SPID: The Complete Guide to Digital Identity

Autore: Francesco Zinghinì | **Data:** 26 Dicembre 2025

Have you ever felt lost in the maze of online bureaucracy? Have you ever had to recover dozens of different passwords to access services from the Public Administration, INPS, the Revenue Agency, or even just to check your health record? If the answer is yes, then you are in the right place. Today we are talking about **SPID**, the Public Digital Identity System, that universal key that promises to simplify our digital lives. **But what exactly is SPID? How does it work? And above all, how can it help me concretely?** In this article, I will guide you step by step to discover this tool, trying to clarify every doubt and showing you why, by now, it has become almost indispensable. Get ready to say goodbye to a thousand different credentials and welcome a single, secure, and fast access method. Trust me, it's worth it.

What Is SPID and Why Has It Become Essential

I still remember the days when every Public Administration (PA) website had its own access system. A nightmare. Different passwords, complicated registration procedures, physical tokens that always ran out of battery at the wrong moment. It was frustrating, I admit. Then came SPID, an acronym for **Sistema Pubblico di Identità Digitale** (Public Digital Identity System). The idea behind it is simple but revolutionary: to provide citizens and businesses with a single digital identity, a set of credentials (username and password, sometimes accompanied by a temporary code) to access all online services of the PA and participating private entities securely and quickly.

Think of SPID as a digital passport. Instead of having to prove who you are every time you "cross a digital border" (i.e., access a new online service), you use your certified SPID credentials and are recognized immediately. No more multiple registrations, no more forgotten passwords. Convenient, right?

But SPID isn't just about convenience. It's also about **security**. The system is managed by the Agency for Digital Italy (AgID), which oversees digital identity providers (called Identity Providers or IdPs) and guarantees high data protection standards. Authentication takes place through different security levels, which we will see shortly, ensuring that only you can access your data and the services reserved for you.

Today, SPID has become practically **essential**. Do you want to access the INPS website to check your contribution position or request a bonus? You need SPID. Do you need to consult your tax drawer on the Revenue Agency website? You need SPID. Do you want to access your Electronic Health Record? You need SPID. Do you need to sign up for an online public competition? Most likely, you need SPID. Even some universities, municipalities, and regions require it for access to their portals. And let's not forget private services: more and more banks, insurance companies, and utilities are integrating access via SPID. In short, not having it means cutting yourself off from a growing number of online services, forcing yourself to resort to slower and more cumbersome methods, when available.

SPID Security Levels: What They Mean

When talking about SPID, you often hear about "levels". But what are they exactly? SPID levels indicate the degree of authentication security. The higher the level, the greater the security required to access the service. Currently,

there are three levels:

- **SPID Level 1:** This is the basic level. To log in, you just need to enter your username and password. It is simple and fast, suitable for services that do not require a high degree of security (for example, consulting general non-sensitive information). Think of a simple door with a standard lock.

- **SPID Level 2:** Here security increases. In addition to your username and password, you must enter a temporary OTP (One Time Password) code generated via an app on your smartphone (such as Google Authenticator or your Identity Provider's specific app) or received via SMS. This mechanism is known as two-factor authentication (2FA) and offers significantly greater protection. It is the level required for most PA services dealing with personal data (INPS, Revenue Agency, Health Record…). Imagine the same door as before, but with an additional security lock. This is the most commonly used level.

- **SPID Level 3:** This is the maximum security level. In addition to Level 2 credentials, it requires the use of an additional physical support, such as a smart card or a USB device with a digital certificate, or the use of specific apps that guarantee the unique association between user and device. It is used for services requiring absolute reliability on the user's identity, such as the digital signing of documents with full legal value or access to extremely sensitive data. Think of a bank vault: it requires multiple keys and complex procedures for access. This level is less common for daily use but fundamental for specific operations.

The choice of level depends on the service you want to access. It will be the service provider (e.g., INPS, Municipality, etc.) that indicates which SPID level is necessary. The good news is that by obtaining SPID, you usually automatically get credentials for Level 1 and 2. Level 3, on the other hand, may require additional procedures and, sometimes, extra costs depending on the chosen Identity Provider.

