a large volume of reliable statistical data is generated, which can be used for strategic decision-making and for the creation of open data (public data release).
- **Cross-border identification:** The broker acts as an intermediary between the national and international ecosystems, performing the necessary transformations and validations to facilitate interoperability.

In a centralized national digital identification system, and especially within an ecosystem facilitated by an identification broker, certain key strategic issues must be addressed, which will be discussed below:

Governance: It is necessary to define governance at the national level, including who will be responsible for defining standards, protocols, regulations, etc. In the case of an ecosystem, governance must also encompass

the development, evolution, and operation of the broker. This implies defining a national regulator to lead initiatives for the cross-border recognition of digital identifications.

Regulations: Regulations associated with digital identity and identification must be formulated, providing a robust legal framework aligned with international standards. Aspects such as the legal validity of digital identifications, guiding principles, and the protection of personal data must be considered. Clear regulations not only provide legal certainty for digital transactions but also facilitate adoption by public and private entities, as well as citizens.

Security Levels: A digital identification can have different levels of security. This level of trust generally depends on two variables: how the person obtained their identification (online without identity verification, in person with biometric verification, etc.) and what forms of identity verification they used when authenticating to a system (weak password, strong password, MFA, or digital signature, among others). It is important that these parameters, and therefore the security levels, are clearly defined at the national level.

Some experiences in the region define three possible levels:

- **Low:** A user who registered online, validated their account via email, and the system performed some simple checks, but there are no guarantees that the person is who they claim to be since their identity was not verified. When identifying themselves digitally, they use their username and a strong password.
- **Medium:** A user who initially had a basic account and validated their identity through an enabled method (in person, biometrics, digital signature, etc.). When identifying themselves digitally, they use their username, a password considered strong, and a second authentication factor.
- **High:** A user who registered with a provider in person and underwent biometric fingerprint validation against the public registry. The registration expires, so it must be renewed periodically. When identifying themselves digitally, they do so using a digital certificate recognized by the National Public Key Infrastructure, employing an advanced electronic signature for digital identification.

Identification data: First, a universal identifier at the national level must be defined. Natural persons will obtain their digital identities from a digital identity provider, either a single provider in the case of a national system, or from one of the providers within the ecosystem in a federated model. For this to work, it is important to ensure that the user is uniquely identified in each system, regardless of the provider used, since in all cases it is the same person. Some ecosystems in the region use three fields to identify a user:

- Country code according to ISO 3166-1 alpha-2, the standard that defines the country codes used in geographic top-level domains (ar, br, pe, pa, uy, etc.).

- Document code: the code of the physical document with which the user registered (ID card, national identity document, passport, etc.).
- Document number used for registration, i.e., the document number corresponding to the above code, issued by the country according to the ISO 3166-1 code.

This combination of the three elements makes identification universal, not just at the national level. This is an important point for cross-border digital identification, which will be addressed in the next section of this chapter.

Other user data: It is necessary to regulate what user data will be managed (exchanged), in addition to the identifier, such as names, surnames, email address, telephone number, and/or date of birth. In this regard, using a sufficient but minimal set of data can be good for protecting personal information. If the services that users access then require more information, they must interoperate with external data sources in a specific manner, always with the user's permission.

Official sources for validating identities: In many countries, governments, through their official civil population registries, have developed digital services that are used by digital identification providers, among others. This service is formalized through an agreement between the parties and allows a third party to validate user identity data, including, in many cases, biometric data, primarily facial images and fingerprints. While the necessary precautions must be taken to protect user privacy, it is an important tool for strengthening trust in digital identification throughout the country, as it can be used by both the public and private sectors.

Technical protocols and standards: It is necessary to incorporate protocols as well as security standards. Regarding protocols, there are several proven protocols for this purpose; the most recognized are Security Assertion Markup Language (SAML), OpenID Connect (OIDC based on OAuth 2.0), and more recently, OpenID Connect for Verifiable Credentials (OIDC4VC) for integrating methods based on the use of verifiable credentials. This topic will be addressed in greater detail in Chapter Three.

Single Sign-On (SSO): Implementing a centralized authentication mechanism, such as SSO, is fundamental to ensuring a smooth and secure user experience within a national digital ecosystem. This mechanism, under a centralized authentication system or ecosystem, allows a user to identify themselves only once and maintain their identification active throughout the entire work session across all integrated systems. This widely used and user-friendly feature, in simplified terms, is implemented as follows:

1. The user chooses an identification provider and enters their credentials (regardless of the method).

2. If the credentials are valid, the identification provider generates an authentication token (SAML assertion or OIDC ID Token).

3. When the user attempts to access a service that trusts the chosen identification provider, instead of requesting credentials again, the service validates the issued token transparently to the user.

   An authentication token is a text string signed by the identity provider, issued in a personalized format to a user, device, or entity once their identity has been verified. This token represents the authenticated session, linked to both the user and their identity provider, considered trusted by the ecosystem.

   When the user accesses a new integrated computer system, that system simply verifies the token's signature, and if the signature is valid, it assumes that the information contained within it regarding the user's authentication is correct. For security reasons, authentication tokens have a limited validity period; a specific duration is defined upon creation, after which the user must re-authenticate.

   In many cases, SSO is combined with appropriate continuous authentication. For example, a user can navigate through different systems within the ecosystem while maintaining an active session, but if they perform a sensitive operation or access confidential information, the system requests the identity provider to re-validate the user's identity.

Toward Cross-Border Digital Identification

As countries advance in developing national digital identification systems or ecosystems, the challenge of cross-border interoperability must be addressed. A simple way to begin thinking along these lines is to look at how this problem has been solved in the physical world and apply the same logic to the digital world.

For many decades, physical identification documents have been obtained from accredited and recognized organizations in the countries of origin. National identification documents, driver's licenses, and other similar documents are processed in person with specific, strict identity verification protocols, such as the use of biometric technology (e.g., fingerprints). These documents are used for identification in public offices, but also in private organizations.

In turn, these documents are also used for identification abroad and are trusted by many organizations worldwide. It is important to keep in mind that while these documents identify natural persons, it should not be forgotten that, in some cases, additional permissions such as visas may be required. These permissions are not part of a person's identification; that is already handled by a passport. They are part of access control or authorization, according to applicable regulations.

This model has its equivalent in the digital environment: once a person has been correctly identified, each system may require additional authorization mechanisms to allow access to specific functionalities, in accordance with policies and/or the level of sensitivity of the information. That is why, in the digital world, we must move in this direction; that is, people should use reliable digital identifications from their countries, not only to identify themselves within their borders, but also internationally, on digital services in other countries.

This would not only be more natural and easier to use, as it would be done in the same way as physical identification has been for many decades, but it would also be more accessible to people and more reliable for all parties. For citizens, it is much simpler to obtain a verified digital ID in their own country—for example, in person with biometric fingerprint verification—than abroad, where in most cases it is not feasible. Furthermore, it would be more secure because better identity checks can be carried out in their country, thus obtaining digital IDs with a much higher level of trust, just as with traditional IDs.

There are several initiatives underway to advance cross-border digital identification, enabling people to use trusted digital IDs from their home countries to access digital services in other countries.

In Europe, eID is a federated electronic digital identification system recognized at the European level. This ecosystem is regulated by eIDAS (Electronic Identification, Authentication and Trust Services) (European Union, 2014). Its objective is to allow citizens, businesses, and public administrations to securely identify themselves and access digital services across borders within the European Union (EU), using trusted IDs from each country. It allows a citizen to use their trusted digital identity from their home country to access public or private services in another EU country.

This ecosystem includes digital identifications based on the use of smart cards that employ a digital signature for identification, mobile identification applications, or identifiers combined with strong authentication systems. The first version of the eIDAS regulatory framework was published in 2016 and created a common scheme for the mutual recognition of digital identifications, regulations for trust services based on digital signatures, seals, and other elements.

At the end of 2024, eIDAS 2.0 was launched. While numerous technical regulations still need to be defined, it introduces and gives significant importance to the use of verifiable credentials in electronic wallets as a method for digital identification (European Commission, n.d.), also utilizing digital signatures. As will be discussed in Chapter 3, the European regulatory framework is moving towards favoring passwordless identification, where credentials are held by the user—for example, through smart cards or verifiable credentials on their mobile device—and identification is based on the use of a digital signature.

Currently, each country owns and manages its own digital identification system, and to facilitate interoperability within Europe, there is a "digital identity hub" (European Commission, n.d.), where citizens can select their country of origin, identify themselves through the corresponding national system, and navigate the various systems integrated into this European digital ecosystem.

In Latin America and the Caribbean, with the support of the Latin American and Caribbean Electronic Government Network (Red Gealc) (n.d.), the first pilot projects for integrating digital identification systems in the region began to be developed.

In 2023, the first integration between Uruguay and Argentina was achieved at the proof-of-concept level, currently in the testing phase. Uruguay has had an active digital identification ecosystem since 2018 with an identification broker called ID Uruguay, which connects four identification providers, three of them using digital signatures as a method for digital identification. Argentina, for its part, has a digital identification broker called Autenticar.

In October 2024, a new milestone was reached with the launch of the first cross-border integration in Latin America and the Caribbean between Uruguay and Brazil. On this occasion, ID Uruguay integrated with Gov.br, a Brazilian digital ID broker. Both brokers, in use for several years, were designed under the same standards and best practices, inspired by eIDAS and NIST best practices, making the integration very simple. As a result, Brazilian citizens can access more than 360 digital government services in Uruguay using their trusted Brazilian digital IDs, including all procedures related to foreign trade in Uruguay.

Experiences among the three countries have demonstrated that the digital ID broker is a fundamental component for enabling cross-border digital identification within each country's digital government "building blocks," thus ensuring the standardization of cross-border digital identification.

This co-creation process between the afore-mentioned countries not only enabled the first instance of cross-border digital identification but also allowed for the design and validation of a standard to promote cross-border digital identification throughout the region. In the cross-border context, having a broker offers strategic advantages in developing an interoperable national ecosystem:

- **Separation:** It allows for a clear distinction between the national and international ecosystems, facilitating the necessary data transformations and validations between countries.
- **Filtering:** It allows for the application of centralized trust criteria, ensuring that only identifications considered reliable by the countries involved are used at the cross-border level.
- **Gradual Implementation:** It allows for the progressive and controlled activation of cross-border digital identifications, enabling each country to activate this functionality according to the maturity level of its services and regulations.

Given this highly positive experience, during the first half of 2025, the Gealc Network, with support from the Inter-American Development Bank (IDB), the Organization of American States (OAS), the World Bank, and Co-Develop, allocated funding for the development of a model digital ID broker for the entire region. The goal is for this broker to be a digital public good, so that countries can implement it, generating an ecosystem of digital identification at the national level, but also creating the conditions to advance cross-border digital identification in Latin America and the Caribbean.

The model digital ID broker, aligned with the latest globally recognized standards and best practices in digital identification, will be a key component for standardizing digital identification across the continent, accelerating integration and adoption. It is expected to have a significant impact across the continent in sectors such as tourism, education, health, foreign trade, tax administration, and migration, among others.

Challenges for Tax Administrations

It is anticipated that, in the future, Latin America and the Caribbean will face challenges related to defining governance and building a hub of digital identity brokers, so that each broker in each country integrates into the hub only once and becomes part of the entire regional ecosystem. Using their own countries' digital identity systems to easily access digital services in other countries implies considerable time and cost savings in various sectors, while also strengthening trust and facilitating the use of digital tools.

Tax administrations have a key role in regional digital integration. In this regard, they have much to contribute, as there are concrete use cases in cross-border digital identity systems, facilitating access to digital services for natural persons and companies in other countries.

borders in a secure, simple, and reliable manner. At the same time, it allows them to leverage the full potential of the digital environment and actively contribute to strengthening regional integration and development.

Beyond being direct beneficiaries of these solutions, tax administrations can act as facilitators, fostering cooperation between countries and helping to build successful experiences, creating secure digital bridges for others to use and addressing the region's integration needs. This topic will be discussed in greater detail in Chapter 3.

2. Current Situation in Tax Administrations in Latin America and the Caribbean

This chapter presents an analysis of the current state of Digital Identification in the Tax Administrations of the Region. To gather information, one of the main methods was to conduct a survey using a structured form (available in Annex I) sent to each Tax Administration. The countries that submitted information were:

- Brazil
- Chile
- Costa Rica
- Ecuador
- Spain
- Guatemala
- Honduras
- Mexico
- Panama
- Peru
- Uruguay

Complementing the information gathered by the survey, research was conducted on digital government portals and tax administration websites to obtain further relevant information. The first section of this chapter presents a summary of the main examples of digital identification systems or ecosystems at the national level and their relationship with the Tax Administration. An analysis was carried out on different dimensions: systems or ecosystems at the national level, digital identification methods, and the relationship with tax administrations.

The following section analyzes the main challenges and difficulties for digitalization in tax administrations and the use of digital channels and their relationship with digital identification from the perspective of the administration's main services. Finally, at the end of this chapter, a summary of the current situation is presented, grouped into different levels or categories with respect to digital identification.

2.1. Tax Administrations and Digital Identification

The following table shows a summary of the main national digital identification initiatives and their relationship with the Tax Administration in some countries of the region.

Country	Initiatives for national digital identification systems or ecosystems and their relationship with tax administration
Argentina	The Secretariat of Innovation, Science and Technology manages the Autenticar platform, which acts as a digital ID broker, enabling a federated ecosystem with official digital ID providers using the OpenID Connect protocol. Autenticar is integrated with digital services so that users can select and use one of its identification providers across all integrated systems. This broker has six integrated official digital ID providers and several more under development (based on the use of digital signatures), including: • RENAPER: Argentina's National Registry of Persons, a state agency that identifies and documents natural persons and has the sole responsibility for issuing the National Identity Document (DNI) and Passport. Natural persons identify themselves online using their Automatic Number Identification (ANI) number and transaction number (printed on the card). It has biometric validation via selfie and liveness detection. This agency is also making progress on a physical document with a chip, with the possibility of signing and identifying oneself digitally. • **AFIP / ARCA: The Argentine Tax Administration is a digital identification provider in the national ecosystem. Users identify themselves with their tax ID number (CUIT) and validate their identity with a strong password.** • Mi Argentina: Users log in with their CUIL number and a strong password. They can validate their registration from the Mi Argentina app by taking a selfie and providing liveness detection. The mobile app also has a digital wallet with the national ID card and driver's license, in accordance with the ISO18013-5 standard. In its experimental phase, Argentina's digital identification ecosystem is advancing towards self-sovereign digital IDs on blockchain. Argentina is also progressing towards the implementation of a chip-based identity document with digital signing and identification capabilities.
Bolivia	The Agency for Electronic Government and Information and Communication Technologies (AGETIC) developed a national digital identification system consisting of the Digital Citizenship Registry and identification through that registry. Natural persons identify themselves through Digital Citizenship by entering their national identity card number and validating it with a strong password. The system also offers the option of identification via the Digital Citizenship App using a QR code with the same credentials. **The Integrated Tax Administration System (SIAT) has its own identification system (not integrated with Digital Citizenship) where users identify themselves using a Taxpayer Identification Number (NTI), Unique Taxpayer Registry (CUR), or National Identity Card and an email address, and validate their identity using a strong password.**

Country	Initiatives for national digital identification systems or ecosystems and their relationship with tax administration
Brazil	Brazil has a digital identification ecosystem with Gov.br as the broker of federated digital IDs. This ecosystem has been operating for several years with over 4,500 integrated digital services and more than 20 identification providers offering three security levels (bronze, silver, and gold). Beyond its scale, several features stand out. Seventeen public and private banks are identification providers on Gov.br, meaning that natural persons with a digital ID from one of these banks can use it to access integrated public services. Additionally, it includes identification providers that offer identification based on the use of digital signatures. This ecosystem also includes a mobile application with tools for biometric identity validation, using liveness detection verification, and can be used for authentication via QR codes on web systems. Furthermore, it is possible to use qualified signature-based methods for digital identification within the Gov.br ecosystem at the "gold" level. Brazil is currently conducting state-level pilot programs for the use of decentralized, self-sovereign digital IDs on a blockchain platform. **The Brazilian Tax Administration (Receita Federal or Internal Revenue Service) is integrated into Gov.br, so it is possible to use any of the digital identifications of the Gov.br ecosystem to access the Tax Administration's digital services.**
Chile	The Ministry of Finance, through the Digital Government Division, administers the Chilean Unique Key. It is a single provider of digital identification for the public sector and private companies that are authorized under agreement and meet the necessary standards. Natural persons identify themselves with their RUN (National Unique Registry Number), obtained from their National Identity Card, and verify their identity with a strong password. At the end of 2024, through a project to modernize the Civil Registry, Chile began issuing a national identity card that incorporates biometric features, complemented by an application that allows users to carry the document digitally, accessed via a QR code. **The Internal Revenue Service (SII) has its own digital identification system where taxpayers identify themselves with their RUT (Taxpayer Identification Number) and validate their identity with a strong password. Additionally, the SII is integrated with a Unique Key, making it possible to use it to access the Tax Administration.**
Colombia	The National Digital Agency developed the Digital Authentication platform, which is a single provider of digital identification for digital public services. Natural persons identify themselves using their national identification number and then verify their identity with a strong password. The National Civil Registry began issuing digital identification cards this year, stored in mobile document holders. This card can be used for digital identification, but it is not yet integrated into the Digital Authentication platform. **The National Directorate of Taxes and Customs (DIAN) has its own digital identification system (not integrated with Digital Authentication) where users can identify themselves with different document numbers (identity card, birth certificate, national identification card, etc.) and verify their identity with a strong password.**

Country	Initiatives for national digital identification systems or ecosystems and their relationship with tax administration
Costa Rica	The Supreme Electoral Tribunal recently launched the Costa Rican Digital Identity, which is obtained using the national identity card and managed through a mobile application (IDC-Ciudadano). Among other controls, this application verifies a person's identity using facial biometrics. This initiative is very recent, so the Central Bank of Costa Rica is developing a provider to enable this identification method for digital public services. **The General Directorate of Taxation is not integrated into the national digital identification system and, in principle, has no plans to do so (the system is still in its early stages). The General Directorate of Taxation has its own digital identification system; users identify themselves with their taxpayer identification number and validate their identity with a strong password. This system also has a two-factor authentication method that is mandatory for all users.**
Ecuador	Ecuador's Civil Registry has been issuing a national identity card since 2021 with a chip containing the citizen's biometric data and digital signature capabilities. Since 2023, the Civil Registry has offered an optional digital identity card, accessible through the Gob.ec app, which is equivalent to the physical card. Additionally, the Gob.ec portal and its app provide a single account for digital identification on government websites and online services. This account serves as a single point of identification for government portals and online services, where users log in with a username and validate their identity with a strong password. **The Internal Revenue Service (SRI) has its own digital identification system, and there are no plans to integrate it with Gob.ec soon. Taxpayers identify themselves with their RUC (Taxpayer Identification Number), national identity card, or passport. They can also enter an additional national identity card number (used to manage profiles) and validate their identity with a strong password.**
El Salvador	El Salvador has a system called Digital Identity, which serves as a single provider of digital identification for public digital services and acts as a Single Sign-On throughout its ecosystem. Natural persons can identify themselves with their DUI (National Identity Document) number, passport, or resident card. They validate their identity with a strong password. The National Registry of Natural persons has plans to develop a digital DUI. **The General Directorate of Internal Taxes (DGII) has its own digital identification system; natural persons identify themselves with their NIT (Tax Identification Number) or DUI number and validate their identity with a strong password.**

Country	Initiatives for national digital identification systems or ecosystems and their relationship with tax administration
Spain	Spain has a centralized provider for identification across all public digital services called Cl@ ve Móvil. Natural persons can obtain identification through this system via video call, in person, or using an electronic certificate (qualified signature). This system has a mobile application (optional but recommended) to facilitate identification using a QR code across all public services in the country. If the application is unavailable, identification can be obtained using the National Identity Document (DNI) or Foreigner's Identity Number (NIE) and validated with a strong password and a second authentication factor. Spain also has an electronic National Identity Document (DNIe), a physical identification card with a cryptographic chip that allows for digital signatures and identification. In addition, there are six qualified electronic service providers that issue certificates for identification on public digital services. **The Spanish Tax Agency is integrated with Cl@ve Móvil. Taxpayers can identify themselves by scanning the QR code with the app or by directly entering their National Identity Document (DNI) or Foreigner's Identity Number (NIE) on the portal. The Tax Agency also acts as a digital identification provider, enabling the creation and validation of identifications within this system. Additionally, the Tax Agency allows the use of electronic DNIs or digital certificates issued by qualified trusted electronic service providers for digital identification.**
Guatemala	Guatemala does not have a digital identification system or ecosystem in the public sector. Each portal and digital service has its own independent digital identification system. **The Superintendency of Tax Administration (SAT) has its own digital identification system. Natural persons identify themselves with their Tax Identification Number (NIT) or Unique Identification Code (CUI) and validate their identity with a strong password.**
Honduras	Honduras does not have a digital identification system or ecosystem in the public sector. Each portal and digital service has its own independent digital identification system. **The Tax Administration Service (SAR) has its own digital identification system. Users identify themselves with their RTN number and validate their identity with a strong password.**
Jamaica	Jamaica is developing the NIDS (National Identification System), which assigns a National Identification Number (NIN), registers biometric and biographical data, and issues a national identification card with a contactless chip containing the natural person's data, managed by the NIRA (National Identification and Registration Authority). This system will offer an online service for identity verification for public agencies and, for a fee, for private organizations to validate data against the national registry. **The Tax Administration has a separate digital identification system. Taxpayers identify themselves with a username and validate their identity with a strong password.**

Country	Initiatives for national digital identification systems or ecosystems and their relationship with tax administration
Mexico	Llave MX (Key MX) is a unique digital identification provider for accessing digital public services. It acts as a single sign-on between all integrated systems and uses Open ID Connect as its digital identification protocol. Users identify themselves with an email address or mobile phone number and validate their identity with a strong password. Currently, RENAPO (National Population and Identity Registry) is developing a project to evolve the national identification document (CURP, Unique Population Registry Code) into a physical and digital version, with its rollout planned for 2026. The INE (National Electoral Institute) Voter ID Card is a physical document widely used for in-person identification. It offers a web service to validate a person's identity after signing an agreement and meeting security requirements. **The SAT (Tax Administration Service) has its own digital identification system that operates in two modes (not integrated with Llave MX). Access is by password, where the user identifies themselves with an RFC (Federal Taxpayer Registry) number and validates their identity with a strong password, with the option of a second authentication factor. The other method is using a digital signature from the SAT (advanced electronic signature in Mexico), presenting the certificate issued by the SAT Certification Authority, the private key, and the password.**
Nicaragua	Nicaragua does not have a digital identification system or ecosystem in the public sector. Each portal and digital service has its own independent digital identification system. The Civil Registry and Identification Service (SRCEI) has an application called Digital Identification for carrying identification on a mobile device and a validator that works using QR codes, but its use is not intended for identification in digital services. **The General Directorate of Revenue (DGI) has its own digital identification system. Users identify themselves with a username and validate their identity with a strong password.**
Panama	The National Authority for Government Innovation (AIG) developed the Panama Digital portal, which evolved into Panama Conecta in 2025. As part of this solution, there is a Single Digital Identity system that allows access to certain digital public services. Currently, natural persons identify themselves with an email address, national identity card number, or passport number and validate their identity with a strong password. A second verification factor is optional. The Electoral Tribunal manages the national identity card and has announced plans to move towards a digital identity card, such as a credential on a mobile device. The digital driver's license was recently launched. **The General Directorate of Revenue has its own digital identification system. Taxpayers identify themselves with a username or Taxpayer Identification Number (RUC) and use a strong password (Tax Identification Number - NIT) to validate their identity.**

Country	Initiatives for national digital identification systems or ecosystems and their relationship with tax administration
Paraguay	The Ministry of Information and Communication Technologies (MITIC) developed an Electronic Identity system for digital identification in digital public services. Users identify themselves with their national identity card number and validate their identity with a strong password. Since 2023, the Identification Department has been issuing identity cards with chips, biometric and biographical records, and digital signature capabilities. With the chip-enabled card, users can create and validate their digital identity in MITIC's Electronic Identity system. **The National Directorate of Tax Revenue (DNIT) has some systems accessible through Electronic Identity and others with independent digital identification systems. Some systems allow identity validation using a photograph of the identity card, and in some cases, they use a qualified digital signature for identity validation.**
Peru	RENIEC (National Registry of Identification and Marital Status) is developing ID Peru with the goal of creating a single digital identification provider for digital public services. There are also plans to develop an electronic identity document that will interact with ID Peru. **The National Superintendency of Customs and Tax Administration (SUNAT) has its own digital identification system. Natural persons identify themselves with their National Identity Document (DNI) number, and companies with their Taxpayer Identification Number (RUC). In both cases, they validate their identification with a strong password. In the case of companies, in addition to the RUC, a username is required to distinguish roles within each taxpayer.**
Dominican Republic	The Dominican Government's Single Portal of Services is implementing an initiative to establish a unified digital identification provider for public digital services, called Cuenta Unica (Single Account). Natural persons register using their National Identity Document (DNI) number, among other data, and the system provides liveness detection verification solution to validate their account identity. They identify themselves with their DNI number and validate their identity with a strong password. Within the scope of the Central Electoral Board (JCE), which is responsible for issuing the National Identity and Electoral Card, progress is being made on an identity document with a chip, biometric and biographical registration, and the ability to digitally sign and identify oneself. **The Dominican Republic's Internal Revenue Service (DGII) has its own digital identification system. Natural persons identify themselves with their national identity card number, and companies with their tax identification number (RNC). They then validate their identity using a strong password and transaction code obtained from a digital token issued by the DGII.**

Country	Initiatives for national digital identification systems or ecosystems and their relationship with tax administration
Uruguay	The Agency for Electronic Government and the Information and Knowledge Society (AGESIC) manage the state's digital identification ecosystem. This platform consists of a digital identification broker called ID Uruguay, which has four digital identification providers that can be used for digital identification in most digital public procedures and services. One provider is usuario.gub.uy, managed by AGESIC, where natural persons identify themselves with their document number (national ID card or foreign passport) and validate their identity with a strong password. This system offers an optional second factor and provides basic (unvalidated identity) and intermediate (validated identity) security levels. The other three providers offer advanced-level identification (legally equivalent to in-person verification), based on the use of advanced electronic signatures within the framework of the National Public Key Infrastructure. One provider is a private company, and another is a public telecommunications company; both provide digital identification based on cloud-based signatures. The fourth provider is the National Directorate of Civil Identification, which since 2015 has been issuing an identity card with a chip that has the capacity to sign and identify oneself digitally. **The Uruguayan Tax Authority (DGI) is integrated into the ID Uruguay platform, making it possible to digitally identify oneself through any of the four digital identification providers within the ID Uruguay ecosystem. The DGI previously had its own digital identification system, where companies identified themselves with their RUT number (tax identification number), but a few years ago it decided to fully integrate with ID Uruguay and gradually deactivate its own digital identification system. To facilitate this, it developed an authorization system that allows natural persons, once identified, to fulfill specific roles within different companies.**
Venezuela	The Administrative Service for Identification, Migration and Foreigners (SAIME) have a centralized digital identification initiative for some procedures, primarily within its jurisdiction. While some digital services from other ministries and agencies have integrated it as a digital identification system, widespread adoption is not yet possible. Natural persons identify themselves with their national identity card number or email address and validate their identity with a strong password. Additionally, SAIME offers web services to validate a person's identity, primarily based on biometric data. Although there has not yet been a mass rollout, Venezuela has implemented the national identity card with a chip, containing biometric information and the ability to digitally sign and identify oneself. **The National Integrated Customs and Tax Administration Service (SENIAT) has its own digital identification system. Natural persons identify themselves with a username and validate their identity with a strong password.**

2.2 Main Findings

Below is a summary of the findings related to the topic, structured according to the different perspectives relevant to the analysis.