SPID vs. CIE vs. CNS: Let's Clarify

In the landscape of Italian digital identity, in addition to SPID, there are two other important tools: the CIE (Electronic Identity Card) and the CNS (National Service Card). It is easy to get confused, so let's try to understand the differences and similarities.

- **SPID (Public Digital Identity System):** As we have seen, it is a system based on digital credentials (username, password, OTP) provided by private Identity Providers accredited by AgID. It is completely digital (except for the initial recognition phase, which can also take place in person) and offers different security levels. It was born specifically for access to online services.

- **CIE (Electronic Identity Card):** It is the evolution of the old paper identity card. It is a physical document (a plastic card) containing a microchip with the holder's personal data, photo, and fingerprints. Besides being a valid physical identification document for travel, it can also be used to access PA online services. To do this, you need a compatible smart card reader connected to a PC or an Android smartphone or iPhone equipped with NFC technology and the "CieID" app. Access with CIE usually corresponds to SPID security level 2 or 3, depending on the

methods used. The CIE PIN is provided in two parts at the time of issuance.

- **CNS (National Service Card):** It is another digital identity tool, often integrated into the Health Card (TS-CNS). The CNS is also a physical smart card with a microchip that allows access to PA online services, requiring a smart card reader and an associated PIN (which must be requested separately at the enabled counters of your region or Local Health Authority – ASL). Like the CIE, it guarantees a high level of security (comparable to SPID 2 or 3).

What are the main differences?

1. **Nature:** SPID is purely digital (credentials), while CIE and CNS are primarily physical documents (smart cards) also usable for online access.

2. **Issuance:** SPID is issued by accredited private providers (Poste, Aruba, Namirial, etc.). The CIE is issued by the Municipality of residence. The CNS is often integrated into the Health Card issued by the Revenue Agency via the ASL.

3. **Usage:** All three allow access to PA online services. SPID is perhaps the most versatile and widespread for this specific purpose. CIE and CNS also have the primary function of a physical document (identity for CIE, health card for CNS).

4. **Levels:** SPID has well-defined levels 1, 2, and 3. CIE and CNS, when used online, guarantee high security levels (2 or 3).

In summary, they are different tools but with overlapping functionality: secure access to digital services. Many services accept SPID, CIE, or CNS indifferently. Having SPID is often the most practical choice for those who frequently interact

online with the PA, given its completely digital nature and ease of use with OTP apps. However, CIE and CNS are also valid and secure tools. Often, the choice depends on which tool you already possess or find more convenient to use.

Who Can Request SPID?

Are you wondering if you can request SPID? The answer is most likely yes! SPID is designed for a vast audience of users. It can be requested by:

1. **All adult Italian citizens:** If you are 18 years old and an Italian citizen, you can request SPID. It is your right to access digital services.

2. **Italian citizens residing abroad:** Even if you live outside Italy, but are an Italian citizen registered with AIRE (Registry of Italians Residing Abroad), you can obtain SPID. It is fundamental for maintaining contact with the Italian PA even from afar. The procedure might differ slightly depending on the provider and the country of residence, but it is absolutely feasible.

3. **Foreign citizens with a residence permit living in Italy:** If you are a foreign citizen living regularly in Italy and possess a valid residence permit and an Italian tax code (codice fiscale), you have the right to request SPID. This allows you to access Italian PA online services exactly like an Italian citizen. It is an important step for integration and simplifying daily life.

4. **Minors (SPID for minors):** Recently, the possibility of requesting SPID for minors (starting from 5 years old) has been introduced. In this case, the request must be made by a parent (or whoever exercises parental responsibility) who already possesses SPID. SPID for minors allows access to online services dedicated to their age group (e.g., school portals, specific health services) under parental supervision. There are age groups

(5-13 years and 14-17 years) with differentiated permissions. It is a tool designed to educate young people on the conscious use of digital services.

5. **Legal persons (SPID for professional use):** There is also a specific SPID for companies and freelancers, called "SPID for professional use". This type of SPID identifies the natural person acting on behalf of a legal person (a company, an entity, a professional firm) and allows access to online services dedicated to businesses. It can be requested by the legal representative or a delegated employee.