Digital Identification Systems or Ecosystems

Regarding national digital identification systems or ecosystems and their relationship with the Tax Administration, the following can be observed:

- **Digital identification ecosystems**: Some countries are consolidating a national digital identification ecosystem. This platform has more than one standardized digital identification provider and is integrated with digital public services, allowing natural persons to use any of these providers to identify themselves in the public sector: Argentina, Brazil, Spain, and Uruguay.

  In these cases, a digital identification broker is generally a critical component for standardizing and facilitating the integration of multiple digital identification providers with digital public services.

  Tax authorities act as a group of integrated digital public services, making it possible to access the tax administration using any of the digital identification providers in the ecosystem. In some cases, such as Uruguay, the DGI opted to gradually disable its own digital identification system, replacing it with the ID Uruguay ecosystem. In other cases, the Tax Administration enabled the ecosystem but also kept its original digital identification system in operation.

  In the case of Argentina, the Tax Administration also acts as a digital identification provider, so it is possible to use the Tax Administration's digital identification to identify oneself in other digital public services.

- **Digital identification systems:** Some countries are developing a centralized digital identification system, that is, a single provider integrated with various digital public services. Some tax administrations (for example, Chile) have integrated and offer their taxpayers the option of using their own tax administration identification or the single digital identification provider (Single Account). In other cases, the tax administration has not yet been integrated and therefore continues to use its own digital identification system exclusively.

- **Natural person digital identifications** for each digital public service or public organization. These cases do not have national systems or ecosystems; instead, each agency (or digital service) has its own digital identification system. In these cases, the Tax Administration has its own digital identification system.

Identification Methods

Regarding identification methods, the following details apply:

- In most cases, usernames are still used for identification and passwords for authentication. In a few cases, the optional use of a second authentication factor has been developed to strengthen identification.
- In some cases, biometric systems exist to validate a person's identity. These systems are generally based on a facial image, taken by the user's mobile device and compared with a public registry (ideally) or with a photo of their identity document provided by the user. This useful tool is sometimes used to validate a user's registration, rather than for identification purposes. It's important to note that very few countries have personal data protection laws, and even fewer have the tools to ensure that images are properly handled and not stored by third parties. In many countries in the region, regulatory gaps exist that could lead to many systems capturing images of people without oversight, and certainly without proper handling of that data.
- Some countries use more advanced and secure methods, such as decentralized identification based on the use of digital signatures within the context of a National Public Key Infrastructure. In this regard, there are different approaches:
    - National identity documents with chips, used as cryptographic devices, contain biographical and biometric data, as well as keys and a digital certificate for signing, issued by the civil identification authority, which also provides digital signature and identification services. The same physical identity document can be used in the digital world with complete confidence. While these methods offer higher levels of security, they present certain usability challenges. The user must have a smart card reader, that is, a device that allows them to insert the card and connect it to the computer. Furthermore, the installation of specific drivers and applications on the computer is required, which can create difficulties related to user privileges, the operating system, browsers, or other technical components. Another critical point is the limited compatibility with mobile devices. Although it is technically possible to develop mobile solutions, no implementations have yet been reported in the region.
    - Accredited digital signature and identification providers issue cryptographic devices—smart cards or tokens—which, although they are not national identity documents, have the same characteristics as those described in the previous point and are used for digital signatures or identification.

The Tax Administration's Perspective on National Digital Identification

- In countries that are advancing in a national digital identification ecosystem or system, the Tax Administration is often integrated as a group of digital services, so the digital identifications available in the ecosystem or system are enabled to access the Tax Administration. As systems or ecosystems expand, administrations will naturally become integrated, and it is likely that in the medium term, the specific digital identification of the tax administration will fall into disuse.
- In some countries, the Tax Administration has also become a provider of digital identification within the national system or ecosystem. Tax Administrations are organizations that possess a large database of verified users, which can be highly valuable to a national ecosystem or system. Therefore, it is a valid scenario for the Tax Administration to also be a provider of digital identification at the national level.
- In other cases, there is still no relationship between the Tax Administration and the digital identification system or ecosystem. This may be due to the absence of a national digital identity initiative, or to the fact that such an initiative is in its early stages, which has led the Tax Administration to not yet decide to integrate. It is expected that, as these systems become more established and expand, Tax Administrations will gradually integrate. This integration can occur, at a minimum, as a consumer of digital services, accessing them using ecosystem credentials; but also, as a national digital identity provider, actively contributing to strengthening the model.

2.3. Digitization and Digital Identification in Tax Administrations

Given that digital identity is a fundamental enabling component for the development of digitization processes in Tax Administrations, the survey explored the main challenges and problems these institutions face in implementing digital services.

Within this framework, the survey sought to identify the technical, regulatory, and operational barriers that limit the effective deployment of digital services in Tax Administrations, with the aim of generating comparative evidence to guide recommendations on digital identification, as well as differentiated roadmaps tailored to the various levels of digital maturity.

Main Challenges: Survey-Based Summary

The survey asked respondents to rank the following challenges according to their importance, based on the perception of each participating country:

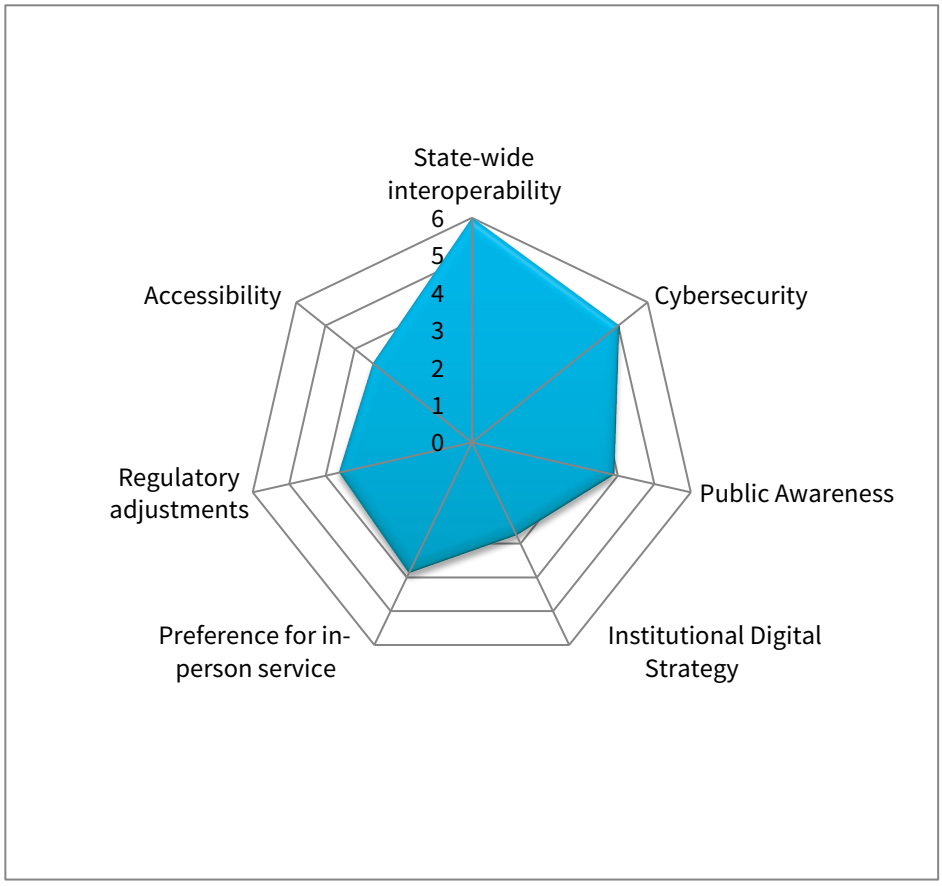
- Taxpayers prefer to visit offices in person
- Lack of a solid digital transformation strategy
- Adaptation of legal regulations to govern digital procedures
- Need to raise public awareness about the advantages of digital services
- Ensuring accessibility for people with disabilities or technological barriers
- Incorporating robust cybersecurity to protect taxpayer data
- Implementing interoperability between government systems
- Other

Eight countries responded in a structured manner to this part of the survey, enabling its systematic analysis. In most countries, interoperability between government systems appears to be one of the top three challenges. This suggests that state technological integration remains a major obstacle to advancing digital services for citizens. Cybersecurity also ranks as a high priority in more than half of the countries, reflecting a growing concern for the protection of personal data and institutional trust. Cultural resistance—manifested in a preference for in-person services and the need for public awareness—remains a significant obstacle.

In five countries, cybersecurity was ranked as the number one or two challenge, indicating that, in certain contexts, data protection is perceived as the primary operational risk. In these same countries, cultural challenges such as in-person service were relegated to lower positions, which could reflect a citizenry more familiar with digital channels.

To conclude the analysis, in most countries the digital transformation strategy consistently appears at the bottom of the ranking. This could indicate that, although recognized as important, it is not perceived as an immediate obstacle to operational implementation. Accessibility for people with disabilities or technological barriers also tends to rank low, representing an opportunity to strengthen the inclusive approach in service design.

Figure 4. Radar map of Challenges for the implementation of digital services - average.



Source: Prepared by the author based on a survey of 8 countries.

Main Problems: Summary Based on Survey Results

The survey asked respondents to rank the following problems according to their importance, based on the perception of each participating country:

- Connectivity problems in the country
- Limited access to digital devices for taxpayers
- Lack of digital skills among the population

- Services with poor user experience
- Lack of IT staff
- Inadequate budget
- Legal problems due to uncertainty about whether the taxpayer is carrying out the procedure
- Other

Eight countries responded in a structured manner to this part of the survey, enabling its systematic analysis. In most countries, the lack of adequate budgeting appears as a priority barrier, ranking first. This situation reflects that, in various contexts, digital transformation still competes with other institutional priorities, limiting investment in scalable and secure solutions.

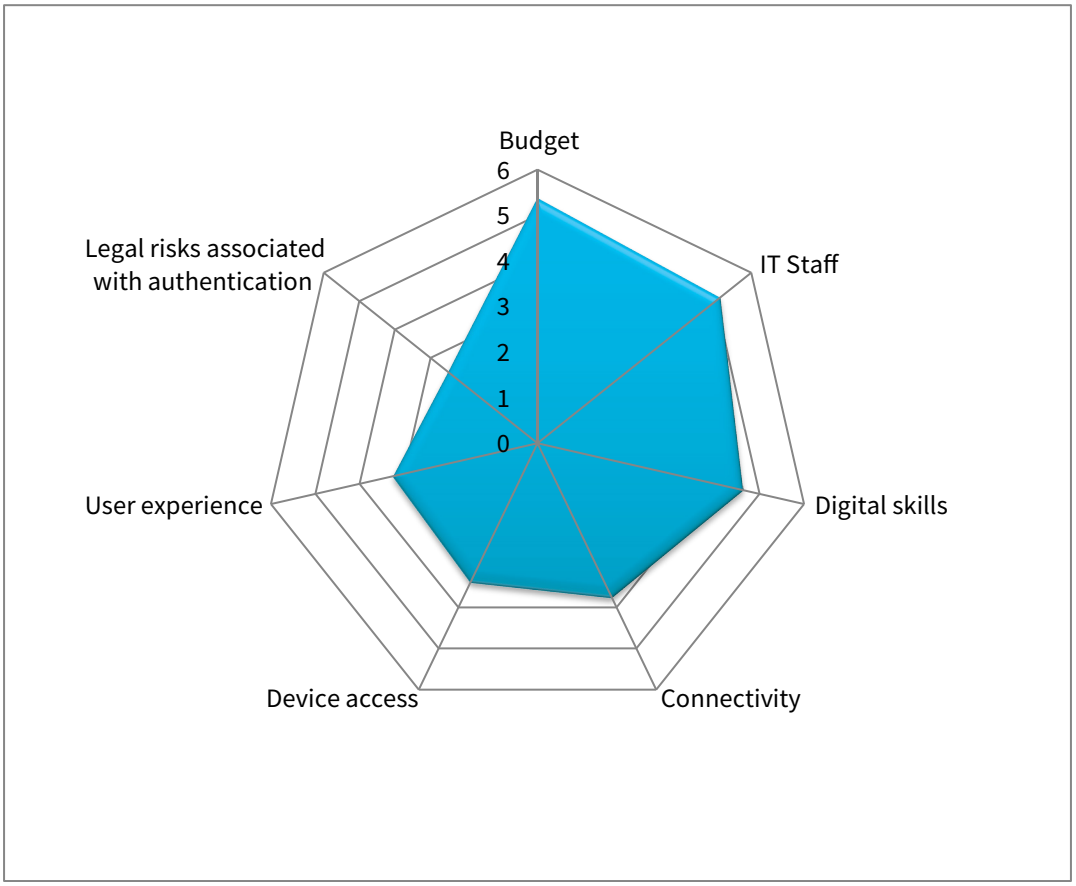
Similarly, the lack of specialized IT personnel is among the top three challenges for six countries. This suggests that, beyond technological infrastructure, human capabilities constitute a critical constraint for the deployment of digital tax services. The shortage of technical professionals can affect operational sustainability, system security, and regulatory compliance.

On the contrary, barriers related to user experience and connectivity tend to rank lower, suggesting that, while relevant, they are not perceived as the main immediate obstacles. This could indicate that progress has already been made in infrastructure and service design in several countries, although challenges in digital inclusion remain.

Although legal issues related to taxpayer authentication do not appear as the main challenge in any country, they do represent a moderate barrier in some contexts. In most cases, this issue ranks low, suggesting that it is not perceived as an immediate obstacle. This perception could be linked, on the one hand, to the existence of regulatory frameworks that recognize the legal equivalence between digital and physical identity; on the other hand, to a lower institutional prioritization of the regulatory risk associated with authentication.

Finally, limited access to devices and the population's digital skills shows a mixed distribution: in some countries they are a priority, while in others they are relegated. This variability suggests that roadmaps should consider differentiated approaches, combining strategies for raising public awareness, providing access means, and strengthening digital capacities.

Figure 5. Radar map of problems for the implementation of digital services - average.



***Source*:** Prepared by the author based on a survey of 8 countries.

Digital Identification in Tax Administrations

The following table presents a summary of the digital identification methods used by each Tax Administration in each country, based on the survey.

References:

- Country
- National ID:
  - No: The Tax Administration is not integrated into a national identification system.

- Optional: The Tax Administration is integrated into a national identification system. Taxpayers can use either the Tax Administration's ID or the national ID, optionally.
- Mandatory: The Tax Administration is integrated into a national identification system, and its use is mandatory.
- Tax Administration is a Provider of Digital Identification: In these cases, the Tax Administration is also a provider of digital identification within the national system or ecosystem.

- User:
  - PF: Natural person
  - NIF: Tax Identification Number
  - Both
- Strong Password: There is a policy that guarantees the use of strong passwords.
- Two-Factor Authentication (2FA):
  - No: There is no option to use a two-factor authentication.
  - Optional: It is available and optional.
  - Mandatory: all access requires two-factor authentication.

Country	National ID	Username	Strong Password	Second-factor authentication
Brazil	Mandatory	PF	Yes, for everyone	Yes, mandatory for some sectors
Chile	Optional	Both	Yes, for everyone	No
Costa Rica	No	NIF	Yes, for everyone	Yes, mandatory for everyone
Ecuador	No	NIF	Yes, for everyone	Yes, mandatory for some sectors
Spain	Mandatory AT is IdP	Both	Yes, for everyone	Yes, mandatory for everyone
Guatemala	No	NIF	Yes, for everyone	Optional for everyone
Honduras	No	NIF	Yes, for everyone	No
Mexico	No	PF	Yes, for everyone	Optional for everyone
Panama	No	NIF	Yes, for everyone	No
Peru	No	NIF	Yes, for everyone	Yes, mandatory for registration
Uruguay	Mandatory for PF	Both	Yes, for PF	Yes, mandatory for PF

Main tax administration services: their use through digital channels and links to digital identification.

The following table shows the services analyzed.

Service	Description
Registration in the tax system	Formal inlegal entity of the taxpayer (natural person or legal entity) into the tax system through the assignment of a tax identification number and the definition of their obligations.
Filing tax returns	Submission of tax information by the taxpayer, detailing income, expenses, calculated taxes, and other data required by current regulations.
Pre-filled tax returns	Tax forms that include information pre-filled by the tax authorities, based on available data, to facilitate filing by the taxpayer.
Payment of tax obligations	Fulfillment of tax obligations through the payment of taxes, fines, or surcharges, using methods authorized by the tax authorities.
Processing of certificates and/or records	Request for issuance of official documents that certify specific tax situations, such as registration, compliance with obligations, or absence of debt.
Payment Agreement Processing	Management of agreements between taxpayers and the administration for payment in installments or deferred payment of tax obligations.
Applications for tax credits or benefits	Submission of requests to access deductions, exemptions, refunds, or other incentives provided for in tax regulations.
Submission of appeals and/or petitions	Formal channel for taxpayers to exercise their right to defense, submit observations, or request specific actions from the tax administration.
Communications and/or notifications	Sending and receiving administrative documents, notices, requests, or other official communications between the administration and the taxpayer.
Sending or uploading information	Transmission of data or documentation required by the tax authorities.
Inquiry about current account/ statement of financial position	Access to up-to-date information of tax obligations, payments made, outstanding balances, and other transactions recorded in the taxpayer's tax account.
Binding inquiries	Formal requests for interpretation of tax regulations, whose response by the administration has legal effects for the applicant.
General inquiries	Non-binding requests for information regarding procedures, regulations, or services offered by the tax administration.
Scheduling an in-person appointment at the office	Requesting an appointment for personalized service at the administration's offices.
Dispute resolution	Administrative or jurisdictional mechanisms available to resolve disagreements between the taxpayer and the administration regarding tax matters.

The digital channels considered were:

- Web: Tax Administration website, accessible via browser.
- Mobile: Tax Administration mobile application.
- API: Interoperability between the Tax Administration systems and another system where the taxpayer performs the service (for example: another public agency, banks, etc.).
- Email: The taxpayer interacts with the tax administration by sending and receiving emails.
- Messaging (SMS, WhatsApp, or similar): The taxpayer interacts with the tax administration by sending and receiving these types of messages.
- Social media: The taxpayer interacts with the tax administration through social media.

In all cases, it is assumed that in-person channels may also exist. The web channel is the most widely used and is available for all services with some exceptions. Secondly, the mobile channel is prominent, but it is available for services that require less information and are simpler, through the Tax Administration's mobile applications. Unlike the web channel, not all services can be accessed via the mobile channel, and most Tax Administrations lack mobile applications.

Thirdly, there are two distinct channels: **API**, which is more popular for payments, sending or uploading information, or filing returns, and **email**, which is more geared towards communications, services such as processing certificates, communication, and notifications.

In some tax administrations, certain services still lack digital channels and can only be accessed in person. Very few utilize innovative digital channels such as **chat** and **video calls** for some services, where an official assists the taxpayer. The use of **social media** as a means for taxpayers to interact with the tax administration is almost nonexistent.

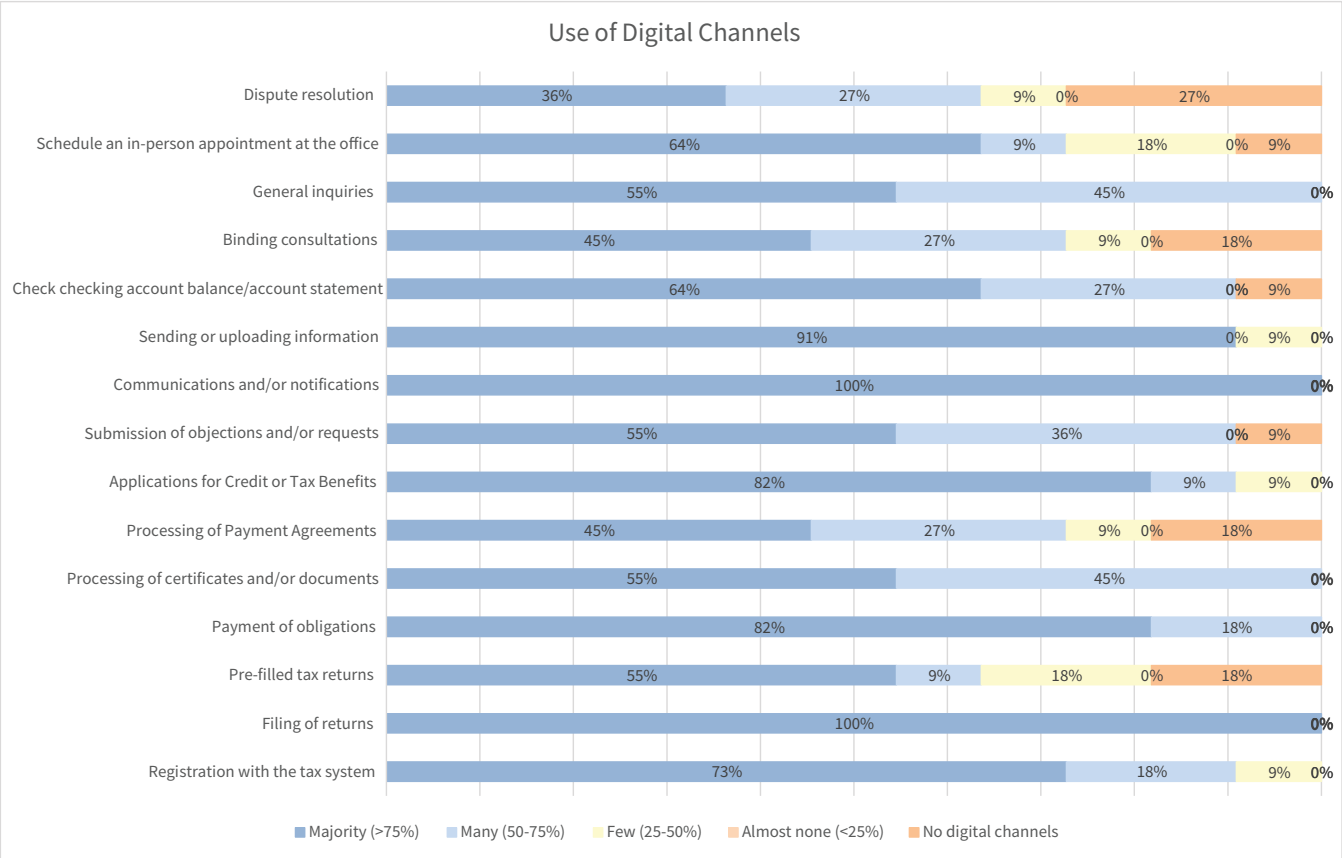
Only one country reported having a developed multichannel model. This country has a strategy that includes consistent interaction with taxpayers through web, mobile, telephone, video assistance, and in-person channels, aiming to provide a seamless experience regardless of the channel.