Basically, almost anyone who needs to interact with the Italian Public Administration online can (and should) obtain SPID. The basic requirements are usually: a valid Italian identity document (identity card, passport, driving license), the health card with the tax code, a personal email address, and a personal mobile number.

How to Get SPID: Steps and Providers Compared

Okay, we understand what SPID is and why it's useful. But how do you actually get it? The process is less complicated than it might seem, but it requires attention. The first thing to do is choose an **Identity Provider (IdP)**, which is one of the private companies authorized by AgID to issue the SPID digital identity.

The choice of IdP is important because, although they all provide valid SPID credentials to access the same services, they may differ in:

- **Recognition methods:** How they verify your identity the first time.

- **Security levels offered:** All offer Level 1 and 2, but not all offer (or offer for free) Level 3.

- **Costs:** Some recognition methods or Level 3 might be paid services.

- **Ease of use:** The interface of the OTP app or the management portal may vary.

- **Customer support:** The quality and availability of support.

Let's look at the general steps and then compare some of the main providers.

Choosing the Identity Provider (IdP)

There are several IdPs authorized by AgID. On the official SPID website (spid.gov.it) you can find the complete and updated list. Among the most well-known and used are:

- Poste Italiane (PosteID)

- Aruba

- InfoCert

- Namirial

- Register.it

- Sielte

- TIM id

- Intesa (IBM Group)

- Lepida

How to choose? Evaluate these factors:

1. **Recognition methods:** Do you prefer doing everything online or going in person to an office?

2. **Tools you already possess:** Do you have a CIE, an active CNS, or a digital signature? They could simplify online recognition. Do you already have a verified account with one of the providers (e.g., Poste Italiane)?

3. **Necessary security level:** Is Level 2 (the most common) enough for you, or do you foresee needing Level 3?

4. **Costs:** Are you willing to pay for a more convenient recognition method or for Level 3, or are you looking for a completely free solution?

5. **Support:** Read reviews or find out about the quality of the provider's customer service.

There is no absolute "best" provider; it depends on your needs and preferences.

Recognition Methods: Online and In-Person

This is the crucial phase: the IdP must verify with certainty that you are actually who you say you are. The most common methods are:

- **In-person recognition:** You physically go to an office of the chosen provider (e.g., Post Office for PosteID, affiliated counters for others) with your documents. The operator verifies your identity and guides you through completing the request. It is a secure method suitable for those who prefer direct contact or are less familiar with digital tools. It is usually free (e.g., with Poste Italiane).

- **Online recognition via webcam:** You schedule an appointment online and, via a video call with an operator, show your documents and answer some questions. The operator verifies your identity in real-time. This method is convenient because you do it from home, but it is often paid (the cost varies between about 10 and 30 euros, depending on the provider).

- **Online recognition with CIE 3.0:** If you have the Electronic Identity Card (version 3.0) with the relative PIN and an NFC smartphone or a smart card reader, you can use it to identify yourself online. You bring the CIE close to the smartphone/reader, enter the PIN, and the system automatically verifies your identity. It is a fast and usually free method.

- **Online recognition with CNS:** Similar to the CIE, if you have the National Service Card (often the Health Card) activated with the PIN and a smart card reader, you can use it for online recognition. This method is also generally free.

- **Online recognition with Digital Signature:** If you already have an active qualified digital signature, you can use it to sign the SPID contract and complete the online recognition autonomously and for free.

- **Recognition via Bank Transfer (some providers):** Some IdPs allow "indirect" recognition via a symbolic bank transfer (a few cents) from an Italian bank account held in your name. The account ownership serves as identity verification. This method may have associated costs.

- **Recognition via existing credentials (e.g., PosteID):** If you are already a Poste Italiane customer with a verified account (e.g., Bancoposta), you might be able to obtain SPID PosteID more quickly online.

Choose the method that suits you best, taking into account time, costs, and tools at your disposal.

Comparison of Main Providers (PosteID, Aruba, Namirial, etc.)