Regarding the use of digital channels, the following scale was used:

1. No digital channels available
2. Almost nothing is done through digital channels – less than 25%
3. Little is done through digital channels – between 25% and 50%
4. A lot is done through digital channels – between 50% and 75%
5. Most is done through digital channels – more than 75%

The following image shows the average usage of digital channels for each service:

Figure 6. Use of digital channels.



Source: Prepared by the author based on a survey of 8 countries.

Although, on average, the “Majority (>75%)” option in digital format predominates in all services, there are still cases where there are no channels or they are used very little. Analyzing these latter cases, the main contributing factors are that the IT systems either don’t allow it or have considerable limitations. The most significant reasons cited by countries with lower digital channel usage were lack of budget, lack of capacity, and insufficient regulatory provisions to enable and build trust in digital channels.

In general, assuming that “most” or “many” represents high use of digital channels and “few,” “almost none,” or “no digital channels” represents low use, the most digitized services are: General inquiries, Current account/statement of position inquiries, Sending or uploading information, Communications and/or notifications, Filing appeals and/or requests, Applications for credit or tax benefits, Processing of certificates and/or attestations, Registration in the tax system, Payment of obligations, and Filing of tax returns. In these last two cases, most inquiries are carried out through digital channels, which demonstrate a high level of technological adoption in compliance with these two fundamental tax obligations.

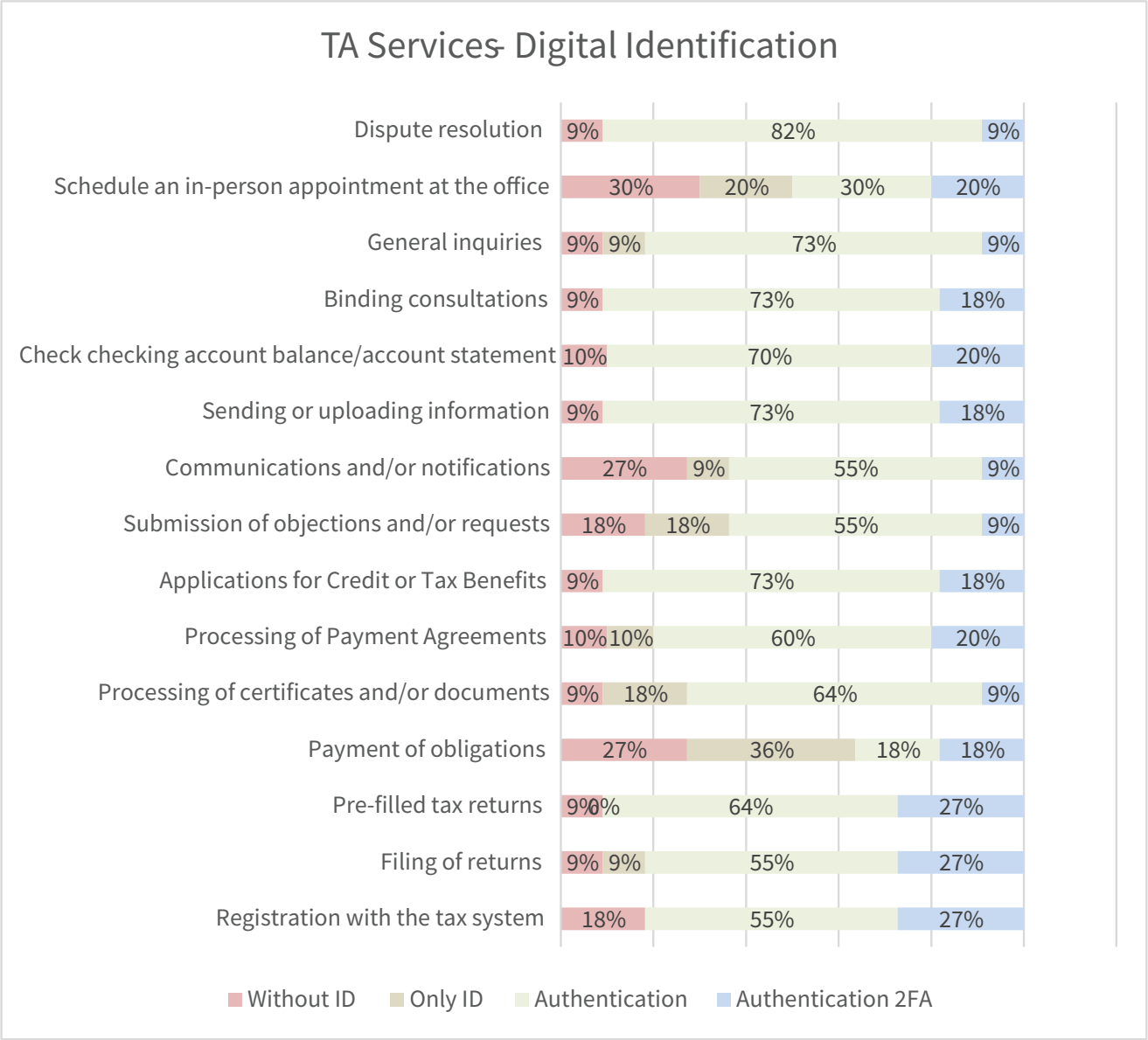
On the other hand, the least digitized services are: Dispute resolution, Payment agreement processing, and Pre-filled returns. The low digitization of the first two is probably because the digital channel does not yet offer the fluidity or reliability necessary to address complex situations related to tax noncompliance, where personalized interaction, document analysis, and discussions of regulatory interpretations may be required. As for pre-filled returns, the absence of a digital channel could indicate that the service has not yet been implemented, since a pre-filled tax return proposal is inherently digital.

To analyze the relationship between each service and identification, we determined whether the service requires digital identification to be performed, using the following scale:

1. No digital identification is required
2. Only the taxpayer identification number is required
3. Authentication is required
4. In addition to authentication, a second authentication factor is required

The following image shows, for each service, the average percentage of each type of digital identification (no ID, ID only, authentication, and 2FA).

Figure 7. Type of digital identification for different services - average.



Source: Prepared by the author based on a survey of 11 countries.

Firstly, it can be concluded that there is varied use of digital identification, beyond whether it is digital identification or specific to the Tax Administration. This is because not all services necessarily require digital identification; only one Tax Administration among those surveyed uses digital identification for all services. As defined in Chapter 1, when we talk about Digital Identification, we are referring to authentication; that is, the user identifies themselves and then validates their identification. Both steps are necessary in the digital world.

This distinction is important because in almost all Tax Administrations, many services only require a taxpayer identifier (taxpayer number), without identity verification. While in many cases this may not be a problem, it can be used by cybercriminals for social intelligence purposes—that is, to discover seemingly "harmless" information about natural persons or taxpayers that can be exploited for fraud or cyberattacks.

Regarding the strength of digital identification, few cases use more secure methods based on digital signatures (this topic will be addressed in more detail in Chapter 3), but these methods are not mutually exclusive, so users can log in with traditional methods based on the username-password combination. Only one Tax Administration requires a second authentication factor for all services, and four Tax Administrations require a second authentication factor for some services.

The two graphs above show that, although there is a high degree of digital channel usage on average, there are also various uses. This highlights certain weaknesses in adopting a "digital by default" approach, which should incorporate strategies aimed at:

- **Multichannel:** Strengthening the relationship between the Tax Administration and taxpayers through a multichannel approach. This means that all channels are integrated, ensuring taxpayers experience the same level of service and quality regardless of the channel they use. It also means being able to start a process on one channel and continue it from the same point in another.
- **Digital Identification:** In most cases, different criteria are required for Tax Administration services. Some services do not include any identifier at all, others require only an identifier, others require digital identification, and in some cases, more robust digital identification.

2.4. Current State of Digital Identification in the Region's Tax Administrations

The regional review allowed for a more precise identification of the obstacles faced by Tax Administrations in adopting digital services, particularly regarding the design, implementation, and management of digital identity systems. The results reveal a diversity of institutional maturity levels, technical capabilities, and regulatory frameworks, which poses specific challenges in terms of interoperability, security, inclusion, and governance.

This comparative analysis provides a basis for guiding differentiated recommendations and promoting a more coherent and sustainable adoption of digital identity in the region in the next chapter, laying the enabling conditions for future regional integration.

While different realities exist, the Tax Administration's approach to digital development is embedded within the specific circumstances of each country. Although in some countries the Tax Administration is among the most digitally mature agencies, in all cases it is highly dependent on the overall national context. The digital gap at the national level impacts the use and utilization of the Tax Administration's digital channels.

For the Tax Administration to integrate into a national digital identification system or ecosystem, such a system or ecosystem must first exist. This requires sustained public policies, a robust legal framework, effective governance, and effective coordination among the various stakeholders—where the Tax Administration plays a strategic role. Furthermore, a thriving digital ecosystem is needed, one that fosters synergies between the public and private sectors, academia, and civil society.

In short, the country's digital development has a direct positive or negative influence on the digital development of the Tax Administration and, therefore, its digital services are positively or negatively influenced depending on the overall context.

Regarding "Authorization," there are also varying levels of maturity. Tax Administrations that are part of a national digital identification ecosystem or system have developed different solutions for access control or Authorization, adapting to an environment where users—already digitally identified—interact with multiple online services. This evolution has required Tax Administrations to address role management, given that they must link natural persons with companies or taxpayers and assign them different profiles according to their functions, responsibilities, or legal relationships. In this respect, there are different levels of progress and criteria in the cases analyzed; some have a superficial role management system, others a slightly more in-depth one, but in almost no case is there a comprehensive role management system aligned with proper data governance.

Tax administrations that are not yet integrated into a national digital identification system or ecosystem still manage authentication and authorization in a nearly unidirectional manner. This means that taxpayers are identified by a tax identifier and, in most cases, have very few roles or even a single role that does not distinguish between processes, functions, or data.

In a world where a clear trend is moving toward national or universal digital identification, tax administration depends on public policies and the development of digital government in each country. However, they must rethink and standardize authorization under a modern role management system, considering at least three levels: functionalities, objects, and data, to prepare themselves to be part of a universal digital identification system. This topic will be addressed in greater detail in the next chapter.

Among other relevant sources, the report Tax Administration Digitalization and Digital Transformation Initiatives published by the OECD in June 2025 (OECD, 2025) offers updated statistics on the state of digital identification in Tax Administrations.

3. Implementation Guide and Roadmap

3.1. Trends in Digital Identification

Best Practices in Digital Identification

Before discussing trends, we highlight some characteristics of standards and best practices that began to emerge a few years ago in digital identification:

- **Avoid using passwords:** While password policies are necessary, their application is often difficult for users to manage. Some modern identification methods avoid using passwords, as they understand that they are no longer reliable and greatly hinder the use of digital IDs. Various techniques and malware currently exist that make passwords vulnerable, even when policies are followed.
- **Biometrics:** The high adoption rate of mobile devices, as well as their extensive capabilities, allows for the efficient use of certain functionalities to strengthen digital identification. The use of the camera, fingerprint reader, and geolocation are features that the device can contribute to strengthening digital identification.
- **User credential custody:** Having a centralized database with millions of user credentials, even if encrypted, represents a considerable risk. The new models are geared towards ensuring that credentials are no longer stored in centralized computer systems, but rather in the user's possession, on cryptographic devices (smart cards, tokens, mobile devices, etc.). This distribution significantly reduces the risks associated with mass credential theft.
- **Use of public-key cryptography methods:** the use of robust cryptographic mechanisms is promoted, especially those based on public keys, particularly digital signatures. In the CIAT publication, "ICT as a Strategic Tool to Enhance the Efficiency of Tax Administrations" (CIAT, 2020), Chapter 10 addresses the topics of asymmetric encryption, digital signatures, and digital identity certificates in greater detail. The challenge in these cases is usability: reducing barriers to make them easy for everyone to use.
- **Greater privacy protection:** With IDs entirely under the user's control, it is not easy to track where the user uses them, or at least not easy from the identification systems; some browsers and web crawlers may have this objective.
- **Scalability and ease of use:** these new methods are designed to scale and, in turn, offer a simpler and more accessible user experience for users and citizens.

Many of the concepts mentioned above have been promoted by the Fast Identity Online (FIDO) Alliance, in conjunction with the World Wide Web Consortium (W3C), through the development of a new open standard for strong, passwordless authentication called FIDO2. FIDO2 combines a W3C standard for authentication based on public-key cryptography (digital signatures) with external devices, such as USB drives, mobile devices, biometric readers, etc., that communicate with a browser without requiring passwords. This allows a user to use an external device, under their custody, to present their credentials, based on the use of a digital signature to identify themselves digitally in a computer system.

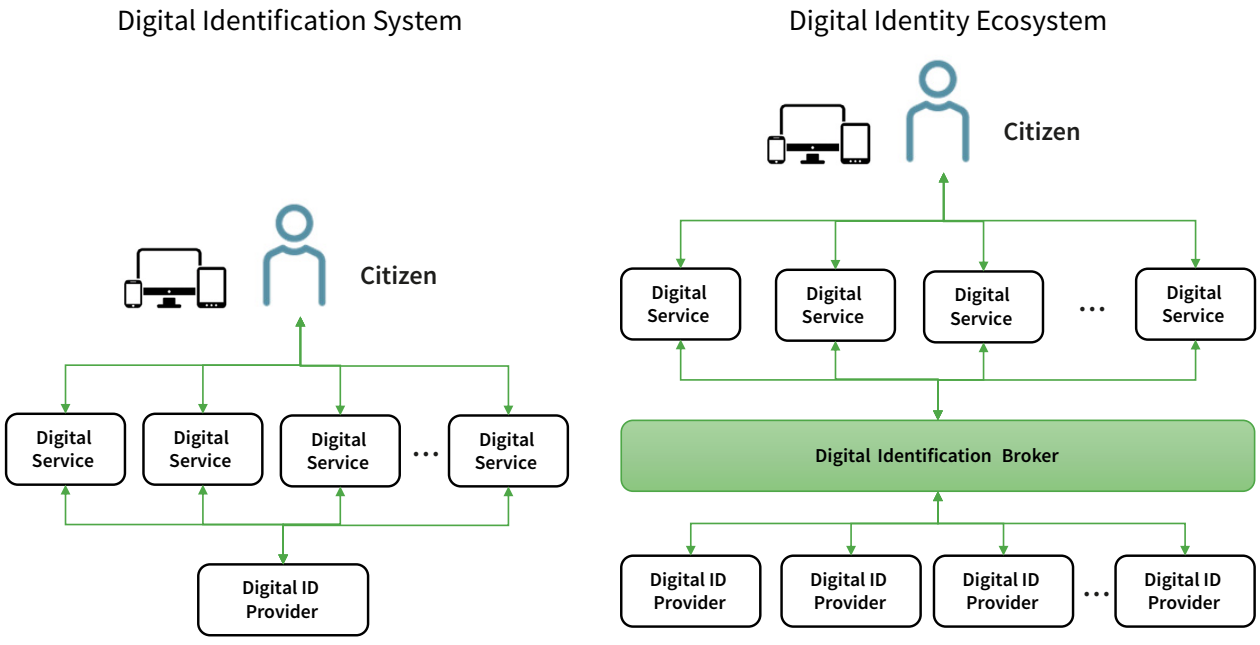
The main trends in four key areas are explored below.

Use of Digital IDs

For some years now, the use of digital IDs has been behaving much like physical IDs have for many decades. People obtain an ID from an accredited and trusted organization and use it in multiple places, as discussed in Chapter 1.

This situation leads to the need to develop systems or ecosystems at the national level so that accredited digital ID providers are available for use across different digital services. The following image compares a simplified model between a system (one provider) and an ecosystem (multiple providers with a digital ID broker as an intermediary):

Figure 8. Comparative scheme between a system (one provider) and an ecosystem.



Source: Prepared by the author

Chapter 1 highlights some advantages of the ecosystem and the broker as a key component. The following chapter outlines some challenges that must be addressed for the implementation of a system or ecosystem at a national level:

- **Protection of information privacy:** ensuring, at a minimum, compliance with regulations. Consider a minimal set of information to be exchanged for everyone (identification provider – broker – digital service). If the integrated IT system subsequently requires more information, it must resolve this situation—with the user's prior consent—by interoperating with other systems.
- **Broker regulation:** Regulating the existence and operation of brokers would not only allow for their validation and formalization but could also constitute a key strategy for consolidating a national digital identification ecosystem, with participation from both the public and private sectors. A broker in the public sector could be a solution for everyone to identify themselves with a provider across the entire public sector. However, integrating the entire private sector into the same broker as the public sector would generate considerable additional costs for the public sector and a high level of risk by centralizing all the country's digital identification in a single piece of software. Regulating brokers can be a strategy to enable the development of new brokers with the same standards, criteria, and identification providers in the country. This would benefit natural persons by allowing them to use the same identifications nationwide, reducing costs and risks. In some countries, after several years of discussion, this conclusion is being reached.
- **Technical intermediation:** In a national digital identification ecosystem, the broker can be compared to how a payment gateway works. A payment gateway is a piece of software that acts as an intermediary between an online store and electronic payment providers. The gateway integrates various payment methods (banks, credit cards, e-wallets, etc.) and is integrated as a service only once for each store. This way, each store performs a single integration and offers its users the payment methods incorporated into the gateway. Like a broker, the gateway must comply with certain regulations, implement specific standards and security controls, among other requirements.

Main Protocols for Federated Systems and Ecosystems

With the emergence of federated digital identification systems, large credential aggregators—such as Google, Microsoft, and Apple, among others—began to position themselves as identification providers. In addition, several specific protocols were developed for this type of use, which are described below:

- **SAML 2.0 (Security Assertion Markup Language):** This is an open standard for authentication and authorization based on XML that allows the secure implementation of a Single Sign-On system between different systems and identification providers. It is based on the exchange of messages called

"assertions," which are digitally signed XML documents containing information about the user's identity. By validating the signature of the XML documents, all systems can trust the information they contain, i.e., the user's identity. It uses signatures on XML files and X.509 certificates.

- **Open ID Connect (OIDC):** This is an authentication protocol developed from OAuth 2.0 (authorization protocol), extending it for authentication. Like SAML, but it uses JSON tokens (JWT), which are lighter formats. This protocol is considered simpler and more modern than SAML and is currently the most widely used for these purposes.
- **Open ID Connect for Verifiable Credentials (OIDC4VC):** This is an extension of the OpenID Connect standard, designed to bring traditional federated authentication to the world of decentralized digital identity or verifiable credentials (this topic is discussed in section 3.2). OIDC4VC allows the use of a credential on a mobile device, for example, a digital ID card or national identity document in a wallet—to digitally identify oneself to a digital service (web or mobile). This standard has two complementary specifications:
  - Open ID Connect for Verifiable Credential Issuance (OIDC4CI): establishes the protocol by which an issuer—such as a national identification authority—can issue a verifiable credential (e.g., an identity document or national ID card) and transfer it directly to the user's digital wallet on their mobile device.
  - Open ID Connect for Verifiable Presentations (OIDC4VP): defines how the owner (person) presents a credential (e.g., a national ID card or national ID card in their digital wallet) to an identification provider within an OIDC-enabled digital ID system or ecosystem.

JSON (JavaScript Object Notation), like XML (eXtensible Markup Language), defined by the World Wide Web Consortium (W3C), is a text format designed to store and exchange structured data, but much lighter. It is widely used in web applications, mobile applications, and APIs because it is easy for humans to read and easy for machines to process. XML uses tags to define the data structure (like HTML) and is more "descriptive," while JSON has a much more compact and readable syntax.

Security and Trust Based on Digital Signatures

The model based on an identifier/validator combination, which has been reinforced in various ways over the last few decades, is no longer sustainable. No matter how strong the password and the number of factors, which makes it increasingly complex and expensive, it remains vulnerable. While a strong password and at least two correctly implemented factors are still considered strong today, its obsolescence is imminent.

This model relies on a centralized database where passwords are encrypted, specifically using mathematical hash functions. However, attack techniques exist that allow these credentials to be compromised without directly attacking the hash algorithm. Examples include rainbow table attacks, which use pre-computed hash dictionaries to perform massive comparisons, and malware that capture passwords before they are encrypted. Social engineering vectors, which exploit human vulnerability, also pose a significant risk. Maintaining a centralized database of millions of credentials inherently presents a considerable risk.

Trends indicate that digital identification methods based on digital signatures, where the keys and certificate are decentralized and held by the owner, will be increasingly used. This would give parties much greater confidence when identifying themselves digitally.

Another way of looking at it would be as follows: Digital signatures (depending on the country, they may be called advanced, qualified, certified, etc.) have two properties:

1. Mathematical verification of the integrity of the signed document.
2. Non-repudiation, meaning that the person who signed the document cannot deny it, which can also be considered a reliable way to verify the signer's identity.

These two properties, based on the use of asymmetric cryptography and hash functions within the context of a Public Key Infrastructure, allow the use of digital signatures as a fully reliable method of digital identification. When a user signs a document, the document is sent to the server, and the server validates the digital signature. This process guarantees the integrity of the content, ensuring that it has not been altered during transmission, and the principle of non-repudiation, which confirms the signer's identity and prevents them from denying their participation in the transaction. This system, implemented in a user-friendly way and with the correct regulations, generates various ways to use digital signatures for digital identification. At the end of this section, after consolidating these trends, we will examine some modern methods of digital identification based on the use of digital signatures.

A person's digital signature on a document is done in two steps:

1. The document's hash is calculated: this function generates a unique code for a document (called a hash) and has two properties:
    a. It is irreversible: given the hash, there is no inverse function that generates the original document.
    b. It is unique: if even a single character is changed in the document, the new hash will be different from the previous one.

2. The hash of the signed document is encrypted with the signer's private key. In this case, asymmetric or public-key cryptography is used. In asymmetric cryptography, each entity possesses a public key, which can be known to everyone, and a private (confidential) key, which is mathematically linked. What is encrypted with one can only be decrypted with the other. When a document is encrypted with the private key and a third party using its "public pair" decrypts it, it can be confirmed that the encryption was performed with the "private pair" corresponding to the public key used.

   A digital signature is obtained by encrypting a document's hash using a person's private key. This securely links that person to the document that generated the hash.

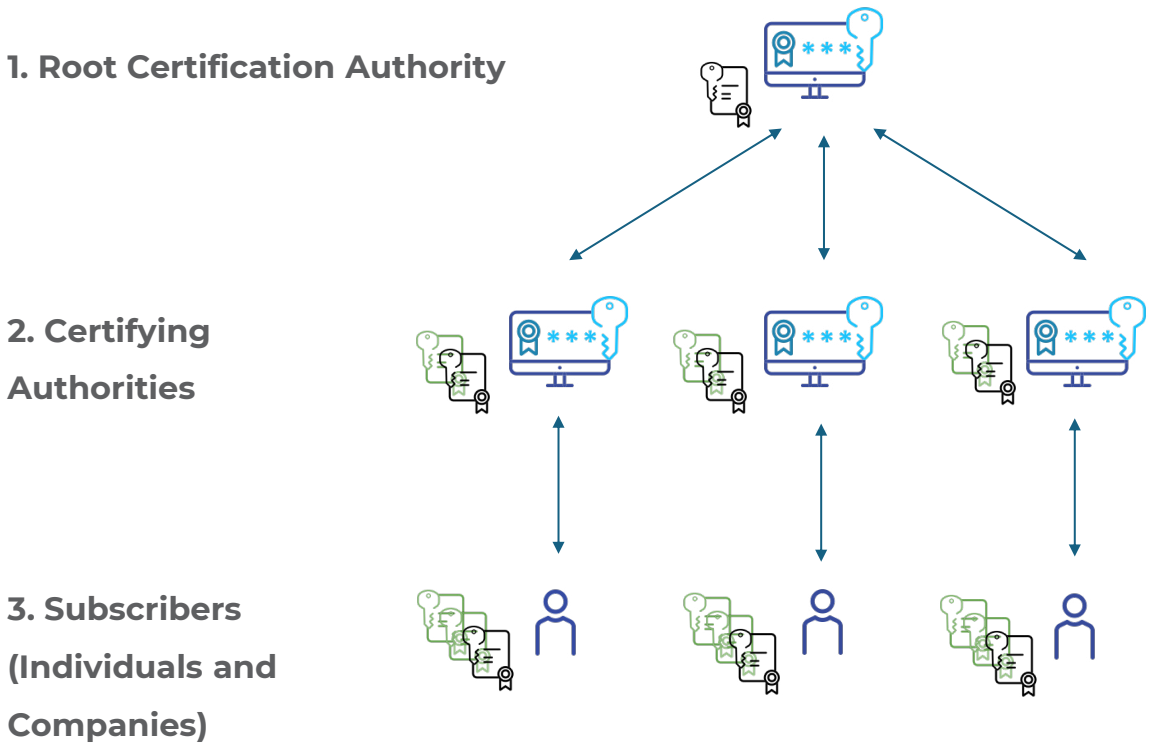
   When a signature is advanced, qualified, or certified (depending on the country), it means that a verification process of the signer's identity was carried out by a Certification Authority. Modern regulations in most countries in the region require two relevant characteristics with respect to the keys granted to the person:

   - **Private key:** must reside on a cryptographic device and never leave it. Furthermore, the device must be protected with at least a PIN or password. A cryptographic device can be a token, a smart card (often also used as a national identification document), a mobile device, or an HSM (Hardware Security Module), which is a physical device specifically designed to protect, manage, and execute cryptographic operations.
   - P**ublic key:** must be in a digital certificate in X.509 format. This is a standardized electronic document used to securely link an identity (person, company, or server) with a public key. This certificate is issued and signed by the certification authority. The certification authority's signature protects the integrity of the certificate and validates it, as it demonstrates that it was issued by an authorized certification authority.

The two points above are critical because they ensure that a signed document guarantees that the private key used never left a cryptographic device and, if the signature is validated, that the public key used is linked to a specific person, as specified in the corresponding digital certificate. The Certification Authority that issued and signed the certificate provides this assurance.

A Public Key Infrastructure (PKI) is a set of technologies, policies, entities, and procedures that enable the secure and reliable issuance, management, distribution, and revocation of digital certificates and cryptographic keys. It is a hierarchical, tree-like structure that can have several levels. While there is often a root level, it is not strictly necessary. The following diagram illustrates an example of a three-level PKI:

Figure 9. Three-level PKI scheme.



Source: Prepared by the author

The “parent” Certification Authorities sign the certificates of the “child” Certification Authorities once they are recognized by the regulations, and so on. Natural persons obtain their keys and certificates from an authorized Certification Authority, keeping the private key in their possession, which is usually stored securely in a cryptographic device.

Each higher-level signs the certificate of the next lower level, thus creating what is known as a chain of trust. The certificate containing a person’s identity and public key is the final link in a chain of trust that ensures the integrity and identity of each link by mathematically validating the signatures.

A country’s trusted list for advanced (qualified or certified) electronic signatures is the list of all certificates issued by all its Certification Authorities authorized under the country’s regulations. This trusted list is a key element for validating a person’s signature on a document and allows for determining when a signature is considered advanced, thus guaranteeing the signer’s identity.

Certificates can be revoked if a private key is no longer trusted, for example, when someone loses their cryptographic device. Each Certificate Authority maintains a revocation list of the certificates it has revoked. This is another key element for validating a signature: a signature is valid if the certificate used to verify it has not been revoked or if the signature was created before its revocation date.

Chapter 10 of the CIAT publication "ICTs as a Strategic Tool to Enhance the Efficiency of Tax Administrations" (CIAT, 2020) delves into aspects related to trust in digital signatures and the role of Public Key Infrastructures (PKI).

In short, digital signatures can be used as a form of digital identification and are a highly reliable method; this trust is provided by the Public Key Infrastructure that underpins the digital signature.

Technologies

Biometric Methods

In the first chapter, biometric methods, primarily facial and fingerprint, were discussed. These methods are being widely used given the widespread adoption of smartphones and their ease of use. While biometric tools for identity verification have reached a very high level of maturity, there are two issues to consider regarding facial biometrics to ensure their reliability:

1. Before taking the photo, a recognized liveness detection verification system must be used to ensure that the photograph taken by the user is of a living person—and not, for example, a photograph of a person. Several recognized systems are available on the market with very good success rates. There are also standards and certifications that guarantee certain levels of reliability, but these come at a significant cost. This ensures that the photograph is taken of a living person; without this tool, these systems are not as secure.

2. The facial image taken of the person should be compared with the public registry and not depend on the document uploaded by the person to the application, as this would compromise security. For this to work, the public registry must have this capability developed. In this case, it is essential that the image be received directly by the public registry and that the biometric comparison be performed within its own systems. This approach guarantees that the image is not transferred to third parties, thus preserving the privacy of the data subject. In many cases, this comparison is made with a document provided by the user and not against the public registry, and in other cases, the comparison is performed outside the registry, which is not the best situation from the perspective of data privacy. Under these conditions, it cannot be guaranteed that images from the public registry are not stored or processed outside its systems, which increases the risks associated with the protection of personal data.

Other biometric methods, such as iris scanning, while highly reliable and accurate, are used only in specific cases due to their invasive nature and the significant resistance they face to widespread adoption.

Biometrics also presents significant challenges. Unlike passwords, biometric data used to validate an identity—such as a face or fingerprint—cannot be easily altered by the natural person. In the event of an accident, physical impairment, or aging, this data may not be recognized correctly, hindering access.

Currently, advances in Artificial Intelligence, and particularly deepfakes (video, audio, or images in which AI makes it appear that a person said or did something that never actually happened), represent a real threat to biometrics. It is likely that soon, liveness detection or facial biometric comparison will no longer be reliable, at least with current technologies and techniques.

RFID Chip

Currently, many national identity documents, as well as passports, contain a contactless RFID chip according to the ICAO (International Civil Aviation Organization) standard. ICAO established standards for electronic passports where the chip must contain structured and standardized information about the person's identity (the same data printed, for example, in the passport), the public key of the issuing country, and the signature of the issuing authority of that country. This is part of a global Public Key Infrastructure (PKI), and the country's public key is part of the trusted list of this PKI, called the Public Key Directory (PKD) by ICAO. The signature on the certificate ensures the integrity and identity of the issuing authority of the country.

The RFID chip can be read by NFC (Near Field Communication), a short-range wireless communication technology that allows data to be exchanged between two devices simply by bringing them close together, typically less than 10 cm apart. Currently, not only airport readers use this technology, but also a multitude of devices, including many cell phones.

According to the International Telecommunication Union's (ITU) ICT indicators for the SDGs, by 2024, 80% of the world's population aged 10 and over will own at least one mobile phone. A less well-known report, the NFC-enabled handsets market report by Verified Market Reports, indicated that approximately 80% of smartphones sold in 2023 featured NFC technology. While these figures are estimates and vary by region (Latin America and the Caribbean are above the global average for mobile phone ownership according to the ITU), a significant number of people still own NFC-enabled mobile devices. It is a widespread, reliable, and simple technology that is underutilized given its potential. These systems are widely used at border crossings such as airports, but less so for authentication in the web or mobile world.

Countries with chip-enabled identity cards could implement a mobile application that allows users with NFC-enabled cell phones to tap their physical documents against the device and digitally identify themselves on a digital service. The mobile application acts as an intermediary between the physical identity document and the digital service. This is a secure method based on the use of digital signatures (not the signature of a natural person, but rather a recognized Public Key Infrastructure, or PKI), with credentials distributed and protected by cryptographic devices (smart cards).

All these standards are open and well known, so it could be of interest and have a significant impact for countries in the region, especially those that have chip-based identity documents, at least for part of the population, to develop methods using these forms of digital identification and benefit the entire ecosystem, tax administrations, and other stakeholders.

3.2. New Digital Identification Models

Based on the trends in the previous section and considering the main standards and best practices promoted by the most recognized organizations in the field, the following are new methods of digital identification.

Cloud-Based Digital Signatures for Digital Identification

The certificates and keys on cryptographic devices held by the user present some challenges in terms of use. Smart cards (identification documents) require a reader, that is, a physical device into which they are inserted and which connects to the computer via USB. Using cards and tokens requires installing the manufacturer's drivers, which generates costs and a high degree of dependence on the country and the manufacturer, as well as specific programs that can cause various problems: user permissions for installation, conflicts with the operating system or components, conflicts with browsers, or even, if downloaded from an incorrect source, they could include malware such as trojans, among others.

This creates barriers to their widespread adoption, preventing them from reaching all audiences. Furthermore, using them on cell phones is either impossible or extremely complex, as their physical interfaces are generally USB, and the drivers are not developed for Android or iOS.

For several years now, centrally managed digital signature services have become increasingly popular. In this case, instead of issuing credentials and a certificate to a natural person on an external cryptographic device

(token or smart card), a signature provider generates and stores them in a secure area for the user within a Hardware Security Module (HSM). This offers significantly larger storage capacity and extremely robust cryptographic controls, ensuring that each user has exclusive access to their keys and certificate, which are then held in safekeeping by the provider.

This "cloud-based" digital signature can also be used for digital identification, just like a signature on a cryptographic device owned by the user, but with less friction. No reader is needed, no drivers are needed, and it can be used from a mobile device. The signature provider also acts as a digital identification provider. In this case, although the keys and certificates are centralized—in the provider's cloud, the characteristics and strengths of HSMs guarantee the independence of the keys and provide a higher level of security than a database with encrypted usernames and passwords.

A widely used standard for cryptographic devices is the Federal Information Processing Standard (FIPS), currently in version 3 since 2020, issued by NIST (National Institute of Standards and Technology, United States). The objective of FIPS is to ensure that any hardware or software performing cryptographic operations meets a verifiable level of protection against physical and logical attacks. Certification Authorities that manage keys in the cloud generally use at least FIPS 2 and FIPS 3 Hardware Security Modules (HSMs). FIPS 3 guarantees, among other things, that private keys can never be extracted in cleartext and features a physical design with seals, anti-intrusion sensors, and electromagnetic shielding that automatically destroys information in the event of unauthorized access.

Digital identification methods based on cloud-based signatures are already operational in several countries in the region. Since the user's private key remains secure within the provider's hardware security module (HSM) and is never exposed, establishing secure connections between the ecosystem's digital services and the provider is essential. In this context, **incorporating a digital identity broker as a core component of a national ecosystem is crucial**, as it enables a single integration with the identity provider, thus facilitating the cross-platform use of this mechanism across multiple digital public services without requiring natural person integrations for each one.

Self-Managed Digital Identity, Verifiable Credentials, and Digital Wallets

In recent years, a set of standards, protocols, and technologies have been developed that aim to offer a new concept of digital identity, granting natural persons complete control over their digital persona. This new identity model is known as self-managed or self-sovereign digital identity and incorporates two innovative technological elements: digital wallets and decentralized information registries.

These are models in which identity is not held by a third party or an identification service provider but rather recognizes that a natural person should own and control their identity without the intervention of administrative authorities.

In 2016, Christopher Allen established the 10 principles for self-managed identity. These principles are:

- Access: Users must have access to their own data.
- Consent: Users must have prior consent for the use of their identity by third parties.
- Control: Users must be able to control their identities.
- Existence: Users must have an independent existence.
- Interoperability: Identities must be widely usable.
- Minimization: Disclosure of claims must be reduced.
- Persistence: Identities must be durable.
- Protection: Users' rights must be protected.
- Portability: Identity information and services must be portable.
- Transparency: Systems and algorithms must be transparent.

One way to realize this concept is through digital wallets, private repositories, for example, in a mobile application, allowing people to manage all their digital assets with complete autonomy and privacy. This could provide quick access to digital versions of identity documents, university diplomas, driver's licenses, etc.

This approach has already been enabled in the European Union with the approval of eIDAS 2.0 and the regulation of the European Digital Identity Wallet (EUDI Wallet).

Concepts and Fundamentals of Verifiable Credentials

Verifiable credentials are a secure, standardized digital way to represent information about a person, organization, or entity, so that it can be cryptographically verified by a third party without relying on a central authority for each verification. In the physical world, it has been common practice for several decades to manage various types of physical credentials, such as:

- Identity: credentials that prove who we are, such as a national identity document, identity card, passport, and driver's license (in some cases).
- Academic and professional: university diplomas, international certificates, language certificates, employment certificates, etc.
- Health: vaccination card, medical certificate, laboratory test results, etc.
- Financial or compliance: proof of identity, verification of solvency or bank affiliation, tax history or compliance certificate, among others.
- Membership or access: accreditations to enter a club, building or event, police officer or traffic inspector credential or member of an organization.

There are many types of credentials, but also different levels of validity. For example, a passport is a globally recognized identity credential, but a gym membership card is only recognized within the gym.

They can also be approached from the perspective of trust level, in which case they can be categorized into three levels:

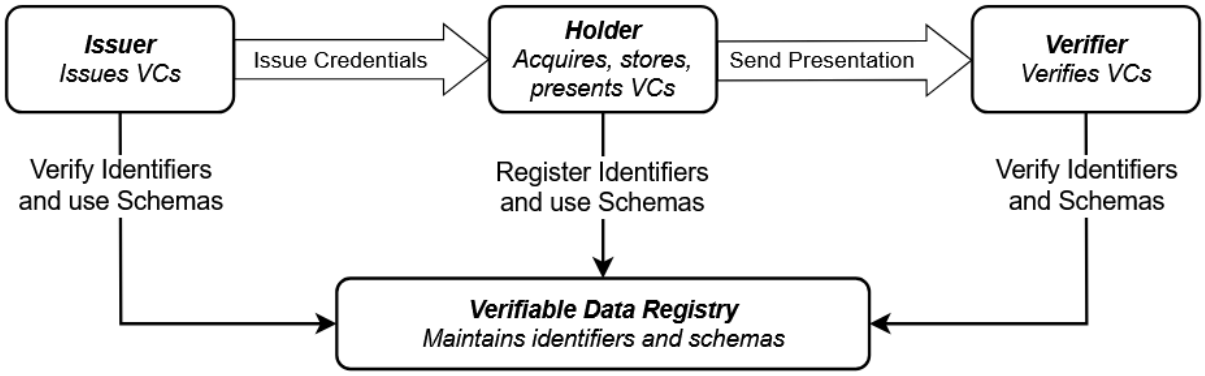
- Low: information self-declared by the holder, for example, a social media account.
- Medium: information verified by an entity, for example, a phone number or document.
- High: credential verified in person or through appropriate technologies (digital signature, NFC chip, biometrics that meet certain requirements). This category includes credentials such as national identity documents, passports, driver's licenses, etc.

Relevant Standards and Protocols

While verifiable credentials have been a developing topic for some years, there are currently a few standards that appear to be prevailing because they have a larger community for their development and evolution, are sponsored by relevant organizations, and are being adopted in a growing number of countries.

The W3C Verifiable Credentials Data Model 2.0 (VCDM 2.0) is the most important international standard for representing digital identities and verifiable credentials on the web. It is developed by the World Wide Web Consortium (W3C), the same organization that defines Internet standards (such as HTML, CSS, etc.). The following diagram illustrates this standard:

Figure 10. Diagram of the W3C VCDM 2 standard.



Note: Adapted from Verifiable Credentials Data Model v2.0, by Sporny, Longley and Lindström (2023). Retrieved from [URL].

This standard focuses on defining the actors involved in this ecosystem to create, issue, share, and verify credentials in a secure, interoperable manner, protecting the privacy of information and a large nomenclature.

It is based on the following principles:

- Decentralization: It does not depend on a centralized authority or a single database;
- Verifiability: Anyone can verify the authenticity of a credential without contacting the issuer;
- Portability: the user stores credentials on their own device (wallet);
- Selective privacy: the holder can choose what data to share;
- Interoperability: compatible with other recognized standards such as DID, JSON-LD, JWT, and OIDC4VC.

This is a standard that is becoming prevalent for defining the entire ecosystem of verifiable credentials at the country level. The European Union and most of its member states are adopting it, as are the United States and Canada, Australia, Japan, and South Korea. In Latin America and the Caribbean, countries with initiatives in this area have defined this standard as the basis for their ecosystem. Within these countries, the level of maturity and progress varies. Some countries have already made the decision, others are beginning development, and still others already have some credentials based on version 1.0 and are therefore in transition. The current version, 2.0, is from May 2025.

Another group of standards that is gaining prominence is the OpenID Foundation, which focuses primarily on exchange protocols, such as OpenID Connect for Verifiable Credentials (an extension of OpenID Connect) in its two versions: OIDC4CI, for the issuer to transfer the credential to the holder, and OIDC4VP, for the holder to present it for identification in person or digitally.

The other major family is ISO/IEC 18013-5, which specifically defines certain identification credentials, such as national identity cards and driver's licenses. This standard is being adopted by the European Union, the United States, Australia, and some countries in Latin America and the Caribbean have expressed interest.

Additionally, there are specific standards such as DID (Decentralized Identifiers) from the World Wide Web Consortium (W3C) that defines global, verifiable, and decentralized identifiers, and the DID Resolution & DID Document specification that describes how to resolve a DID to obtain public keys and metadata, as well as other specific standards that define the details of digital signatures on credentials and other relevant security issues.

Operating Ecosystem - Actors and Verifiable Credential Flow

These physical credentials, which have been used naturally for decades, represent the same concept as today's verifiable credentials in the digital world. Regardless of their type or level of trust, the actors involved in a verifiable credential ecosystem are as follows (this also applies to physical credentials):

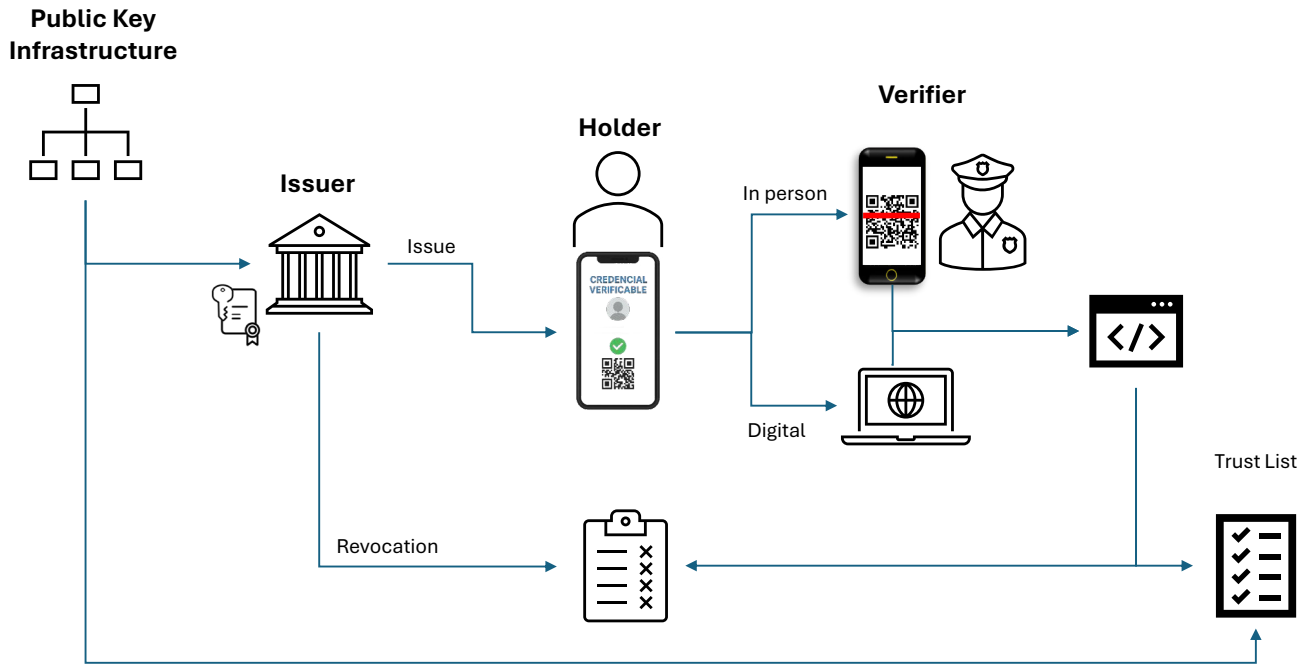
- Issuer: The legally competent entity that issues credentials of a specific type. This entity is recognized as trusted by the ecosystem for a given credential, regardless of its scope (a civil identification agency has a national or global scope in the case of a passport, while a sports club's scope is limited to its facilities). The issuer signs the credential, which provides the verifier with assurance that all the information contained in the credential is reliable. The signature may vary depending on the credential, its ecosystem, and its criticality. An identity credential must be signed with the digital signature (advanced, qualified, or certified) of the competent authority, as part of a National Public Key Infrastructure. A gym access card may be signed with a simple signature from the gym, but one recognized as trusted within the gym's facilities. Issuers can also revoke credentials according to the regulations applicable to each card (some may not be revocable).
- Holder: The person who possesses the card in their electronic wallet, usually on their mobile phone, and decides when and with whom to share it. The holder can display it in person on their device in graphic format (human-readable, but less secure), in QR format (readable by a validator, where, moreover, the QR

code is signed, thus guaranteeing its content), or use it to digitally identify themselves (authenticate) on a web or mobile digital service using the OIDC4VP protocol.

- Verifier: The entity that receives and validates the credential. This depends on the credential's scope; it could be a police officer verifying an identity card or a building doorman verifying an access card. This process can be automated, and the information provided by the holder can be minimal or more extensive. The verifier, among other things, must have access to the ecosystem's trusted list (Issuer certificates) to validate the signatures of the verifiable credentials and thus trust the information they contain. Another aspect the validator must review is credential revocation.

The following diagram shows a simplified view of a verifiable credential ecosystem:

Figure 11. Verifiable Credentials Ecosystem.



Source: Prepared by the author

The steps for the ecosystem to function are as follows:

1. The issuer (for example, the civil registry for the national identity document) obtains a key pair and a certificate from the National Public Key Infrastructure to sign the credentials it issues. This signature is like

the signature or seal of a legal entity or company used for electronic invoicing. In the case of electronic invoicing, the company that will issue invoices obtains keys and a certificate to sign them. When it issues an invoice, it is signed by the company, guaranteeing the integrity of the document (invoice) and the identification of the signer. The certificate granted by the provider links the company's tax identification number or identifier to its public key.

2. The certificate granted to the issuer is registered in the trusted list of authorized issuers.

3. A person (the cardholder) who wishes to obtain their credential goes to the issuer (or does so remotely with the appropriate verifications, depending on the credential's criticality). The issuer issues and signs the credential and transfers it to the electronic wallet on the person's mobile device. The OIDC4VCI protocol is used for this transfer.

4. The cardholder manages their credential in the wallet on their mobile phone. Each credential may have different requirements regarding wallet authentication, mobile device specifications, and other factors. The cardholder chooses to identify themselves using the credential in person or digitally:

    a. In-person (machine-readable): a person (for example, an agent) asks the cardholder to identify themselves using their verifiable credential:

        i. The Agent, using a compatible and recognized validator on their mobile device, displays a dynamic QR code signed by the validator.

        ii. The cardholder brings their mobile device close to the validator, scans the QR code with the wallet, and the wallet requests permission to share a specific credential with the validator. In some cases, these credentials can be minimal, protecting the privacy of the information (for example, if proof of age is required, only this information needs to be transferred, not the date of birth, nationality, names, surnames, etc.).

        iii. The cardholder approves, and the wallet sends the credential to the validator. This transmission can be done using different wireless proximity technologies such as NFC or Bluetooth.

        iv. The validator receives the credential and validates the signature of the issuer. It uses the ecosystem's trusted list and revocation list for this purpose. Both lists can be stored locally on the validator and updated whenever it has a connection.

        v. If the format and signature are correct, the credential information is displayed on the screen. Validation can be performed 100% locally and offline, with complete confidence, based on the issuer's signature within the context of the National Public Key Infrastructure. An alternative, although it requires a connection, is for the validator's QR code to have a dynamic Uniform Resource Identifier (URI, endpoint) to which the wallet sends the credential.

b. Human-readable in person: the cardholder displays the credential graphically on the screen of their mobile device, as is currently the case when showing plastic ID cards or identity cards.

c. Digital: The cardholder wishes to access a web or mobile portal or service (for example, the Tax Administration) and selects the option to identify themselves with a verifiable credential in the authentication system. The digital identification system implements the OIDC4VP protocol:

   i. When this option is selected, the web system generates a dynamic QR code containing the information of an endpoint (URI) on the server to which the wallet must send the verifiable presentation.

   ii. The wallet reads the QR code from the portal (for example, the Tax Administration) and requests permission from the cardholder to send credentials. In this case, the cardholder can also customize the information they wish to share with the portal, which must be necessary and sufficient for identification.

   iii. The wallet creates a presentable verification, that is, a set of verifiable credentials under a single presentation created for this purpose, signs the presentation, and sends it along with its public key (the wallet's public key) to the portal endpoint.

   iv. The portal endpoint receives the presentable verification and uses its valid public key to sign it to guarantee its integrity. It then validates each verifiable credential included in the presentable verification. Each credential is signed by its corresponding issuer (recognized by the trusted list). It also validates the revocation and, if everything is correct, uses the information from the transferred credentials to identify the user (holder).