Let's take a closer look at some of the most popular IdPs, highlighting their main features (remember that offers and conditions can change, always check the official websites):

- **Poste Italiane (PosteID):**
  - **Recognition:** Free in person at the Post Office; online with CIE/CNS/Digital Signature; online via Bancoposta/Postepay App (if eligible); paid via bank transfer or home service.
  - **Levels:** Offers Level 1, 2 (via PosteID App or SMS), and 3 (paid with physical device or via PosteID App with specific requirements).
  - **Pros:** Widespread network of post offices for free recognition, widely used PosteID app.
  - **Cons:** Possible queues at counters, Level 3 activation is paid (if not using the enhanced app). *There are articles on TuttoSemplice.com regarding Poste Italiane services (such as PosteID, PEC, Postepay) that may be useful*.

- **Aruba (Aruba ID):**
  - **Recognition:** Online with CIE/CNS/Digital Signature (free); online via webcam (paid); in person at affiliated partners (may have costs).

- **Levels:** Offers Level 1, 2 (via Aruba OTP App or SMS), and 3 (paid with smart card/USB token).

- **Pros:** Well-known company in the digital sector, various online options.

- **Cons:** Webcam recognition is paid, Level 3 is paid.

- **Namirial (Namirial ID):**

  - **Recognition:** Online with CIE/CNS/Digital Signature (free); online via webcam (paid); in person at affiliated partners (paid).

  - **Levels:** Offers Level 1 and 2 (via Namirial OTP App or SMS). Also offers solutions for Level 3.

  - **Pros:** Streamlined online process, company specialized in digital identity and electronic signature. *TuttoSemplice.com has an article on how to contact Namirial*.

  - **Cons:** Webcam and in-person recognition are paid.

- **InfoCert (InfoCert ID):**

  - **Recognition:** Online with CIE/CNS/Digital Signature (free); online via webcam (paid); in person at InfoCert Points or affiliated tobacconists (paid).

  - **Levels:** Offers Level 1, 2 (via MyInfoCert App or SMS), and 3 (paid with physical devices).

  - **Pros:** Network of physical points (including tobacconists), historic provider.

- **Cons:** More convenient recognition methods (webcam, physical points) are paid.

- **Sielte (SielteID):**
  - **Recognition:** Online with CIE/CNS/Digital Signature (free); online via webcam (free!); in person at their offices (free).
  - **Levels:** Offers Level 1 and 2 (via MySielteID App or SMS).
  - **Pros:** Offers webcam recognition for free, a significant advantage over many competitors.
  - **Cons:** Fewer physical offices compared to Poste, less known to the general public.

Comparative Table (Indicative – Always check official websites)

Provider	Webcam Rec.	CIE/CNS/Sig Rec.	In-Person Rec. (HQ/Partner)	Level 3 Offered	Notes
PosteID	Paid	Free	Free (Post Office)	Yes (paid*)	Widely used, PosteID App
Aruba ID	Paid	Free	Paid (partner)	Yes (paid)	Online options
Namirial ID	Paid	Free	Paid (partner)	Yes	Specialized in digital identity
InfoCert ID	Paid	Free	Paid (InfoCert/Tobacconists)	Yes (paid)	Physical point network
SielteID	**Free**	Free	Free (Sielte offices)	No (standard)	Free webcam recognition
TIM id	Paid	Free	Free (TIM Stores)	Yes (paid)	Linked to TIM operator
Register.it	Paid	Free	Paid (partner)	Yes (paid)	Web hosting services

Provider	Webcam Rec.	CIE/CNS/Sig Rec.	In-Person Rec. (HQ/Partner)	Level 3 Offered	Notes
Lepida	Free	Free	Free (Emilia-Romagna Region Counters+)	Yes (paid)	Mainly Emilia-Romagna, but not only
Intesa	Paid	Free	Not available (standard)	Yes (paid)	IBM Group

PosteID Level 3 can be activated via the enhanced PosteID App on certified devices, otherwise it requires a paid physical device.

Take the time to compare options on the AgID website and individual provider websites before deciding. Once you have chosen the IdP and the recognition method, follow the guided procedure on their site: enter your personal data, upload the required documents, perform the recognition, and wait for the activation of your SPID credentials. Usually, after recognition, activation is a matter of minutes or a few hours.

Practical Uses of SPID: What You Can Actually Do

We have obtained our SPID credentials. Now what? What are they for in everyday life? The uses are many and constantly growing. SPID is the access key to a world of digital services, both public and private. Let's look at some concrete examples.

Accessing **Public Administration** services is the primary use. Think about how many times you have had to interact with entities like:

- **INPS:** Consult your contribution statement, request bonuses (such as the Single Universal Allowance, NASpI, baby bonus), check the status of your applications, simulate your pension. With SPID, you access the MyINPS personal area in a few seconds.

- **Revenue Agency (Agenzia delle Entrate):** Access your Tax Drawer, consult past tax returns, pay taxes and duties (such as IMU via PagoPA), verify payments, manage your tax position.

- **Electronic Health Record (FSE):** Consult medical reports, book visits and exams (online CUP), view vaccination history, access electronic prescriptions. Healthcare becomes more accessible and just a click away.

- **Municipalities:** Pay the TARI (waste tax), request online registry certificates (often free with SPID), access demographic services, enroll children in school.

- **Schools and Universities:** Enroll online, consult electronic registers, pay university fees, access e-learning platforms.

- **ACI – Motorist's Portal:** Check insurance coverage and inspection status of your vehicles, check your driving license points balance, manage car paperwork.

- **App IO:** The public services app that aggregates many PA services and allows you to receive communications, make payments (PagoPA), and take advantage of bonuses (like the old State Cashback). Access is via SPID or CIE.

- **Public Competitions:** Register online for PA competition notices.

- **Regional Services:** Each region offers portals accessible with SPID for specific services (transport, agriculture, tourism, etc.).

But SPID doesn't stop at the PA. More and more **private entities** are adopting SPID as a secure and recognized authentication system. Some examples:

- **Banks and Financial Institutions:** Some banks allow access to home banking or subscription to online products via SPID. It could also simplify opening online bank accounts or requesting loans.

- **Insurance Companies:** Fill out quotes or manage your policy online. It could be useful for comparing online car insurance.

- **Utilities (Electricity, Gas, Water):** Access the customer area to check bills, communicate meter readings, manage contracts. Useful when comparing electricity and gas tariffs.

- **Postal Services:** Access Poste Italiane online services, such as shipment tracking or PEC management.

- **Digital Signature:** Some qualified electronic signature services use SPID (especially Level 3) for the strong authentication needed to sign documents with full legal value.

The list is constantly expanding. The goal is to make SPID the single key to access any online service requiring certain user identification, greatly simplifying our digital life and reducing the risk associated with managing dozens of different passwords (a fundamental aspect for online security). Having SPID today means having control of your digital identity in a secure and centralized way.

Security and Privacy: Is SPID Reliable?

When entrusting your digital identity to a system, the question naturally arises: is it secure? Can I trust it? In the case of SPID, the answer is definitely yes, and for several reasons. The system was designed with high security standards, under the supervision of AgID.

First of all, as we have seen, SPID uses **different authentication levels**. Even Level 2, with the use of OTP (One Time Password), makes it extremely difficult for a malicious actor to access your account even if they managed to discover your password. The OTP is a code valid only for a few seconds and linked to your personal device (usually your smartphone), adding a crucial security factor (two-factor authentication). Level 3 adds a further layer with physical devices or advanced cryptographic mechanisms.

The **Identity Providers** are subject to rigorous checks and must comply with precise technical regulations defined by AgID to guarantee infrastructure security and user data protection. They are not simple companies offering a service, but accredited and supervised entities.

Furthermore, SPID **does not share your data indiscriminately**. When you access a service via SPID, the Identity Provider communicates to the service provider (e.g., INPS) only the data strictly necessary for identification and the provision of that specific service, and only after your explicit consent. There is no massive sharing of information between all entities. You maintain control over which data is shared and with whom.

What can you do to increase the security of your SPID?

1. **Choose a strong password:** Use a complex, long password with uppercase letters, lowercase letters, numbers, and symbols. Do not use the same password for other accounts. Change it periodically. *Consult our guide on how to create* [secure passwords](#).

2. **Protect your OTP device:** The smartphone on which you receive the OTP (via app or SMS) becomes a key element of your security. Protect it with a PIN, fingerprint, or facial recognition. Do not leave it unattended.