5. Depending on the regulations associated with each credential, the issuer can revoke a credential by adding it to the revocation list. This can generally occur at the issuer's discretion, at the request of the holder, or at the request of a third party, such as a judge.

Advantages of verifiable credentials and implications for tax administration

This form of in-person and digital identification has gained significant relevance in recent years for numerous reasons and is becoming the new standard for both in-person and digital identification worldwide, as it offers several advantages:

- The same credential is used both digitally and in person, making it simple and intuitive for people to use, just as physical credentials have been obtained and used for decades.

- In some cases, digital identification credentials are legally equivalent to their physical counterparts (national identity card, passport, driver's license, etc.), which lends complete confidence to the verifiable credentials.
- High adoption of smartphones worldwide means there are no major barriers to carrying and using them.
- High level of trust: the digital signatures involved, if they comply with current recognized standards and the regulations associated with the National Public Key Infrastructure, are impossible to falsify or alter. They are even more reliable than their physical counterparts.

Regarding its use for digital identification (authentication), this innovative system offers multiple advantages:

- Distributed credentials and private keys remain protected on cryptographic devices; they never leave them. Credentials, and especially the public key, are distributed and under the complete control of their owner. This avoids the need for centralized databases with millions of credentials, which, even if encrypted (password hashing), are inherently a considerable risk.
- Credentials based on the use of digital signatures and without passwords, as suggested by current trends, but significantly reducing the friction (barriers) present in digital identification methods based on digital signatures on other cryptographic devices (smart cards or tokens). They even further reduce the barriers generated by cloud-based signature use cases for identification.
- Easy to use. The high penetration of mobile devices has made it very simple and intuitive for people to install and use mobile applications, use proximity data transfer methods (NFC or Bluetooth), and read QR codes, among other things.
- There is no need for smart card readers, specific programs, or drivers that could cause permission or compatibility issues with operating systems, other components, or browsers.
- Open standards lead to low dependence on proprietary software. If the credentials use a specific standard, any wallet compatible with that standard can be used, which considerably expands the possibilities for accessing wallets and reduces dependence on a few manufacturers and national digital identification systems.
- Low technological requirements, as only a mobile device with NFC or Bluetooth is needed.

A relevant aspect is the vision of using verifiable credentials for digital identification across borders. In this case, different scenarios can occur:

- In-person identification outside the country, for example, appearing at the tax authority of another country. The following is required to use an ID card outside the country:
  - The identification credential held by the provider must be in a format compatible with the validator. This requires using standards recognized by different countries.
  - The trusted signature list of the country of origin must be accessible to the validator of the other country.
- Digital identification across borders, for example, accessing the tax authority's website in another country. In this situation, there could be two scenarios:
  - There is no cross-border integration of digital identification between the countries: the user accesses the tax authority's website of the other country, which has developed an identification method using OIDC4VP. For the website to validate the credential, it must know the standard used by the credential and have the trusted list from the country of origin. While this situation is feasible, it is not the most recommended. Ideally, scenarios should be achieved where the digital identification systems or ecosystems at the national level are integrated with their counterparts in other countries.
  - There is cross-border integration between the systems or ecosystems of both countries. This would be the ideal scenario, given that the credential is validated in the user's country of origin, and the user then returns to the tax authority portal of the validated foreign country. As discussed in Chapter 1, the user accesses the tax authority portal, selects their country of origin for identification, and is redirected to their country's digital identification system or ecosystem (broker). At this point, they choose to present their credential, and the system or ecosystem must request the credential using OpenID Connect for Verifiable Presentations. Once the user is identified, the system redirects them to the Tax Administration portal.

In a national digital identification system or ecosystem where the Tax Administration is a key player and fully integrated, allowing its users to digitally identify themselves on its portal and applications (web and mobile) using national digital IDs, this innovative method can be of great interest.

If the country has an ecosystem managed by a digital ID broker, implementing this new method as an identification provider is considerably easier. The broker will need to implement the OpenID Connect for Verifiable Presentations protocol (an extension of the OpenID Connect protocol, which it likely already has), and this new method will then be enabled for all integrated systems, including the Tax Administration.

As part of the broker's governance and the country's digital identification ecosystem, in addition to implementing this protocol that enables the use of verifiable identity credentials for digital identification, it is necessary to make some decisions related to standards. These decisions are important for several reasons:

- They facilitate interoperability, not only nationally but also cross-border. Ensuring that natural persons have verifiable identity credentials in their wallets that meet the appropriate standards is critical for them to be able to use them throughout the country and abroad.
- They facilitate evolution and lifespan. Appropriate standards endure over time, thus ensuring the entire lifespan of the credentials.
- They facilitate usability. The prevailing standards will support a wider range of wallets and features, across more platforms, and with better conditions for future development.

Summary and Roadmap

In summary, regarding digital identification in Tax Administrations, using verifiable credentials as an identification method will surely be the dominant method in the future given its simplicity and high level of trust. The following points are noteworthy:

- Defining appropriate standards at the national level is a major and critical challenge. For verifiable identification credentials, basing their ecosystem (actors and roles) on the World Wide Web Consortium (W3C) Verifiable Credentials Data Model 2.0, using OIDC4VC for transfer and ISO/IEC 18013-5 for detailed specification seems to be a winning combination at present and is likely to remain so for this use case in the coming years.
- Developing appropriate governance and regulations, ensuring that verifiable credentials are equivalent to their physical counterparts.
- Having an ecosystem coordinated by a digital identification broker that implements the OIDC4VP protocol to enable digital identification across all digital and mobile services using a verifiable credential is important to facilitate and enable this secure and easy-to-use method, achieving an impact at the national level. If the Tax Administration is integrated, it is not necessary to develop or modify its systems.
- In addition to adopting the correct standards, integrating cross-border digital identification systems or ecosystems would enable the simple and secure use of verifiable identification credentials for digital authentication in services in other countries, as well as opening access to domestic services to people from other countries. Tax administrations could greatly benefit from this scenario.

3.3. Evolution of Digital Identification in Tax Administrations

Tax Administrations should become part of a national digital identification ecosystem or system. Clearly, this doesn't depend solely on the Tax Administrations, but it does depend on the following:

- **Promote national digital identity:** As a relevant actor within the public administration, if one exists, or at least if there is an initiative, lending support to the development of a national solution or a coordinated ecosystem, given that this represents significant economies of scale for the State. By delegating identity verification to a unified provider or system, operating costs are reduced by avoiding duplication of security investments by each agency and by repurposing the country's investment in new authentication methods. All this also contributes to offering a more unified, convenient, and secure experience for citizens when identifying themselves to access all digital government services.
- **Integrate into the national digital identity:** If a national system or ecosystem exists, integrate as a consumer of its digital identifications, that is, delegate authentication.
- **Offer digital identification (if appropriate):** Together with ecosystem stakeholders, explore the possibility of becoming an additional digital identification provider. For this, the Tax Administration must have the necessary conditions and invest in IT development and infrastructure. In general, the requirements include having a database of natural persons whose identities are validated (only natural persons, not companies, are considered for national identification), and the data used to identify a person must be compatible with the data defined by the national ecosystem, or at least easy to transform and adapt. The Tax Administration must be able to isolate its digital identification system and implement a known protocol to integrate with the national broker, such as those mentioned previously. It must also consider the operational burden that using its identification system to access other public systems may cause. Consequently, investments in infrastructure, security and quality reviews, and establishing a service level agreement to guarantee the system's availability and reliability will be necessary. In countries where national digital identification is an emerging initiative, using the tax administration's identification system at the national level can be beneficial for accelerating ecosystem development.
- **Authorization:** provide a comprehensive solution for Authorization, once the natural person is identified through the national ecosystem or system. This point will be addressed in detail below.
- **Audit:** Design a detailed audit system (system activity traceability), given that different people with diverse roles related to companies and taxpayers will begin to access the system. Audits are essential for reconstructing information in case of data breaches, accurately and reliably reconstructing events, and providing evidence in cases of crime or fraud.

- **Easier-to-use and more secure national digital IDs for greater trust:** Support and, at the same time, require national systems or ecosystems to strengthen available identification methods by mandating the use of two-factor authentication or, even better, evolving towards passwordless, decentralized methods based on the use of digital signatures.
- **More reliable IDs in tax administration:** If a national system or ecosystem is not in place, the Tax Administration should strengthen its digital IDs by requiring at least one second authentication factor and, if possible, evolving towards passwordless, decentralized methods based on the use of digital signatures.
- **Beyond borders:** supporting national systems or ecosystems to integrate with their counterparts outside their borders, thereby facilitating simple and reliable access for foreign taxpayers.

In summary, tax administrations should support the development of national identification systems or ecosystems, where possible, by delegating the identification of their users to them and concentrating on developing in-depth **authorization and audit** systems.

3.4. Authorization in Tax Administrations

The concept of "authorization" takes on a central role—as discussed in Chapter 1 of this publication—by becoming an essential operational foundation within digital identity systems. In the field of tax administrations, authorization transcends its technical dimension as an access control mechanism: it is configured as an instrument of institutional guarantee, ensuring that each digital interaction is carried out under explicit criteria of legitimacy, in accordance with current regulations on representation and avoiding situations of repudiation.

Delegated Access and Role Management

Authorization cannot be understood in isolation, as it requires a solid foundation of reliable and contextualized authentication. Once a person has been authenticated (identified) by the system, the system authorizes them to access specific information and perform specific actions. This process is conditioned by the user's profile, the level of trust associated with the identification method used, and the specific rules defined by the system. While this Guide does not address in depth the design and implementation of authorization mechanisms, it is essential to recognize their close dependence on digital identification and to address their fundamental aspects.

In the field of tax administration, the delegation of functions is the legal mechanism by which a taxpayer or legal representative transfers certain powers to an authorized third party, ensuring the validity and traceability of said representation. This delegation should be reflected in the **management of roles** within digital systems, where specific profiles are assigned that determine the permissions and responsibilities of each user.

Principles of access allocation

Security in digital tax identification systems must be based on a fundamental principle: access must be allocated to natural persons, even when they are acting on behalf of entities. Tax administrations must avoid granting credentials directly to legal entities or associations without legal status.

Instead, it is recommended to allocate access to natural persons acting on behalf of these entities, under a clearly defined role or delegation of permissions scheme. Each user must declare, upon authentication, whether they are acting on their own behalf or on behalf of another taxpayer—whether a natural person or a legal entity, for which they must have previously received formal authorization that grants them a role and allows them to operate on their behalf.

This authorization must have adequate legal backing. In the case of natural persons, the owner can directly grant the role. In the case of legal entitys, the allocation of roles must be carried out by their legal representatives or by those formally authorized by them. When there is joint representation, it will be necessary to ensure the express consent of all those involved to validate the allocation.

Authorization Levels

The roles to be delegated that must be managed by the authorization system could have these three levels, ranging from the most general to the most specific:

- **By function or professional role:** The taxpayer can assign specific functions to natural persons, such as manager, accountant, lawyer, etc. The Tax Administration could offer a suite of digital services linked to each role: for example, the accountant would have access to all tax services, while the lawyer would only have access to those related to legal aspects. These roles could be predetermined by the Tax Administration, with the possibility of customization by the taxpayer. Furthermore, “sub-delegation of roles” could be enabled, as in the case of a manager who delegates functions to employees of their firm. In this scheme, it is essential that, upon revoking the original role, all associated sub-delegations are automatically deleted.

- **By objects:** The taxpayer can assign permissions on specific objects offered by the Tax Administration within the functionalities of the systems. To facilitate this management, the use of role assignment matrices is recommended, as these allow for the clear and structured visualization and administration of granted permissions.
- **By data point or data set:** This level allows granting or revoking permissions on specific data associated with the company or natural person, within the objects for the various functionalities. Its implementation must align with the Tax Administration's Data Governance policies, considering the classification of data criticality according to the institutional information security guidelines.

The vision of implementing authorization at these three levels—by function, by object, and by data—can offer a good combination of simplicity for the taxpayer, while still providing the potential to manage access down to the data level if deemed necessary. At each of these levels, the Tax Administration could establish the required security level, depending on the type of action to be performed. For example, submitting a tax return might require an advanced level of identification, while requesting a certificate would only require an intermediate level.

The access control system should be accompanied by guides and support tools, as well as reports, queries, and alerts directed to key roles (such as owners or representatives), so they can monitor the allocation of permissions for the company and how those permissions are being used.

Identity and Permission Lifecycle

Authorizations must be able to be granted generally or specifically, with a time limit and the possibility of immediate revocation. The role and delegation system must consider the lifecycle of identities and permissions in the tax field, including critical events that impact the validity of access:

- Addition: inlegal entity of new representatives or agents.
- Modification: changes in role, reallocation of functions, or updating of access levels.
- Removal: situations such as retirement, death, termination of employment, mergers, or institutional spin-offs. If roles have been subdelegated, the removal must revoke the subdelegated roles in a cascade.

Each of these transitions must be recorded and audited to ensure the integrity, traceability, and reliability of the digital identity system. From a security perspective, it is important to emphasize the **principle of least privilege**. This means that a user should have the minimum privileges necessary to perform their job. The reason for considering this principle is simply to limit the impact of malicious user behavior (whether intentional or accidental), as well as identity theft, among other information security risks.

Tools and Technologies to Strengthen Role Management

Role management is an important aspect of tax administration, directly contributing to its transparency, efficiency, and reduction of compliance and information security risks. Throughout this Guide, aspects related to digital identification have been explained where these systems identify natural persons and these natural persons have relationships modeled under roles with taxpayers in the Tax Administration.

These relationships need to be verified, so each person must demonstrate that they possess the authority to act on behalf of a specific taxpayer before the Tax Administration. Currently, there are several ways to register these relationships. The necessary documentation is submitted to the Tax Administration to prove a specific relationship or link between a natural person and a particular natural person or legal entity. From then on, when a natural person accesses the Tax Administration system, it recognizes them with a specific role and enables them to perform the operations defined by the functionalities, objects, and data for that role.

Depending on the specific case, the importance of the operations and information, the applicable regulations, and the capabilities of the Tax Administration's systems, this role allocation can be resolved remotely and easily, or it may require a more complex in-person process (presenting certified documentation that validates these powers). In the latter scenario, given the importance of the functions and the sensitivity of the information, it can be cumbersome and costly for a taxpayer to keep these records updated, since any change would require preparing the relevant documentation and appearing in person at the Tax Administration.

For these more complex, sensitive, and risky cases, tools and technologies currently exist that, when properly enabled (with the necessary regulations), could resolve role management in a 100% remote and digital manner with very high levels of reliability. This would significantly reduce time and costs, but also the associated risks, as it would be much easier for taxpayers to keep their records with the Tax Administration up to date.

The following are three tools and technologies based on the use of digital signatures and the trust inherent in a recognized Public Key Infrastructure (PKI) to address this issue in a 100% remote and digital manner:

1. **Digital Signatures with Attributes:** This is an advanced electronic signature that includes attributes defining the holder's role or competencies. This signature is issued by an accredited certification service provider, which not only validates the holder's identity but also their competencies and specifies them in the issued digital certificate. The holder presents themselves to the certification service provider (digital signature) and requests a form that also specifies a particular competency (for example, lawyer, doctor, company representative, company partner, etc.). Depending on the requested competency, they must submit information to the provider that validates said competency. The provider verifies the competency (based on the information submitted and/or by interacting with the organization that holds the authority

for the requested competency). If the holder possesses the requested competency, this is specified in the attributes included in the certificate issued by the provider. Attributes are additional data to the signature, so when a person signs a document with this type of signature, they are not only signing as a natural person, but are also fulfilling a specific role, authority, or competence, as specified in the certificate's attributes. These attributes could relate to professions (doctors, architects, lawyers, etc.), positions (manager, director, owner, representative of a particular company), roles (auditor, administrator, public official, etc.), certifications, licenses, or any other authority, attribute, or competence that a competent authority (regulated for such cases) can certify regarding the person. This model ensures confidence in the powers attributed, in the same way that advanced electronic signatures guarantee the identity of the signatory. Once implemented, it is not complex to use, given that a document is signed only once with the corresponding attributes. Some difficulties with this model are:

- Where required, signature providers must securely interact with governing organizations to determine if a natural person possesses the necessary competencies and issue the corresponding signature certificate. Ideally, this should be resolved through interoperability between both systems for greater automation. However, in a less digitally developed environment, the natural person could submit all supporting documentation to the signature provider. While this creates challenges, it also simplifies the process by centralizing the issuance of all signatures with accredited signature providers (who already possess the necessary capabilities).
- The user must have a set of signatures and be clear about which one to use at any given time according to the regulations for the use case and manage all of them. They should have a signature for a natural person, but also a signature for each of the attributes they possess, which could lead to a large set of signatures to manage.

Revocation: Upon request from the appropriate party (in the case of a company, the owner), the service provider, or a third party (depending on the case), the service provider must revoke the entire signature. Therefore, anything signed after the revocation will be invalid. The accredited service provider must keep the revocation list updated and accessible.

2. **E-seals:** While the previous case is also considered a seal in some countries (in the European Union, the concept of a legal entity's signature no longer exists, having been replaced by that of seals), this model is simpler for natural persons (end users) but more complex for responsible authorities. In this scenario, each person has their own personal signature, and each responsible authority has a system for sealing documents. When someone needs to sign a document to demonstrate competence, they sign it with their personal signature and, using a service provided by the competent authority, request that the document be sealed. Based on the signature, the competent authority uses its records to determine whether the person currently possesses the authority and, if so, seals the document. The seal is technically equivalent

to an advanced electronic signature for a legal entity and provides proof that the person who signed at that time possessed specific authority. This model has both advantages and disadvantages. As an advantage, the process is simpler for natural persons, since they only need their advanced electronic signature as a natural person, and revocation is not required. The document is stamped at a given moment, which guarantees that the person had that competence at that moment. It is recommended that this be accompanied by a verifiable timestamp to guarantee the date of the stamping. One barrier or difficulty with this model is that all responsible authorities must have a system for stamping documents. Depending on the specific regulations, the stamped document may have a certain validity period or remain valid until the taxpayer indicates otherwise.

Revocation: In this scenario, the process is simpler, since the authority, when issuing the seal, must verify whether the authority is still in effect and, if so, issue the seal. Trust in this case is based on the moment the seal is issued; a revocation list is not required.

3. **Verifiable Credentials for Competencies:** Earlier in this chapter, the concept of verifiable credentials for identification purposes, equivalent to a national identity document, was discussed. Similarly, there are verifiable credentials that certify competencies, roles, or powers. In this case, the interested party contacts the relevant responsible authority, requests a credential, the authority generates it, and sends it to the holder's electronic wallet. This process can be carried out remotely or in person, depending on the regulations and solutions provided by the authority responsible. In this scenario, the Tax Administration must develop a service within its authorization system so that the user, once identified, can send their credential. These credentials are not for identification purposes, so the user must first identify themselves digitally. Then, when requesting a specific role, the credential is sent using a protocol such as OpenID Connect for Verifiable Presentations, discussed earlier. The user would manage their competencies in their electronic wallet and could use them both in person and digitally, as seen in the case of verifiable credentials for identification. In a scenario where verifiable credentials become widespread, as current trends indicate, this option would face fewer barriers. Users could use their identification credentials to remotely and securely request authority credentials and manage all their credentials simply and conveniently in their digital wallet. Responsible authorities should be on the trusted list at the national level and have a revocation system in place, like the one used for verifiable identification credentials.

   Revocation: Like digital signatures with attributes, authorities that issue verifiable credentials must maintain a revocation list that will be consumed by validators. Depending on the model, the revocation list may be centralized (for all credentials), as suggested by the World Wide Web Consortium (W3C) model, or distributed, i.e., one list for each authority, like digital signatures.

The following table presents a comparative summary of the three models. It is important to emphasize that, from a trust perspective, all three are equivalent and fully reliable.

Digital signatures with attributes	E-seals	Verifiable credentials for authorities
Responsible authorities		
They interact with digital signature providers to validate competencies and request revocations. Low or moderate technological development. The authority responsible must request the digital signature provider to issue the revocations it deems necessary based on its regulations.	They must develop a service to seal documents using a certificate within the context of a recognized Public Key Infrastructure. High level of technological development. Revocation is simplified since it is verified at the time of sealing.	They must develop a service to issue and revoke verifiable credentials using a certificate in the context of a recognized Public Key Infrastructure. High level of technological development. Each Authority must maintain a revocation list.
Users		
They interact with signature providers. They must possess multiple signatures with their respective authorities and use a system for signing. Complex management.	They must have a single signature from a natural person and use an official service to seal documents. Simple management.	They must have an electronic wallet to manage their credentials. Intermediate management.
Tax administration		
It must develop functionalities to allow users to submit signed documents and more complex validators for each type of signature or perform manual reviews.	It must develop functionalities so that users can send signed and sealed documents, and the validator must have the ability to validate the user's signature and the authority seal or perform manual reviews.	It must develop capabilities that allow users to present their verifiable authority credentials from their electronic wallet to the Authorization system after digitally identifying themselves. It must also develop the ability to validate the credentials presented by the user.

Depending on national capabilities, for all validation processes (in all three cases), the Tax Administration could integrate into a service developed and maintained by a centralized system under the responsibility of the competent Digital Government authority.

The last section of this chapter, "3.8 Roadmap," presents suggestions on how the Tax Administration could move forward in developing these tools and technologies to strengthen and streamline the management of roles or delegation as part of the Authorization system.

Access Control Models

Access management in digital identity systems requires structured approaches that allow for the secure, traceable, and adaptable assignment, modification, and revocation of permissions, depending on the operational context. In this regard, two models widely recognized by international standards are presented, offering robust conceptual frameworks for designing authorization policies in tax environments.

On the one hand, the RBAC (Role-Based Access Control) model, formalized by the ANSI INCITS 359-2004 standard, allows for the allocation of permissions based on predefined roles, facilitating centralized and consistent access management in organizations with clear hierarchical structures. On the other hand, the ABAC (Attribute-Based Access Control) model, described in the NIST SP 800-162 framework, introduces a more dynamic logic based on user, resource, and environment attributes, enabling more granular and contextual access decisions.

Below, we describe their main characteristics, suggested applications, and considerations for implementation, as well as two other models that are not as widely used or ideal for tax administration:

Model	Description	Application
RBAC (Role-Based Access Control)	Assigns permissions based on predefined roles within the organization. Each role groups a set of permissions that reflect specific responsibilities, facilitating centralized and consistent access management.	Ideal for stable profiles such as managers, tax advisors and accountants, where the functions are clearly defined.
ABAC (Attribute-Based Access Control)	Defines access based on dynamic attributes of the user, resource, or environment. These attributes can include entity type, risk level, access schedule, and more. This approach allows for more granular and adaptive decision-making.	Recommended for scenarios where context influences authorization, e.g., access only at certain times from a specific jurisdiction.
DAC (Discretionary Access Control)	The resource owner defines who can access it and with what permissions directly.	Some UNIX-based operating systems implement it. It is simple and flexible but difficult to scale and control in large environments.
MAC (Mandatory Access Control)	The system defines policies according to security levels and information classification. Resources are classified into levels (e.g., public, restricted, and confidential) and associated with user groups based on the policy design.	It's a centralized approach with little flexibility, complex to implement, but easy to scale. RBAC is a less rigid and easier-to-manage alternative.

Both approaches (RBAC and ABAC) offer complementary advantages and can be strategically combined to address the security, representativeness, and flexibility challenges faced by tax authorities in their digital processes. Combining these two models enables flexible, secure, and scalable access management, considering the three proposed levels.

3.5. Auditing in Tax Administrations

As part of the AAA model, presented in Chapter 1, in a scenario where Authentication (Digital Identification) is resolved at the country level and delegated to a system or ecosystem by the Tax Administration, the latter must focus on adequately developing Authorization and Auditing.

With respect to Auditing, in this context, it refers to the traceability of all activity of all users within the Tax Administration's system. This implies recording a trace of each action, which must include at least the following:

- User: identifier of the user who performed the action;
- Timestamping: accurate date and time obtained from a reliable time server at the time of operation;
- Origin: information about the starting point from which the user was working. This can include not only the IP address used by the user, but also a fingerprint of the device the user used to work;
- Information about the action: a description of the transaction the user performed, as well as structured information about a catalog of possible actions (new, modified, deleted, displayed, etc.) on the data;
- Previous state of the data to be modified and other relevant information.

While auditing serves multiple purposes, each of the systems that make up the Tax Authority's platform may have different tools, and there are also specific tools for log management, although these are generally intended for events of interest from a cybersecurity perspective rather than data traceability.