3. **Beware of phishing:** Be wary of suspicious emails, SMS, or messages asking for your SPID credentials or inviting you to click on strange links. No Identity Provider or public entity will ever ask for your full credentials via email or message. *Read our articles on* [online scams](#) *and* [phishing](#) *to learn more*.

4. **Do not share your credentials:** SPID credentials are strictly personal and must not be communicated to anyone, not even family or friends.

5. **Check access logs:** Many IdPs offer the possibility to view the history of accesses made with your SPID. Check it periodically to ensure there are no anomalous accesses.

6. **Update the OTP app:** Always keep the application of your IdP that generates OTP codes updated.

By following these simple precautions and relying on the intrinsic robustness of the system, you can use SPID with peace of mind. It is a tool designed to be secure and to protect your identity in the digital world. Its reliability is guaranteed by stringent regulations and constant supervision by AgID.

Conclusions

Having reached the end of this journey, I hope I have provided you with a clear and complete overview of what SPID is and why it has become such a central tool in our daily digital lives. I confess, at first I was a bit skeptical too. Yet another acronym, yet another procedure to learn in a country that often seems to love complication. Yet, I must admit that SPID, once understood and activated, represents **a significant step forward towards simplification and security** in interacting with the digital world, especially that of the Public Administration.

Thinking of being able to access INPS, the Revenue Agency, Health Records, municipal services, and much more with a single pair of credentials (plus the OTP, of course, but we are used to two-factor authentication for almost everything by now) is **no small relief**. Goodbye to loose pieces of paper with improbable passwords, goodbye to endless credential recovery procedures. Sure, the initial activation process requires a bit of effort: choosing the right provider, understanding which recognition method suits us (free or paid? online or in person?), gathering documents. But it is an initial effort that is amply repaid by the subsequent convenience.

The issue of **security** is fundamental, and SPID seems to respond well, thanks to the differentiated levels and AgID's supervision. Obviously, absolute security does not exist and part of the responsibility always falls on us: choosing strong passwords, protecting our devices, being careful about phishing. But the system structure is solid.

Today, not having SPID means encountering increasingly frequent obstacles in accessing essential services. It has effectively become **the new standard for digital identity in Italy**. Whether you are an Italian citizen, a foreign resident, or a professional, SPID is the key that opens many digital doors. If you haven't done so yet, my dispassionate advice is to activate it as soon as possible, choosing the provider and method that best suit your needs. It will be a small investment of time that will significantly simplify your online life.

Frequently Asked Questions

What is SPID in simple terms?

SPID is like a universal key (username and password + temporary code) that allows you to access many online services (INPS, Revenue Agency, Municipality, etc.) without having to create different accounts for each site.

Is SPID free?

Yes, obtaining SPID Level 1 and 2 credentials is generally free with most providers, especially if you choose recognition via CIE/CNS/Digital Signature or in person (e.g., Post Office). Some recognition methods (such as via webcam) or Level 3 may be paid services depending on the provider.

Which SPID level do I need?

For most PA services (INPS, Revenue Agency, Health Record), Level 2 is required (username + password + OTP code). Level 1 is for less sensitive services, Level 3 for operations requiring maximum security (e.g., qualified digital signature).

Can I have more than one SPID identity?

Yes, technically you can request SPID from multiple different Identity Providers. However, a single SPID identity is sufficient to access all services.

How do I get the OTP code for SPID Level 2?

The OTP code is generated via a specific app provided by your Identity Provider (to be installed on your smartphone) or, in some cases, can be sent via SMS to your certified mobile number. Using the app is generally considered more secure and is often the default method.

Does SPID expire?

SPID credentials (username and password) do not expire, but the password must be changed periodically (usually every 6 months) for security reasons. The SPID digital identity remains valid as long as the Identity Provider is accredited and you do not request its revocation.

What should I do if I forget my SPID password?

Every Identity Provider offers an online procedure for password recovery, usually via the email address or mobile number associated with your SPID.

Can minors have SPID?

Yes, parents with SPID can request SPID for their minor children (aged 5 and up), who will be able to access online services suitable for their age under parental supervision.

Is SPID, CIE, or CNS better?

All three allow secure access to online services. SPID is natively digital and often more practical for exclusive online use. CIE and CNS are physical documents that can also be used online. The choice depends on your needs and the tools you already possess.