Information sources generated for auditing must be treated with the same care as the data sources from the systems, given that they contain sensitive information and even greater detail because they retain their complete history.

The goal is to be able to determine with precision and confidence what each user did, from where, and when, at every moment within the system, maintaining a complete and detailed history of the traceability of all actions of each internal and external user.

The audit system should include, at least, the following components:

- **Event capture:** a module that automatically captures every user's action (login or logout, creation, modification, deletion, query, export, permission changes, etc.). It is important that the exact time of day be obtained from a central server at the Tax Administration for greater reliability. In a more sophisticated

case, a timestamp using NTP could be used. Unambiguously identifying the user, their authorization (when applicable), and the specific action being performed on the resource is also key to the quality and reliability of the audit information. For this purpose, it is important that the information be as structured as possible to facilitate storage and searches, as well as quality checks or the detection of anomalies or inconsistencies.

- **Trace persistence:** These systems generate large volumes of information, making the choice of solution a considerable challenge, as are the resources allocated to them and their backup policies, confidentiality protection, etc. Traceability should have tools to protect its integrity; it should not be possible to modify it, and this should be mathematically verifiable. The use of hash functions to protect and verify its integrity over time can be an important tool.
- **Correlation or analysis systems:** There may be systems that review, in real time (or very near real time) as well as retrospectively, the different movements in search of anomalies, fraud attempts, unauthorized access to information, etc. Integrating the audit into a Security Operations Center (SOC) can be a very good strategy for detecting potential fraud or unauthorized access in the Tax Administration. The SOC could use a SIEM (Security Information and Event Management) tool to correlate or analyze events, even cross-referencing them with external sources (other servers and network traffic).
- **Retention and deletion:** Retention and preservation should be aligned with the Tax Administration's data governance. It is important to have an adequate backup system.

The main standards in this area are:

- ISO/IEC 27001, which establishes the operation of an Information Security Management System, includes two controls: A.12.4 "Logging and Monitoring" and A.12.7 "System Audit Considerations."
- ISO/IEC 27002, a supplementary guide to good practices: how to implement and protect audit logs.
- NIST SP 800-92, a guide on log storage and analysis.
- NIST SP 800-137, a framework for continuous information security monitoring, which includes monitoring user activity.

Building Valid Evidence

The need to build robust audit trails of activity across different systems and data access points is directly related to the need to build valid evidence for the Tax Administration. Digital evidence is fundamental in digital identification processes because it guarantees the authenticity, integrity, and traceability of the actions and data used to verify a person's identity.

Digital evidence supports each step of these processes, allowing the legitimacy of a digital identity or transaction to be demonstrated.

According to ISO/IEC 27037:2012, digital evidence is defined as "information or data, stored or transmitted digitally, that can be used as evidence." Its proper management strengthens trust in authentication systems, protects against fraud, and facilitates the traceability of operations.

Its relevance can be expressed at several levels:

- **Proof of authenticity:** Digital evidence (such as access logs, electronic signatures, metadata, or biometrics) allows proof that a person participated in an identification or authentication process. It allows for reliably linking a person to a specific action or event
- **Data integrity:** It guarantees that identity data (documents, images, biometric records, etc.) has not been altered since its capture.
- **Traceability and Auditing:** Digital evidence documents who, when, and how an identification process was carried out. It is vital for audits and forensic investigations, as digital evidence has probative value in cases of disputes, fraud, unauthorized access, or identity theft.

The proper collection, preservation, and validation of digital evidence strengthen user and institutional trust in digital identification systems. Digital evidence is the verifiable support that backs up each step in a digital identification process, guaranteeing security, legality, and reliability in the management of electronic identities.

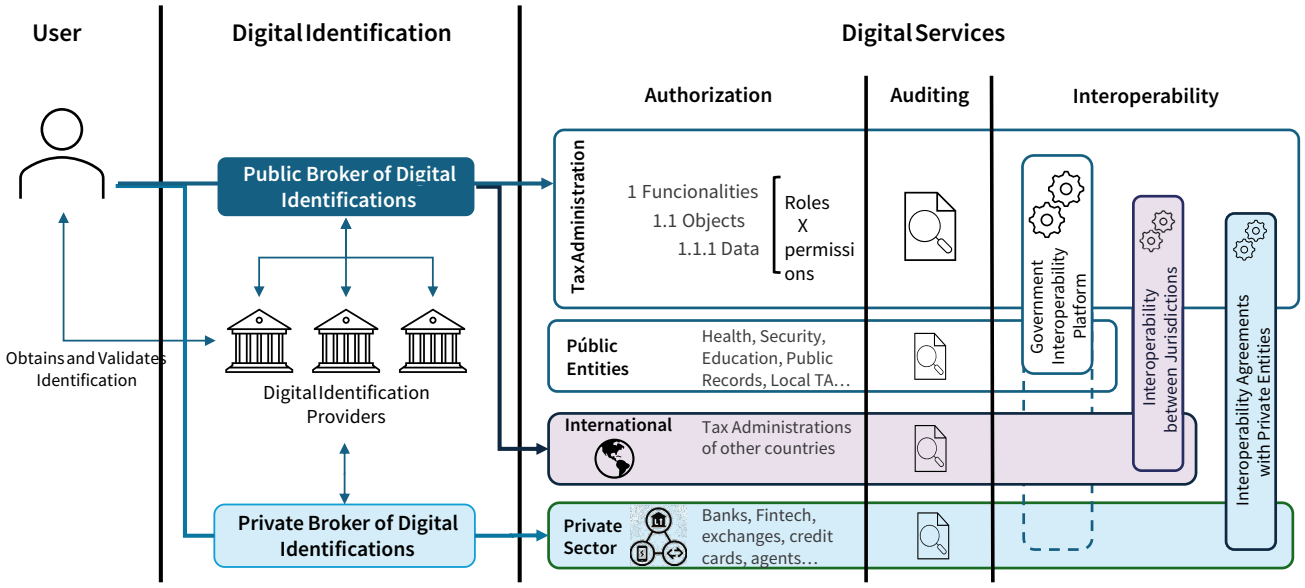
3.6. Integrated Model Diagram

In the CIAT publication, "ICT as a Strategic Tool to Enhance the Efficiency of Tax Administrations" (CIAT, 2020), in Chapter 10, section 10.1.7 "Internal Security in Information Systems and their Applications," three levels of role-based security are defined:

- Functional: permissions to grant access to the functional parts of the system within each process.
- Objects: managing permissions for access to objects; for example, within a taxpayer, specific permissions can be defined to access tax returns.
- Fields (data): This is the most granular permission and involves allowing access to a specific field or piece of data.

The above publication presents a very comprehensive diagram, modeled on use cases that have roles through which various permissions on functionalities, objects, and/or fields are defined, thus presenting a complete access management or authorization scheme. The following diagram shows the relationship between digital identification and an access control or authorization system based on the scheme in the above publication, continuing with auditing and then interoperability:

Figure 12. Diagram of the relationship between digital identification, access, auditing and interoperability.



Source: Prepared by the author

The following sections can be distinguished in the diagram above regarding the relationship between a user and the Tax Administration:

- **Digital identification providers:** a user obtains and validates their digital identification from a provider accredited or regulated by the ecosystem.
- **Digital identification:** a user digitally identifies themselves to a digital service. In this case, several scenarios are possible:
  - **Public digital identification broker:** this refers to a national ecosystem structured by a broker, as detailed above. In this case, the user could use one of the integrated identification methods to access the Tax Administration or another public body.

- **Cross-border digital identification:** this is the scenario outlined in Chapter 1.3, where it is possible to access digital services in another country using trusted digital identifications from their own country. In this way, the user accesses a Tax Administration in another country. In the above diagram, the broker in the other country is not shown to simplify matters; it is assumed to be part of the digital identification ecosystem.
- **Private digital ID brokers:** While this concept is recent, in some countries the national digital ID strategy, aimed at achieving greater nationwide reach, regulates the creation of brokers in the private sector. These brokers would include recognized ID providers (at least those with high levels of trust) and offer their integration to the private sector. While this could be resolved with a single national broker, separating the public and private sectors could reduce risk (the entire country wouldn't depend on a single piece of software for digital ID) and allow for the coexistence of different business models, making the ecosystem more sustainable. From the user's perspective, this would maintain the idea of using one or a few digital IDs for identification throughout the country (and beyond) because accredited ID providers would be present in all brokers.

- **Authorization:** Upon logging into the Tax Administration's services, the Tax Administration's Authorization system defines which functionalities, objects, and data the user will have permissions for, based on their associated roles. In turn, based on the permissions assigned to these roles, the system determines what the user can do with the associated functionalities, objects, and fields (create, delete, modify, view, remove, execute, approve, etc.). There must be accurate and up-to-date mapping between all functionalities, their associated objects, and the fields (data) involved in each case with each role and, in turn, what operations (permissions) each case allows. This is a complex but extremely powerful and flexible authorization system, designed to facilitate each user's operations while reducing risks related to information security. The reporting, alert, and checking tools that the Tax Administration develops for the Authorization system are fundamental to facilitating configuration and maintenance for each taxpayer. It is essential that each taxpayer maintain consistency between the roles assigned in the system and the actual functions performed by its users. Consequently, the addition of new staff (whether internal or outsourced), changes in position, or the termination of personnel must be reflected immediately in the Tax Administration's Authorization System. Keeping the Authorization System updated for each taxpayer is critical to protecting their information. The CIAT publication, "ICTs as a Strategic Tool to Enhance the Efficiency of Tax Administrations" (CIAT, 2020), in Chapter 10, section 10.1.7 "Internal Security in Information Systems and Their Applications," elaborates on this topic in much greater detail. Section 3.6 "Digital Identification and Tax Intelligence" briefly addresses some of the advantages that national identification, proper management of Authorizations and Audits, and interoperability can bring to tax intelligence.

- **Auditing:** This section highlights the importance of auditing within a tax administration, particularly considering the current trend of using digital identification for natural persons nationwide who enter the tax system in various roles across multiple taxpayers. While standards and best practices exist, auditing remains a matter specific to each organization.

- **Interoperability:** It is important to clarify that this topic is extremely complex and broad. This document only addresses it superficially, given that digital identification is an element that promotes more efficient or accurate interoperability. The diagram above shows the following configuration from the Tax Administrations:
    - **Government Interoperability Platform:** This is a cross-cutting platform across the State that resolves interoperability between public organizations. This platform can also include the private sector (dotted diagram), so interoperability can also be resolved at the national level from this platform.
    - **Interoperability between jurisdictions:** Interoperability between Tax Administrations is essential to strengthen international cooperation and tax control. The exchange of tax information through international agreements allows administrations to share data on taxpayers, financial transactions, and business structures. This exchange can be achieved through various mechanisms; however, the existence of national digital identification ecosystems, integrated under common standards, will be key to achieving more efficient and secure cross-border interoperability between administrations. This technical interoperability between countries is crucial for these agreements to translate into effective and legally valid operational capabilities.
    - **Interoperability agreements with private entities:** While agreements between the Tax Administration and various private actors (banks, Fintech companies, exchanges, credit card companies, payment hubs, etc.) should always exist, it is important that these agreements ultimately materialize through interoperability. This can be resolved in different ways regarding the technological solution: using the same government interoperability platform (shown in dotted lines in the diagram) or developing an interoperability platform between the Tax Administration and the private sector (shown in the diagram), or resolving point-to-point interoperability between the Tax Administration and each of the relevant actors.

From the perspective of the diagram above, which represents a user's workflow when performing a function related to a taxpayer within the Tax Administration, the standardization of digital identification at the national level is crucial. This standardization substantially influences subsequent processes and directly impacts the consistency of the various procedures within the Tax Administration.

It is essential that the national digital identification scheme be complemented by a robust authorization and auditing system within the Tax Administration.

3.7. Digital Identification and Tax Intelligence

Tax intelligence can be defined as fiscal intelligence applied to the tax field. In (CIAT, 2020), it is conceptualized as a fundamental function that a modern tax administration must create, autonomously, to transform data into useful information for decision-making. Its main objective is for the tax administration to know its taxpayers and be as predictive as possible regarding their present and future behavior, seeking to improve efficiency and fairness and minimize the risks of evasion and avoidance.

Data is a critical asset for all organizations today. Tax administrations are no exception and must leverage it to improve efficiency and effectiveness in all processes. This requires defining proper data governance but also developing other important factors that can be addressed based on the workflow that a user, on behalf of a taxpayer, performs with the Tax Administration.

Analyzing the integrated model diagram presented in Figure 12 of this publication, several stages can be identified along each user's workflow within the Tax Administration systems. Below are some factors that contribute to improved tax intelligence at each stage:

1. **Digital Identification:** Having a national ecosystem, ideally with cross-border interoperability, standardized and managed by a digital identification broker, offers numerous opportunities. The fact that all digital services identify each user with the same data and that this is mapped to each natural person means that it will be much easier to obtain and exchange information. Furthermore, robust identification methods contribute to greater confidence in the veracity of interoperable data, as they significantly reduce the risks associated with identity theft.

   On the other hand, digital identification not only facilitates the technical verification of who is behind a digital transaction but could also allow tax authorities to map corporate structures and reduce the use of shell companies, although it is obviously not infallible. Data such as legal name, date of birth, nationality, and residence could be reliably linked to corporate records in different jurisdictions, reducing the possibility of using front men or false identities. By requiring robust authentication methods (e.g., biometrics, MFA, digital certificates) for company formation or account opening, it would ensure that the person listed as a shareholder or director is indeed who they claim to be, or at least make it more difficult for someone to unknowingly act as a "front" to conceal the true Ultimate Beneficial Owner (UBO). Furthermore, if digital identification systems could interact with commercial, notarial, and banking registries, it would facilitate the cross-referencing of information to detect who truly controls a company. The Legal Entity Identifier (LEI), championed by the G20 and promoted by the OECD, can be very powerful when combined with digital identity, functioning as a unique and standardized identifier for legal entitys. Linking them would allow tax authorities to more accurately

map business and corporate relationships and identify beneficial owners. For example, if a company is registered with a unique LEI, and a natural person with a national digital identity opens a bank account for that company, by cross-referencing both sets of data, the tax authorities could identify the suspected ultimate beneficial owner (UBO), verify the legitimacy of the transaction, and detect links to other entities in different jurisdictions.

2. **Authorization:** A properly designed, developed, and updated authorization system, based on three-tiered role and permission management (functionality – objects – data), further enhances the wealth of data held by the Tax Administration. Furthermore, information related to authorizations (i.e., who accesses, modifies, or queries specific objects or data within tax systems) is a valuable input for uncovering functional, operational, and legal relationships between actors. These records allow for the identification of interaction patterns, internal hierarchies, delegations of responsibility, and indirect links that are not always evident in traditional tax data. In this sense, the "metadata" of the authorization system becomes a valuable element for tax intelligence, especially when integrated into relational network visualization analysis programs, completing the multi-layered picture of commercial and legal relationships. By incorporating this data, it is possible to enrich risk models and detect more complex evasion structures. Using more reliable and robust methods to manage authorization, such as those mentioned above (digital signatures with attributes and e-seals), further strengthens trust in the relationships between taxpayers and users acting on their behalf before the Tax Administration.

3. **Auditing:** Starting with national identification and authorization management, auditing allows for the precise tracking and determination of each user's activity for each taxpayer within the Tax Administration over time. It not only guarantees operational integrity but also provides valuable input for tax intelligence. Information derived from audit logs helps detect non-traditional patterns of behavior, such as access at unusual times, IP addresses originating from atypical jurisdictions, temporal correlations between critical events and specific actions, or anomalies in the logical sequence of operations. When integrated into analytical models, these elements enable the identification of atypical behavior and strengthen the capacity to detect suspicious transactions both within and outside the organization.

4. **Interoperability:** Mature data interoperability systems, generally developed and managed by the leading digital government organizations in each country, are a key element in the country's digital development. They should be addressed as a cross-cutting platform across the entire government, geared towards data interoperability, while complying with information security and privacy guidelines. Regulations are needed in this area, not only an Information Privacy Law. Also, regulations governing data exchange in certain situations are needed, subject to certain guarantees and the consent of their owners, as well as clear data governance at the national level. Each organization integrates into the interoperability

platform and exposes its data in a secure, controlled, and reliable manner, while also being able to access and obtain data from other organizations. It is not the objective of this Guide to analyze interoperability in detail, but it is a relevant topic for the Tax Administration's interests, as interoperability allows the Tax Administration to access information from civil registries, customs, social security, land registries, production registries, and more. This enriches the user experience by allowing for smoother interaction with the administration, but also, with the appropriate consent, it can enhance the taxpayer's profile and enable the detection of inconsistencies or risks.

Developing a robust tax intelligence system requires solid and well-structured foundations. These include standardized digital identification at the national level (preferably with cross-border capabilities), authorization and auditing systems, data governance and quality, and cross-country interoperability.

Proper management and quality assurance of the data generated by the various processes of the Tax Administration are essential to meeting its institutional objectives. When this data is reliable, it enhances the agency's analytical, operational, and strategic capabilities.

In this context, Artificial Intelligence tools currently offer disruptive and unique opportunities to improve compliance management, risk detection, and decision-making. However, their effectiveness depends directly on the strength of the above pillars: without reliable digital identification, well-designed authorization systems, adequate auditing, and data governance, the benefits of AI cannot be maximized or sustained over time.

3.8. Conclusions

In a world where daily activities increasingly depend on Information and Communication Technologies (ICTs), and where cyber threats have grown exponentially, protecting our digital identity and having robust, simple, and secure identification methods is critical.

Traditional digital identification methods are becoming obsolete, regardless of the factors included. These methods are also costly and difficult to use. One of the main vulnerabilities is that these methods, based on the identifier/verification pairing (generally username and password), use a centralized database with millions of user credentials. Another is that managing strong passwords is inconvenient for users.

Biometric tools have greatly improved their accuracy, and with the widespread use of smartphones, they have become very popular for validating identities or digital identification. However, these methods generate some friction; to be more reliable, they should interact with public records, and they incur considerable costs.

Additionally, they are currently threatened by Artificial Intelligence, although it is not possible to know exactly what will happen soon, AI may be able to deceive biometric tools and liveness detection.

There is a need to rapidly evolve towards digital signature-based identification methods, with all the trust that a Public Key Infrastructure (PKI) implies, where, moreover, the keys are distributed and held by the owner. The keys are on a cryptographic device and never leave it, so there is no centralized database with millions of user credentials.

Cloud-based digital signatures are a very good solution that leverages the advantages of digital signatures and simplifies their use. However, Verifiable Credentials are undoubtedly the method that will truly scale signature-based digital identification on a massive scale. Verifiable Credentials have several advantages: identification based on digital signatures, distributed credentials, public key infrastructure for trust and privacy protection. In addition, they are very easy and intuitive to use and can also be used to identify yourself in person with complete ease and confidence. It is a reliable and robust form of identification used both in person and digitally.

Another trend that has been developing for years is that digital IDs are beginning to behave like physical IDs; that is, natural persons obtain a digital ID from a trusted provider and use it across multiple systems. This greatly simplifies ID management for natural persons. We are currently in a transition phase, where natural person IDs are disappearing in each digital service, replaced by systems or ecosystems at the national level. Cross-border digital IDs are already a reality in the European Union, and in Latin America and the Caribbean, there is an initiative encompassing 13 countries within the Inter-American Digital Government Network.

This new scenario will enable national systems or ecosystems to interoperate, so that natural persons can use their trusted digital ID not only to identify themselves in digital services within their own country, but also in other countries, reducing costs and time, simplifying use, increasing inclusion, and generating greater trust.

Tax administrations play a strategic role within a country's digital ecosystem, so it is important that they support and integrate with national digital identification systems or ecosystems. As discussed in Chapter 2, the taxpayers-tax administration relationship is, in practice, predominantly digital. Some countries have moved toward multichannel models, which not only consolidate their status as digital tax administrations but also optimizes the taxpayer experience.

Integrating tax administration services into national digital identification systems or ecosystems offers several advantages. These include the ability for taxpayers to access tax services just as they do other public

services. Furthermore, they will benefit from all the country's investments in security (such as continuous authentication managed by the digital identification broker) and as new digital identification methods are added, such as the use of verifiable credentials, without having to make their own investments.

In some cases, tax administrations may also consider decoupling their digital identification system and integrating it into the national ecosystem as a provider under certain conditions, allowing taxpayers to use their tax administration identification to access other digital public services.

In this context, where tax administrations delegate digital identification to another trusted provider, it is necessary to rethink and design an authorization system based on roles and permissions at three levels: functions, objects, and data. Natural persons will be identified as a natural person before the Tax Administration and will have roles that associate them with taxpayers and provide them with certain permissions at these three levels.

Another critical issue is Auditing. With many users acting in roles associated with taxpayers, it is essential to have an auditing system that accurately determines who performed each action, from where, and when. This is important for preserving or restoring the integrity of information, having reliable evidence in cases of fraud or legal proceedings, and contributing quality data to tax intelligence systems.

Finally, given that the relationship between taxpayers and the Tax Administration is digital, administrative processes should be designed as "digital by default," under a multichannel strategy that facilitates and simplifies interaction with taxpayers in a uniform and standardized manner, regardless of the channel used, achieving high levels of satisfaction, trust, and transparency.

3.9. Roadmap

The objective of this section is to present an evolutionary roadmap from the perspective of digital identification, while also considering other relevant and associated factors such as authorization, auditing, and interoperability within tax administrations.

Based on the current situation of the tax administrations analyzed in Chapter 2, the roadmap specifies two distinct alternatives: one for a scenario where no national digital identification system or ecosystem exists, and another for countries that have ongoing digital identification initiatives, regardless of whether the tax administration is integrated.

Digital identification	
Scenario without national identification	**Scenario with national identification**
Redesign the digital identification system to identify natural persons (not companies) who will be acting in different roles within each company. Choose a minimalist and universal dataset to identify natural persons: • Minimalist to protect data privacy. • Universal because in the future it will be relevant to be able to identify a person beyond the context of tax administration and country. Example: country code – document code – document number. Carry out the necessary technological developments and adaptations so that the systems are based on identifying natural persons. It is important that this system coexists with the current one and gradually replaces it. The new identification system must be unique for all systems and all taxpayers, acting as a Single Sign On across all Tax Administration solutions.	Redesign the identification system by delegating identification to the national system or ecosystem, assuming that only natural persons will be identified. National identification can be incorporated as an alternative to that of the Tax Administration, and gradually, all revenues will be required to be registered through the national system or ecosystem until 100% is reached. Make the necessary adjustments to adapt to the national digital identification (for example, in identity data) and the required technological developments.

Strengthen digital identification (short term):
 	
• All tax administration functionalities should require digital identification across all channels.
 	
• All digital identifications should ensure the use of a strong password and a two-factor authentication method. It is recommended, at a minimum, to enable an authentication application and the option to receive it via email (other options are described in Chapter 1.3).
 	
• Develop Continuous Authentication functionalities (Chapter 1.2) based on risk management such as trusted device management, integration with Security Operation Center (analysis of security events linked to digital identification), etc.
	Strengthen digital identification (short term):
	
	• All access to Tax Administration functionalities should require digital identification across all channels.
	
	• Support the organization responsible for the national digital identification system or ecosystem to strengthen digital identification:
	
	  ○ At a minimum, a strong password and a two-factor authentication method.
	
	  ○ The national system or ecosystem should develop Continuous Authentication functionalities (Chapter 1.2) based on risk management, such as trusted device management, integration with the Security Operations Center (analysis of security events related to digital identification), etc.

<table>
<tr><th colspan="2">Digital identification</th></tr>
<tr><th>Scenario without national identification</th><th>Scenario with national identification</th></tr>
<tr><td></td><td>If the national digital identification system or ecosystem does not progress according to the Tax Administration's requirements, the Tax Administration could develop some complementary actions, such as a mandatory two-factor authentication method after accessing the Tax Administration website and requirements related to the concept of Continuous Authentication.</td></tr>
<tr><td>Resilience in digital identification:
Implement digital identification methods based on digital signatures. This involves implementing a Public Key Infrastructure (or entering into an agreement with specialized public or private organizations) to provide each user with a digital signature-based method, on a token or smart card, as discussed in Chapter 3.1.
Develop standards and requirements for reliable digital identification methods based on digital signatures.
In the long term: implement quantum-resistant encryption algorithms for the Tax Administration's public key infrastructure and distribute new post-quantum certificates and signature keys to taxpayers. The algorithms are detailed in the NIST publication, "Post-Quantum Cryptography" (NIST, updated 11/19/2025).</td><td>Tax Administration as a Digital Identification Provider in the National Digital Identification Ecosystem:

If deemed appropriate (by the Tax Administration and the governing body of the national ecosystem), the Tax Administration may act as a digital identification provider.

This entails developing and potentially strengthening capabilities so that the Tax Administration's digital identification system can be integrated into the national ecosystem using one of the protocols defined by the national ecosystem (such as OpenID Connect or SAML).</td></tr>
<tr><th colspan="2">Access control</th></tr>
<tr><td colspan="2">Redesign the access control system so that natural persons logging in with their digital identity can act in different roles within the company:
Define roles, for example: Owner, manager, accountant, lawyer, administrator, etc.
Define operations (creation, deletion, modification, editing, reading, execution, etc.).
Define functionalities for each of the Tax Administration's processes and for the taxpayer's compliance cycle.
Link Roles – Operations – Functionalities.
In this first stage, the role system could focus on functionalities.</td></tr>
</table>

Digital identification	
Access control	
Expand and enhance managed access control at the object and data level: • Identify the objects for each function, defining the possible operations in each case. • Considering data governance, associate data with objects and roles. Develop the necessary components to implement access control at all three levels.	
Develop reports and alert systems to facilitate user access control, particularly for company managers. In a complex environment where numerous users will access the Tax Administration to perform various operations at different levels (functions, objects, and data) on behalf of various taxpayers, whether natural persons or legal entitys, it is necessary to develop functionalities that allow the responsible parties or owners in each case to easily manage access, roles, and users. An intelligent system of approvals, verifications, and alerts can be useful in preventing errors and/or fraud.	
Auditing	**Interoperability**
Redesign a comprehensive and detailed audit system that records all user activity, as detailed in section 3.5. Consider developing a complete audit system and using it to feed an anonymized data source for statistical purposes. Auditing information should be considered sensitive and therefore requires tools and techniques to protect its confidentiality.	While interoperability does not depend solely on the Tax Administration, if other organizations possess the capabilities to enable interoperability with the Tax Administration, it is suggested to move forward along three lines (according to the diagram in Figure 12 of Chapter 3.6): • Interoperability in the Public Sector: Integrate into the public sector interoperability platform, actively participating in its evolution by defining requirements and data access in conjunction with the governing body for Digital Government. • Interoperability between jurisdictions: Within the framework of tax information exchange agreements, both bilateral and multilateral, work on generating effective operational capabilities so that international audits are based on reliable, traceable, and legally valid evidence. • Interoperability with the private sector: Establish agreements and develop interoperability with relevant private operators such as banks, Fintech companies, exchanges, credit card companies, etc. • Social: Although not specified in the diagram in Figure 12 of Chapter 3.6, it may be important to interact with social media to obtain information of interest.

Digital identification
Tax intelligence

As the points mentioned above progress, along with other factors, tax intelligence can be refined and enhanced, positively impacting cost and time savings, transparency, fairness, and revenue collection, among other things.
 	
In general terms, to achieve a mature and sophisticated tax intelligence scenario, the following points must be considered:
 	
• Infrastructure.
 	
• Information: incorporating information sources such as digital identification, access control, auditing, other internal sources, and sources accessible as discussed previously regarding interoperability.
 	
• Structured data lakes (centralized data repositories) for performing different types of analysis.
 	
• Data governance and quality: related to the above, it is important that data governance is clearly defined and that policies, tools, and techniques are in place to ensure a high level of data quality.
 	
• Data analysis tools, in some cases using Artificial Intelligence, such as:
 	
  ○ Tools that analyze data in real time and automatically.
 	
  ○ Tools that allow the generation of analytical models for risk and taxpayer segmentation.
 	
  ○ Compliance and predictive models.
 	
  ○ Tools for developing controls, alerts, or anomaly detection.
 	
  ○ RPA (Robotic Process Automation) tools could be used for non-deterministic decisions, based on machine learning.
 	
  ○ Geospatial tools, for example, for taxes related to the identification of luxury goods on land.

The table above does not establish precedence or dependency relationships; that is, achieving a “resilient” level in digital identification is not a prerequisite for progress in areas such as auditing, interoperability, or tax intelligence. The primary focus of this document is digital identification within tax administrations; other relevant aspects are presented in a general manner, and therefore, not all elements necessary for a comprehensive approach may be included.

Glossary and Abbreviations

Term	Definition
AAL	Authenticator Assurance Level, authentication strength level. Used in ISO/IEC 29115 and NIST to define security levels in authentication.
ABAC	Attribute-Based Access Control (ABC). It is an access control model where decisions (allow or deny) are made based on attributes of the user, the resource, the environment, and the action, rather than relying solely on fixed roles.
AECID	Spanish Agency for International Development Cooperation.
ANSI	American National Standards Institute (ANSI). It is a US organization that coordinates the development of national standards for multiple industries: technology, security, telecommunications, engineering, healthcare, manufacturing, etc.
API	Application Programming Interface (API). An API is an interface that allows two programs or systems to communicate with each other easily and securely.
Authentication	The process of verifying the identity of a person, system, or device. In other words, it serves to ensure that someone is who they claim to be. This can be done using a password, a fingerprint, a biometric comparison of a facial image, among other factors.
IDB	Inter-American Development Bank.
Blockchain	It is a distributed ledger technology that allows information to be stored securely, immutably, transparently, and without the need for a central intermediary.
Bluetooth	It is a short-range wireless communication standard that enables data transmission between electronic devices using radio waves in the 2.4 GHz band. Its main objective is to facilitate wireless connectivity, ensuring interoperability between equipment from different manufacturers.
Digital ID Broker	A software system that positions itself between digital services and recognized ID providers within its ecosystem. In this way, one or more providers integrate with the broker, and many digital services use the broker to offer their users different digital identification methods.
Digital channels	These are all the online media or platforms used to communicate, interact, or conduct business over the internet, such as websites, email, social media, WhatsApp, and others.
Chatbots	It is a program or system that can simulate a conversation with people, either through text or voice. Its purpose is to answer questions, help with tasks, or provide information, all automatically, generally based on the use of artificial intelligence.
Biometric facial image comparison	These are specialized algorithms for comparing two images. Applied to digital identification, if the system has access to a photo of a person's face, either previously registered or obtained from a public registry, a facial image can be taken and compared to the one in the prior record. This technique can be used to validate a person's identity, like fingerprint comparison.

Term	Definition
Access control	Once a person has digitally identified themselves, a computer system has a mechanism to determine what information and functionalities they can access, based on the trust level of the digital identification used and their roles within the organization.
Single account	Equivalent to a "National Digital Identification," in some countries a single digital identification (possibly a username/password) used to access multiple digital services in the public sector is often called a "single account."
CIAT	Spanish acronym for Inter-American Center of Tax Administrations.
DAC	Discretionary Access Control (DAC) is an access control model where the owner of a resource (file, record, database, document) has the ability to delegate permissions to other users.
Data lakes	A centralized repository thatRPA stores large volumes of raw (unprocessed) data, as it arrives from multiple sources: databases, applications, logs, sensors, APIs, IoT devices, etc.
Deepfake	This is audiovisual content manipulated using artificial intelligence, generally deep neural networks, to alter a person's appearance, voice, or actions, making it seem real, even though it is fake.
DID	Decentralized Identifiers (DIDs) are a new type of digital identifier designed to enable sovereign, decentralized, and interoperable identity, without relying on a central provider (government, company, platform).
Trusted devices	In the context of digital identification, many computer systems have developed functionality for users to manage their trusted devices. When a user logs into the system with their computer or mobile device, the system obtains a device fingerprint (identifying information) and allows the user to save it associated with their digital identity as a trusted device. This means that each time the user logs in with a trusted device, the system might not require a second authentication factor, assuming there is less risk since it is the device the user commonly uses to log in.
eIDAS	European Regulation on Digital Identity, Trust Services and Electronic Transactions. It defines how digital identities, electronic signatures, seals, certificates and trust services should function in the European Union.
FAL	Federation Assurance Level. Level of trust in the token in a federated authentication system. Used in ISO/IEC 29115 and by NIST to define the levels of trust between identity providers in a federated authentication system.
FIDO	Fast IDentity Online, it is an international standard for strong passwordless authentication, designed to replace traditional keys with more secure, faster, and phishing-resistant methods.
FIPS	Federal Information Processing Standards. These are technical and security standards published by NIST (National Institute of Standards and Technology) of the United States.
G20	An international forum that brings together the world's 20 largest economies to coordinate economic, financial and strategic policies at a global level.
Digital Government	Digital government is the use of digital technologies (such as the internet, applications, online platforms, artificial intelligence, etc.) to enable governments to provide services, communicate with citizens, and manage processes more efficiently, transparently, and accessibly.

Term	Definition
Google Authenticator	It's a free Google mobile app used to generate OTPs (One-Time Passwords). This app is configured with the computer system, synchronizing algorithms to generate one-time passwords so that when the user enters the second authentication factor, they enter the code provided by Google Authenticator, which should match the code the computer system expects to validate their identity.
GPS	Global Positioning System. A worldwide satellite navigation system that allows the determination of the geographic position of an object or person anywhere on the planet with high precision.
Hash	It is the result of applying a hash function, that is, a cryptographic algorithm that converts any data (text, file, password, transaction, etc.) into a fixed string of characters.
HSM	Hardware Security Module. A specialized physical device designed to securely protect and manage cryptographic keys. It is used to perform critical operations such as encryption, decryption, key generation, and storage, ensuring high levels of security against unauthorized access.
HTML	HyperText Markup Language. It is the standard language that defines the structure of all web pages on the Internet.
IAL	Identity Assurance Level. A level of identity verification. Used in ISO/IEC 29115 and NIST to define security levels in digital identification.
ICAO	The International Civil Aviation Organization (ICAO) is a specialized agency of the United Nations responsible for regulating, coordinating, and standardizing international civil aviation, including matters of air safety, travel documentation, and electronic passports.
Digital Identification in Tax Administration	System for digital identification within the Tax Administration's computer systems (possibly username/password).
National Digital Identification	This refers to a unified digital identification system where users employ a single identifier (possibly username/password) to access multiple computer systems across the public sector.
IdLAC	Digital Identification Model for Latin America and the Caribbean.
IETF	The Internet Engineering Task Force is the international organization responsible for developing and standardizing the technical protocols that make the Internet work.
Public Key Infrastructure	Public Key Infrastructure (PKI) is the set of technologies, processes, and entities that enable the use of public-key cryptography to: • authenticate identity, • digitally sign documents, • encrypt and decrypt information, • ensure integrity and non-repudiation. It is the technical foundation for digital signatures, electronic certificates, electronic passports, eID, HTTPS, digital banking, digital government, and more.

Term	Definition
ISO	The International Organization for Standardization (ISO) is the global body that develops and publishes international standards for nearly every industry: technology, quality, health, safety, environment, energy, production, logistics, and more.
ITU	The International Telecommunication Union (ITU) is an official dictionary of technical terms in telecommunications and information technology, available in several languages and constantly updated.
JSON	JavaScript Object Notation (JOB). A lightweight, text-based data interchange format that is easy for humans to read and write, and simple for machines to process. It is widely used to structure information into key-value pairs and ordered lists, facilitating communication between systems and applications.
keyloggers	A malicious program or physical device designed to record every keystroke a person types on a keyboard (computer, tablet, or cell phone), usually without the victim's knowledge.
LEI	A Legal Entity Identifier (LEI) is a 20-character globally unique identifier used to identify legal entities participating in financial transactions worldwide.
MAC	Mandatory Access Control (MAC) is one of the strictest access control models, used when security must be centralized, rigid, and non-delegable.
Malware	Malware is a term that encompasses any type of malicious software designed to damage, disrupt, or steal information from a computer system or device. The word comes from "malicious software" and refers to programs created for harmful or criminal purposes.
MFA	Multi-Factor Authentication (MFA) is an authentication method that requires two or more independent factors to verify a user's identity before granting access.
NFC	Near Field Communication (NFC) is a short-range wireless communication technology that allows two devices to communicate with each other simply by bringing them close together (within a few centimeters).
NIST	National Institute of Standards and Technology (United States).
Security levels	In the context of digital identification, this refers to the varying degrees of security or trust that can be associated with the use of digital IDs. A low level of trust occurs when someone uses an ID that has not been validated, while a higher level of trust is achieved when someone uses an ID that has been validated by a third party and employs a second authentication factor, meaning the computer system the person is accessing has a high degree of confidence in that digital ID.
NTP	Network Time Protocol. It is a protocol that allows synchronizing the exact time between computers, servers, and devices across a network.
OECD	Organisation for Economic Co-operation and Development.
OAS	Organization of American States.
OIDC	OpenID Connect is a modern authentication standard that allows a user to log in to an application using an identity managed by another provider.
OIDC4VC	OpenID Connect for Verifiable Credentials is an extension of OIDC that allows users to issue and send verifiable credentials to a digital wallet on their mobile phone.

Term	Definition
OIDC4VP	OpenID Connect for Verifiable Presentations is an extension of the OIDC standard that allows users to present verifiable credentials from digital wallets as a method of digital identification.
OTP	“One-Time Password” or “One-Time Code.” It is used as a second authentication factor. The computer system generates a one-time code and sends it to the user through a means known to both parties (email, SMS, WhatsApp, etc.). The user receives it through another means and enters it into the system. If the code is entered correctly, the user is verified.
Passkeys	Trade name of the passwordless authentication technology based on FIDO2 + WebAuthn standards, created to definitively replace traditional passwords.
Passwordless	Passwordless authentication model, where users access systems using more secure and simpler methods such as biometrics, cryptographic keys, or verification links, instead of memorizing and typing passwords.
Phishing	It is a deceptive technique used by cybercriminals to steal personal information such as passwords, bank data, credit card information, or even access to social media accounts, emails, or other sensitive data.
PKI	Public Key Infrastructure (PKI) is a set of technologies, policies, entities, and procedures that enable secure and reliable issuance, management, distribution, and revocation of digital certificates and cryptographic keys.
Identification providers	An organization that complies with specific regulations and provides digital identification to users. Natural persons visit this recognized organization to obtain and validate their username, create their password, and register their contact information. They then use this identification to access computer systems.
QR	Quick Response code, it is a type of two-dimensional barcode that can store information in a pattern of black and white dots.
Quishing	It is a form of phishing that uses QR codes to trick people into going to malicious sites, stealing credentials, or infecting devices.
RBAC	Role-Based Access Control. It is one of the most widely used access control models in businesses, governments, and computer systems, where access to objects is defined based on roles and users are associated with roles.
Red Gealc	Electronic Government Network in Latin America and the Caribbean. A network to promote cooperation among countries for the development of Digital Government.
RFID	Radio Frequency Identification. Automatic identification technology that uses radio waves to transmit data between a reader and a tag or electronic device. It allows for the recognition, tracking, and management of objects or people without the need for physical contact or direct line of sight.
RPA	Robotic Process Automation. Technology for Robotic Process Automation.
Second factor authentication (2FA)	The user digitally identifies themselves with their identifier (document number, email, etc.), then enters a first authentication factor (such as a password), and subsequently, the system requires a second factor. This is generally implemented by sending a one-time code to their mobile device (SMS, WhatsApp, or similar) or to their email address, but other methods are possible. Currently, two-factor authentication (2FA) is considered essential for strengthening digital identification.

Term	Definition
SAML	Security Assertion Markup Language (SAM). It is an identity authentication and federation standard that allows a user to log in to a system using an identity managed by another provider.
SIEM	Security Information and Event Management (SIEM) is a cybersecurity platform that centralizes, correlates, and analyzes events from multiple systems to detect threats, respond to incidents, and comply with auditing standards.
Single Sign-On (SSO)	Single sign-on (SSO) is an authentication mechanism that allows a user to access multiple applications, systems, or services with a single credential (username and password, certificate, token, etc.). Once the user's identity is validated on the primary system, they do not need to re-authenticate on each linked application.
Smishing	SMS phishing is a type of SMS phishing. The attacker sends a fake text message to trick the victim.
SMS	Short Message Service (SMS) is the standard text messaging service that allows sending and receiving short messages between mobile phones.
SOC	Security Operations Center (SOC) is the central hub for an organization's security operations. It is a specialized team —with personnel, processes and technology— responsible for monitoring, detecting, analyzing and responding to cybersecurity incidents in real time.
Brute force techniques	A cybersecurity attack method that involves systematically trying all possible combinations of credentials (such as passwords or cryptographic keys) until the correct one is found.
Cleartext	A data representation format that contains only human-readable characters, without any formatting, style, special encoding, or multimedia elements.
Timestamping	Timestamping is a cryptographic mechanism that allows you to prove when a digital event occurred, without the possibility of alteration. It serves to prove that a document, file, transaction, or data existed at a specific moment and was not modified afterward and consists of sealing a document by stamping it with a timestamp from an authorized timestamp authority.
Physical Token	It is a physical device that generates OTPs. It is configured by synchronizing with the computer system, so that both generate the same one-time passcode within a specific time. Therefore, when the user enters the second authentication factor, they enter the code indicated by the physical token, which should be the same code the application expects. In that case, the user's identity is validated.
TOTP	A time-based one-time password is a method of two-factor authentication (2FA) or multi-factor authentication (MFA).
UBO	Ultimate Beneficial Owner (UBO) is the natural person who ultimately owns, controls, or benefits from a business, bank account, trust, foundation, or other legal structure.
EU	European Union.
URI	Uniform Resource Identifier (URI) is a standard identifier used on the Internet to name, locate, or identify a resource, whether it is a web page, a file, a service, a user, a DID, etc.
Usability	Ease of use of a computer system.

Term	Definition
USB	Universal Serial Bus. It is a physical connection and communication standard used to connect devices (computers, phones, keyboards, cameras, flash drives, etc.) and transfer power and data simply and universally.
Vishing	It is a type of voice phishing, where the attacker uses phone calls (traditional or VoIP) to trick a person into handing over personal data, credentials, MFA codes, banking information, or making payments.
W3C	World Wide Web Consortium is an international organization that defines the technical standards of the Web.
XML	eXtensible Markup Language. It is a markup language designed to store, structure, and transport data in an organized, readable, and standardized way.

References

Agency for Electronic Government, Information Society, and Knowledge. (n.d.). ID Uruguay. https://www.gub.uy/agencia-gobierno-electronico-sociedad-informacion-conocimiento/id-uruguay

Bray, T. (2017). *The JavaScript Object Notation (JSON) data interchange format (RFC 8259).* RFC Editor. https://www.rfc-editor.org/rfc/rfc8259

CIAT. (2020). *ICTs as a strategic tool to enhance the efficiency of tax administration*. https://biblioteca.ciat.org/opac/book/5731

CIAT. (2025). *How company data can "talk" to each other: The Legal Entity Identifier (LEI)* (Nuria Vegas). https://ciat.org/ciatblog-how-companies-data-can-talk-to-each-other-the-legal-entity-identifier-lei-a-g20-initiative-for-transparency-and-efficiency-in-international-transactions/

Electronic Certification Unit. (2023). *First use case of cross-border digital identification between Brazil and Uruguay*. https://www.gub.uy/unidad-certificacion-electronica/comunicacion/noticias/primer-caso-uso-identificacion-digital-transfronteriza-entre-brasil-uruguay

Energy and Water Services Regulatory Unit. (n.d.). *Procedures and services available for Brazilian identifications*. https://www.gub.uy/unidad-reguladora-servicios-energia-agua/tramites-y-servicios/tramites

European Union. (2014). Regulation (EU) No 910/2014 on electronic identification and trust services for electronic transactions in the internal market (eIDAS Regulation). *Official Journal of the European Union*. https://eur-lex.europa.eu/eli/reg/2014/910/oj

European Union. (2014). *eIDAS Regulation on electronic identification and trust services for electronic transactions in the internal market*. https://digital-strategy.ec.europa.eu/es/policies/eidas-regulation

European Union. (2024). Regulation (EU) 2024/1183 on electronic identification and trust services for electronic transactions in the internal market (eIDAS Regulation 2.0). *Official Journal of the European Union*. https://eur-lex.europa.eu/eli/reg/2024/1183/oj

European Union. (2024). *European Digital Identity Framework*. https://eur-lex.europa.eu/eli/reg/2024/1183/oj

European Union. (n.d.). *European Digital Identity (eID).* https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/european-digital-identity_es

European Commission. (n.d.). *eID – Electronic identification.* https://ec.europa.eu/digital-building-blocks/sites/display/DIGITAL/eID

European Commission. (n.d.). *European digital identity.* https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/european-digital-identity_es

European Commission. (n.d.). *EU Login: Log in with your eID.* https://ecas.ec.europa.eu/cas/login?loginRequestId

Federal Government of Brazil. (n.d.). *Gov.br – Single portal of the federal government.* https://www.gov.br/pt-br

FIDO Alliance. (n.d.). *FIDO Alliance.* https://fidoalliance.org/

FIDO Alliance. (n.d.). *FIDO authentication: A passwordless vision.* https://fidoalliance.org/fido2/

Fusillo, M. (2021, May 12). *The 10 principles of self-sovereign identity. Self-Sovereign Identity.* https://www.selfsovereignidentity.it/los-10-principios-de-la-self-soveregn-identity/

Inter-American Development Bank. (2023). *Digital Maturity Index: How to Measure the Progress of Digital Transformation in Tax Administrations.* https://blogs.iadb.org/gestion-fiscal/es/indice-de-madurez-digital-como-medir-el-avance-de-la-transformacion-digital-en-las-administraciones-tributarias/

International Civil Aviation Organization. (n.d.). *Document 9303 – Machine readable travel documents.* https://www.icao.int/publications/doc-series/doc-9303

International Organization for Standardization. (2012). *Guidelines for identification, collection, acquisition and preservation of digital evidence (ISO/IEC 27037:2012).* https://www.iso.org/standard/44381.html

International Organization for Standardization. (2013*). Information technology — Security techniques — Entity authentication assurance framework (ISO/IEC 29115:2013, revised* 2020). https://www.iso.org/es/contents/data/standard/04/51/45138.html

International Telecommunication Union. (n.d.). *ICT indicators for the SDGs.* https://www.itu.int/en/ITU-D/Statistics/Pages/SDGs-ITU-ICT-indicators.aspx

Latin American and Caribbean Electronic Government Network. (n.d.). *Official website of the GEALC Network*. https://www.redgealc.org/

Lodderstedt, T., Yasuda, K., Looker, T., & Bastian, P. (2023, July 13). *OpenID for verifiable presentations 1.0. OpenID Foundation*. https://openid.net/specs/openid-4-verifiable-presentations-1_0.html

Lodderstedt, T., Yasuda, K., Looker, T., & Bastian, P. (2025, September 16). *OpenID for verifiable credential issuance 1.0. OpenID Foundation.* https://openid.net/specs/openid-4-verifiable-credential-issuance-1_0.html

M'Raihi, D., Machani, S., Pei, M., & Rydell, J. (2011). *TOTP: Time-based one-time password algorithm (RFC 6238). Internet Engineering Task Force.* https://doi.org/10.17487/RFC6238

Ministry of Public Health of Uruguay. (n.d.). *Application for certificates for the transport of yerba mate.* https://www.gub.uy/tramites/solicitud-constancias-transporte-yerba-mate

National Institute of Standards and Technology. (2017). *Digital identity guidelines (NIST Special Publication 800-63).* https://www.nist.gov/itl/applied-cybersecurity/special-publication-800-63

National Institute of Standards and Technology. (n.d.). *Federal Information Processing Standards (FIPS) publications.*

National Institute of Standards and Technology. (n.d.). *Digital identity guidelines (NIST SP 800-63-4)*. https://pages.nist.gov/800-63-4/

National Institute of Standards and Technology. (2025). *Post-quantum cryptography (Updated 19/11/2025)*. https://csrc.nist.gov/Projects/post-quantum-cryptography/post-quantum-cryptography-standardization/round-3-submissions

OECD. (2020). *Tax Administration 3.0: The Digital Transformation of Tax Administration.* http://www.oecd.org/tax/forum-on-tax-administration/publications-and-products/taxadministration-3-0-the-digital-transformation-of-tax-administration.htm

OECD. (2024). *Tax Administration: Comparative Information on OECD Countries and Other Advanced and Emerging Economies.* https://www.oecd.org/es/publications/administracion-tributaria-2024_ac2f5866-es.html

OECD. (2025). *Tax administration digitalization and digital transformation initiatives.* https://www.oecd.org/en/publications/tax-administration-digitalisation-and-digital-transformation-initiatives_c076d776-en/full-report.html

OpenID Foundation. (2014). *OpenID Connect core specification*. https://openid.net/

OpenID Foundation. (2023). *OpenID for verifiable credentials (OpenID4VC).* https://openid.net/sg/openid4vc/

Organization for the Advancement of Structured Information Standards. (2005). *Security assertion markup language (SAML) V2.0*. https://www.oasis-open.org/standard/saml/

Presidency of the Argentine Nation. (n.d.). *Autenticar.* https://www.argentina.gob.ar/jefatura/innovacion/autenticar

Resnick, P. (2008). *Internet message format (RFC 5322). Internet Engineering Task Force.* https://doi.org/10.17487/RFC5322

Sporny, M., Longley, D., & Lindström, N. (2023, October 3). *Verifiable credentials data model v2.0. World Wide Web Consortium (W3C)*. https://www.w3.org/TR/vc-data-model-2.0/

Uruguay's Single Window for Foreign Trade (VUCE). (n.d.). *Single Window for Foreign Trade.* https://vuce.gub.uy

Verified Market Reports. (n.d.). *NFC-enabled handsets market.* https://www.verifiedmarketreports.com/product/nfc-enabled-handsets-market/

World Economic Forum. (2025). *The global risks report 2025.* https://www.weforum.org/publications/global-risks-report-2025/

World Economic Forum. (2025). *Global cybersecurity outlook 2025.* https://www.weforum.org/publications/global-cybersecurity-outlook-2025/

World Wide Web Consortium. (2008). *Extensible markup language (XML) 1.0* (Fifth edition). https://www.w3.org/TR/REC-xml/

World Wide Web Consortium. (n.d.). *World Wide Web Consortium (W3C*). https://www.w3.org/

Annex I: Evaluation Survey

This appendix presents the form used for the information gathering survey of Tax Administrations.

Tax Administration Data

Please complete the following table:

Regarding tax administration
Name
Country
Web portal
Responsible party in tax administration for the questionnaire
Name
Position
Phone Number
Email
Leader in information technology
Name
Position
Phone Number
Email

Section A. National Digital Identification

This section is intended to gather information on digital identification at the national level. If your country does not have an initiative (regardless of its level of development) in this regard, please continue to section B.

Which organization oversees the national digital identification system?	
Which organization oversees the national digital identification system?	
Please enter the link to the organization's website:	
Which organization implements the national digital ID? (If it's the same as the governing body, you can skip this question)	
Please enter the link to the national digital identification system.	
Please enter a link to the national digital identification regulations.	

Use and characteristics of the national digital identification	
Status of national digital identification regarding the integration of public digital services (please mark the correct option in bold).	1. There is an initiative that has not yet been implemented. 2. There is an initiative underway, integrated into very few digital services. 3. There is an initiative underway, integrated into many digital services, but less than 50%. 4. There is an initiative underway, integrated into most digital services. 5. Digital identification is integrated into all public digital services.
Providers of digital IDs available in the national digital ID system (please mark the correct option in bold).	1. There is only one "single account" provider, and there are no plans to integrate new providers. 2. There is only one "single account" provider, and there are plans to integrate new providers. 3. More than one digital identification provider is available in the national digital identification system.
Relationship with the private sector (please mark the correct options in bold).	1. The digital identification system has no connection to the private sector. 2. While there is no connection, the inclusion of the private sector in the national digital identification system is planned. 3. Private computer systems are integrated into the national digital identification system, so a user can use their ID to access the public sector and some private sectors. 4. Digital identification providers are available within the national digital identification system.

Use and characteristics of the national digital identification	
The national digital identification system distinguishes between different types of users. Please select the correct options in bold.	1. The system identifies natural persons, without distinguishing their roles or relationships. 2. The system also manages legal entitys. 3. Among natural persons, public officials stand out. 4. Among natural persons, foreigners stand out. 5. The following types of users stand out are [COMPLETE]:
What information about each user does the national digital identification system manage? Please select in bold.	1. National Identification Number 2. State or Provincial Identification Number 3. First and Last Name or Company Name 4. Residence or Address 5. Sex 6. Date of Birth 7. Country 8. Email 9. Mobile Phone Number 10. Photograph (face) 11. Signature (scanned hologram) 12. Contains other attributes or data relevant to Tax Authorities (e.g., public official, company representative, etc.). Please specify:
The system manages more than one level of security for digital IDs. Please mark the correct options in bold. **Note**: If this information is available on a website, we suggest you only enter the link; it is not necessary to answer the question.	1. Low trust: Online registered user whose identity is not guaranteed by verification. 2. Medium trust: User validated through various means (in person, biometrics, biometrics + liveness verification, etc.). 3. Very high trust: User validated with strong authentication (multiple authentication factors, use of biometrics or digital signature, etc.).

Relationship between national digital identification and tax administration	
Is the Tax Administration integrated into the national digital identification system? Please select the correct options in bold.	1. It is not available and there are no plans to implement it. 2. It is not available, but integration is planned. 3. The Tax Administration is a digital identification provider within the national system. 4. The Tax Administration is integrated; taxpayers can use either the tax administration's identification or the national identification. In this case: a. Very few taxpayers access the tax administration using their national digital identification. b. Taxpayers use both the national digital identification and the tax administration's digital identification similarly. c. Most taxpayers use their national digital identification to access the Tax Administration. 5. In addition to option 4, the tax administration aims to increasingly use the national digital identification and gradually "phase out" the tax administration's digital identification. 6. The tax administration is integrated, and only the national digital ID can be used to access the Tax Administration.
Considering the security levels of the national digital identification system, which levels does the tax administration accept? Please select the correct options in bold.	1. Low trust 2. Medium trust 3. Very high trust
Is it possible to obtain or validate a national digital identification at the tax administration offices? Please select the correct option in bold.	1. No 2. Yes
What do you believe are the main challenges and opportunities for future improvement in national digital identification?	Answer:
What do you believe are the main benefits for users and computer systems of integrating into the national digital identification system?	Answer:

Section B. Digital Identification in Tax Administration

This section aims to gather information on the digital identification of the Tax Administration, regardless of whether a national digital identification system exists. If the tax administration is fully integrated into the national digital identification system and only uses the national digital identification system, please proceed to Section C.

Characteristics of the digital identification of the tax administration	
When a taxpayer is going to enter the tax administration, they are usually asked for an identifier (user code).	1. The taxpayer identification number. In the case of legal entitys, all users linked to the company share a username and password. 2. The taxpayer identification number. While there is only one taxpayer identification number per legal entity, there is a method to distinguish which natural person is operating on behalf of the legal entity. The method works as follows: 3. A user identifier, and the tax administration system already knows which legal entities the user is associated with. 4. Other [Specify]:
Regarding the enabled authentication methods, once the user logs in, please mark the correct options in bold.	1. A password is used, and there is no strong password policy. 2. There is a password policy that ensures (and requires) users to maintain strong passwords. 3. Regarding the possibility of using a second authentication factor (select the correct option in bold): a. Mandatory for all users b. Mandatory for some user groups c. Optional for all users d. There is no possibility of using a second authentication factor 4. If a second factor exists (mandatory or not), please select the methods available to users (select the correct options in bold): a. OTP (one-time password or one-time code) to email or mobile phone (SMS, WhatsApp, or similar) b. Authentication applications such as Google Authenticator or similar c. Physical token issued by the tax administration d. Biometric comparison of facial image with an image stored in the system of a person associated with the company e. Biometric comparison of facial image with an image stored in the system after liveness detection of a person associated with the company f. Other (specify): [COMPLETE]

Characteristics of the digital identification of the tax administration	
Regarding access control and roles for digital tax identification, please mark the correct options in bold.	1. The system determines whether the user is a taxpayer, tax administration official, system administrator, a natural person, a legal entity, etc. 2. If the user is a natural person, the system determines which companies they are associated with but does not distinguish their roles within those companies. 3. If the user is a natural person, the system determines which companies they are associated with and what roles they can hold in each company (owner, manager, representative, accountant, etc.). 4. Other [COMPLETE]:
Regarding the delegation of permissions from a holder to third parties, please select the correct options in bold.	1. There is no possibility of delegating functions, so the user and their managers use the same digital identification. 2. The user can select, from a catalog, other users who can operate within their company in different roles (accountant, manager, etc.). 3. There is a possibility of delegating roles, but in person; the owner(s) must go to the tax administration to indicate which users can operate with which roles within their company. 4. Other [COMPLETE]:
Regarding the methods for obtaining a digital tax identification number, which ones are used? Please mark the correct options in bold.	1. The user registers online and there is no identity check or duplicate registration check. 2. The user registers online and the system checks that the user is not already registered (using their identifier, document number, email address, etc.). 3. The user registers online; in addition to checking for duplicates, the system also performs some data consistency checks by interoperating with other public services. (For example, the user uses a web service to obtain their registration data from the relevant public agency). 4. The user registers online; the system performs a biometric comparison of a photo taken of the user's face with a photo from the public registry. 5. The user registers online; the system performs a biometric comparison of a photo taken of the user's face with a photo from the public registry but first applies an automatic liveness detection check. 6. The user registers in person only at the Tax Administration. 7. The user registers in person at the Tax Administration and/or at other public agencies to which the tax administration delegates this function. 8. The user registers in person at the Tax Administration and/or at private companies to which the tax administration delegates this function. 9. Other [COMPLETE]:

Characteristics of the digital identification of the tax administration	
Was the tax administration's digital identification developed based on any known framework? Please mark the correct option in bold.	1. No, it was carried out based on the requirements of the tax administration. 2. The following frameworks were used partially in some services [COMPLETE]. 3. The following frameworks were used completely [COMPLETE]:
Is it possible for natural persons without an identity document or birth certificate to receive a digital identification for tax purposes? (select the correct options in bold):	1. No. 2. Not yet, but the need to implement it is being considered. 3. Yes, through the national digital identification system integrated with the tax administration. 4. Yes, using private means of identification, for example, bank cards. 5. Yes, using foreign physical identification documents (for example, passport). 6. Other [COMPLETE]:
Is the taxpayer's digital identification, which they use to access digital services provided by the tax administration, used to interoperate with other public organizations? (Select the correct options in bold):	1. No. 2. Not yet, but the need to implement it is being considered. 3. Yes, to obtain or verify information regarding potential tax benefits based on the taxpayer's activity, taxpayer type, etc. 4. Yes, to obtain or issue certificates necessary to complete digital procedures. 5. Yes, to initiate a procedure or service with the tax administration and continue it with another agency (or vice versa). 6. Yes, to obtain information about the user's profile, such as whether they belong to a professional association (lawyers, accountants, tax professionals, etc.).
Regarding the protection of the Tax Administration's Digital Identification (select the correct options in bold):	1. Campaigns are conducted periodically to raise awareness among users (only tax administration officials) regarding the precautions associated with digital identification. 2. Campaigns are conducted periodically to raise awareness among all users regarding the precautions associated with digital identification. 3. Campaigns are conducted to raise awareness about issues such as phishing. 4. There is a system that allows users to manage the trusted devices they use to access the Tax Administration. 5. The digital identification system is integrated with a service that analyzes information in real time to detect possible anomalies or fraud related to the use of digital identification. 6. The system mentioned in the previous question, in some cases, takes automatic actions such as blocking users. 7. The tax administration's digital identification is integrated with a death registration service to block deceased users. 8. Controls and actions are in place to prevent users from sharing digital identifications.

The future of digital identification in tax administration	
Do you consider it important to develop a national digital identification ecosystem, where the Tax Administration is integrated so that users can use a single national identification to access various public and private digital services?	Comments:
Do you believe it is important to integrate digital identification at a regional level to facilitate access to tax administration services for foreigners, including using trusted digital identification from other countries? What benefits could this initiative bring to tax administrations and taxpayers?	Comments:

Section C. Digital Development

For the various services offered by the Tax Administration, please select the available digital channels and their coverage (mark the correct options in the "Enabled Digital Channels" column and the correct option in "Digital Coverage").

Please use the following approximate scale:

1. Most transactions are conducted through digital channels – more than 75%.
2. Many transactions are conducted through digital channels – between 50% and 75%.
3. Few transactions are conducted through digital channels – between 25% and 50%.
4. Almost none are conducted through digital channels – less than 25%.
5. No digital channels are available.

Service	Enabled digital channels	Digital coverage
Registration in the tax system	• Web • Mobile • API • Email • Others:	1. Most are done through digital channels 2. Many are done through digital channels 3. Few are done through digital channels 4. Almost none are done through digital channels 5. No digital channels are available
Filing of tax returns	• Web • Mobile • API • Email • Others:	1. Most are done through digital channels 2. Many are done through digital channels 3. Few are done through digital channels 4. Almost none are done through digital channels 5. No digital channels are available
Pre-filled tax returns	• Web • Mobile • API • Email • Others:	1. Most are done through digital channels 2. Many are done through digital channels 3. Few are done through digital channels 4. Almost none are done through digital channels 5. No digital channels are available

Service	Enabled digital channels	Digital coverage
Payment of tax obligations	• Web • Mobile • API • Email • Others:	1. Most are done through digital channels 2. Many are done through digital channels 3. Few are done through digital channels 4. Almost none are done through digital channels 5. No digital channels are available
Processing of records and/or certificates	• Web • Mobile • API • Email • Others:	1. Most are done through digital channels 2. Many are done through digital channels 3. Few are done through digital channels 4. Almost none are done through digital channels 5. No digital channels are available
Processing of Payment Agreements	• Web • Mobile • API • Email • Others:	1. Most are done through digital channels 2. Many are done through digital channels 3. Few are done through digital channels 4. Almost none are done through digital channels 5. No digital channels are available
Applications for loans or tax benefits	• Web • Mobile • API • Email • Others:	1. Most are done through digital channels 2. Many are done through digital channels 3. Few are done through digital channels 4. Almost none are done through digital channels 5. No digital channels are available
Submission of rebuttals and/or requests	• Web • Mobile • API • Email • Others:	1. Most are done through digital channels 2. Many are done through digital channels 3. Few are done through digital channels 4. Almost none are done through digital channels 5. No digital channels are available
Communications and/or notifications	• Web • Mobile • API • Email • Others:	1. Most are done through digital channels 2. Many are done through digital channels 3. Few are done through digital channels 4. Almost none are done through digital channels 5. No digital channels are available
Sending or uploading information	• Web • Mobile • API • Email • Others:	1. Most are done through digital channels 2. Many are done through digital channels 3. Few are done through digital channels 4. Almost none are done through digital channels 5. No digital channels are available

Service	Enabled digital channels	Digital coverage
Inquiry about current account/statement of financial position	• Web • Mobile • API • Email • Others:	1. Most are done through digital channels 2. Many are done through digital channels 3. Few are done through digital channels 4. Almost none are done through digital channels 5. No digital channels are available
Binding inquiries	• Web • Mobile • API • Email • Others:	1. Most are done through digital channels 2. Many are done through digital channels 3. Few are done through digital channels 4. Almost none are done through digital channels 5. No digital channels are available
General inquiries	• Web • Mobile • API • Email • Others:	1. Most are done through digital channels 2. Many are done through digital channels 3. Few are done through digital channels 4. Almost none are done through digital channels 5. No digital channels are available
Scheduling an in-person appointment at the office	• Web • Mobile • API • Email • Others:	1. Most are done through digital channels 2. Many are done through digital channels 3. Few are done through digital channels 4. Almost none are done through digital channels 5. No digital channels are available
Dispute resolution	• Web • Mobile • API • Email • Others:	1. Most are done through digital channels 2. Many are done through digital channels 3. Few are done through digital channels 4. Almost none are done through digital channels 5. No digital channels are available

For each of the services and procedures (if any), please indicate its relationship with digital identification (mark the correct options in bold).

Service	Relationship with digital identification
Registration in the tax system	1. There is no digital identification 2. Only the taxpayer identification number is entered 3. Authentication is required 4. In addition to authentication, a second authentication factor is required
Filing of tax returns	1. There is no digital identification 2. Only the taxpayer identification number is entered 3. Authentication is required 4. In addition to authentication, a second authentication factor is required
Pre-filled tax returns	1. There is no digital identification 2. Only the taxpayer identification number is entered 3. Authentication is required 4. In addition to authentication, a second authentication factor is required
Payment of tax obligations	1. There is no digital identification 2. Only the taxpayer identification number is entered 3. Authentication is required 4. In addition to authentication, a second authentication factor is required
Processing of records and/or certificates	1. There is no digital identification 2. Only the taxpayer identification number is entered 3. Authentication is required 4. In addition to authentication, a second authentication factor is required
Processing of Payment Agreements	1. There is no digital identification 2. Only the taxpayer identification number is entered 3. Authentication is required 4. In addition to authentication, a second authentication factor is required
Applications for loans or tax benefits	1. There is no digital identification 2. Only the taxpayer identification number is entered 3. Authentication is required 4. In addition to authentication, a second authentication factor is required

Service	Relationship with digital identification
Submission of rebuttals and/or requests	1. There is no digital identification 2. Only the taxpayer identification number is entered 3. Authentication is required 4. In addition to authentication, a second authentication factor is required
Communications and/or notifications	1. There is no digital identification 2. Only the taxpayer identification number is entered 3. Authentication is required 4. In addition to authentication, a second authentication factor is required
Sending or uploading information	1. There is no digital identification 2. Only the taxpayer identification number is entered 3. Authentication is required 4. In addition to authentication, a second authentication factor is required
Inquiry about current account/statement of financial position	1. There is no digital identification 2. Only the taxpayer identification number is entered 3. Authentication is required 4. In addition to authentication, a second authentication factor is required
Binding inquiries	1. There is no digital identification 2. Only the taxpayer identification number is entered 3. Authentication is required 4. In addition to authentication, a second authentication factor is required
General inquiries	1. There is no digital identification 2. Only the taxpayer identification number is entered 3. Authentication is required 4. In addition to authentication, a second authentication factor is required
Scheduling an in-person appointment at the office	1. There is no digital identification 2. Only the taxpayer identification number is entered 3. Authentication is required 4. In addition to authentication, a second authentication factor is required
Dispute resolution	1. There is no digital identification 2. Only the taxpayer identification number is entered 3. Authentication is required 4. In addition to authentication, a second authentication factor is required

Annex II: Digital Identification Model for Latin America and the Caribbean (IdLAC)

In previous chapters, we discussed some recognized and widely used digital identification models, such as those of NIST, ISO, and eIDAS in the European Union. In Latin America and the Caribbean, a digital identification model called IdLAC is being developed.

The Inter-American Digital Government Network (Red GEALC), created in 2003, comprises the agencies or ministries responsible for the development of digital government in each member country of the Organization of American States (OAS). It is a network designed to promote cooperation among countries for the development of digital government, the creation of participatory public policies, the training of public employees, knowledge sharing for the development of national digital government strategies, and the exchange of solutions and experts in the region.

The overall objective of the GEALC Network is to support digital government policies that focus on citizens, particularly the most vulnerable populations, and it has several cross-cutting technical working groups among member countries. One of the groups aims to promote cross-border recognition of digital signatures and cross-border interoperability of digital identification in the region. In this group, significant progress has been made in cross-border digital identification over the last two years.

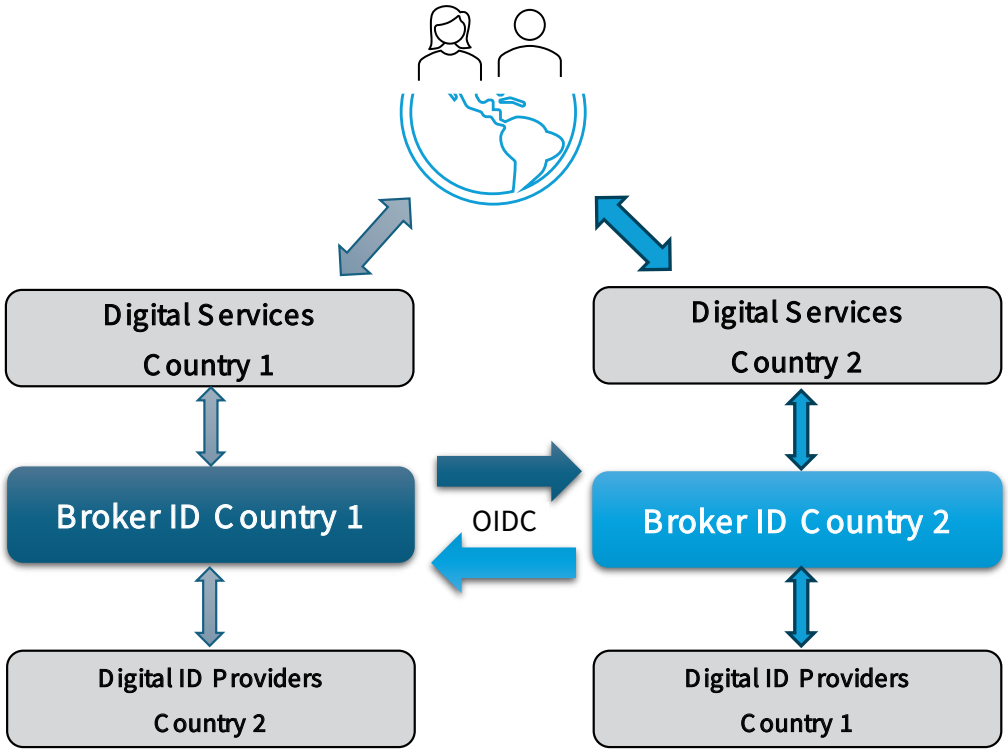
Argentina, Brazil, and Uruguay have national digital identification ecosystems, each structured by a broker: Autenticar, Gov.br, and ID Uruguay, respectively. During the COVID-19 pandemic, the need arose to begin developing cross-border digital identification, as many people were unable to leave their countries of origin but needed to carry out procedures and access services in other countries. In these countries, it was not possible to validate a person's identity, so if they obtained a digital ID in a foreign country, it would always be considered unreliable. From this situation, it was concluded that people should have reliable identifications from their countries and be able to use them to identify themselves digitally in services of other countries, just as is done with physical identifications, but taking advantage of all the benefits of the digital world.

Thus, the Network's Cross-Border Identification and Signature working group began defining how natural persons could access digital services in one country using their trusted national digital identification. Along these lines, Uruguay and Argentina began technical analysis and testing to integrate their two digital identification brokers: Autenticar and ID Uruguay. Each broker is the core of the federated digital identification

ecosystem. Each broker has a set of digital identification providers suitable for its ecosystem and standardizes identification (protocols, data that identifies a person, and security levels).

The fact that each broker has a set of identification providers led to the conclusion that integrating one broker with another would enable the identification providers of one country in the other, and vice versa. Furthermore, integrating one broker with another effectively enables a group of identity providers within one broker and vice versa. This situation led to the conclusion that integrating one broker with another simply required using the OpenID Connect protocol from one side and then from the other. The following diagram illustrates this:

Figure 13. Simplified scheme of cross-border integration of digital identification ecosystems.



Source: Prepared by the author

The logic behind integrating both ecosystems is to create two flows, as shown in the previous figure. Country 1 views the other broker as a group of federated digital identity providers and integrates accordingly via OpenID Connect. The same applies to Country 2.

This extremely simple and secure solution (with some conditions) is the way to integrate one ecosystem with another, allowing citizens of one country to use their national IDs to access services in both countries. The first prototype was developed between Uruguay and Argentina in mid-2023 to validate this idea, and work began with Brazil.

The development between Uruguay and Brazil was simpler because the methodology had already been validated through prior experience. In October 2024, the first cross-border identification system in the region went into production, allowing Brazilian citizens to digitally identify themselves using their trusted Brazilian IDs across 40 Uruguayan digital services provided by the Water and Energy Services Regulatory Unit (URSEA) and the Uruguayan Ministry of Public Health's application for yerba mate transport permissions. In December 2025, all procedures and services of Uruguay's Single Window for Foreign Trade (VUCE) were enabled, reaching more than 360 digital procedures and services in Uruguay compatible with trusted Brazilian digital IDs.

This sparked interest among several countries in the region in developing a broker, and this opportunity was presented to the GEALC Network. The opportunity consisted of developing a model broker, updated and minimalist, designed collaboratively by all the countries so that each could implement it locally. This would not only save costs by requiring a single development process, but, more importantly, would create a standardized regional platform comprised of all the brokers from each country. By having all countries use the same broker, a digital identification ecosystem would develop in each country, while a standardization layer would be built across the region, composed of all the brokers.

Given this opportunity, the GEALC Network announced a project to develop a model broker, financed by the Inter-American Development Bank, the World Bank, and Co-Develop, with support from the Organization of American States and other leading organizations in the field. In addition, a working group comprised of 13 countries was formed to establish requirements and begin designing the region's digital identification model.

The IdLAC project comprises the broker, designed to facilitate and standardize digital identification in the region, and the model that establishes protocols, security levels, term equivalence, security requirements, and the data set to be used to identify a natural person. The broker's development is expected to be finalized during the first quarter of 2026, after which the first implementations will begin in the 13 countries that make up the working group.

In this way, a digital identification model for Latin America and the Caribbean called IdLAC is being co-designed. This model includes digital identification methods based on verifiable identity credentials, and the OIDC4VP protocol is expected to be developed so that the broker can enable verifiable credentials for digital identification. One advantage of this model is that the protocol will be implemented only once and distributed among the countries that implement the broker. As the model is designed, the broker does not need to possess the trusted lists of all countries. Each person will use their credential as their identification provider with their country's broker, and through integration between brokers, will access digital services from other countries. Each broker trusts the identifications of the others, thus simplifying the model.

ciat@ciat.org

ciat.org

MINISTERIO
DE ASUNTOS EXTERIORES, UNIÓN EUROPEA
Y COOPERACIÓN

aecid

cooperación
española