GENERAL INFORMATION

Agenzia per l’Italia Digitale (Agency for Digital Italy)
Viale Liszt, 21
00144 Rome, Italy
t+39 06 85264.1
Certified e-mail: protocollo@pec.agid.gov.it
Contents

PUBLIC DIGITAL IDENTITY SYSTEM.......................................................................................................3
THE DIGITAL IDENTITY PROVIDER (IdP) .............................................................................................3
   Authentication function...................................................................................................................4
   Handling applications for digital identities ..................................................................................5
   The responsibility of the IdPs........................................................................................................8
   IdP requirements ..........................................................................................................................9
CREDENTIALS AND LEVELS ...........................................................................................................12
THE CONSEQUENCES OF IDENTITY THEFT .......................................................................................12
PUBLIC DIGITAL IDENTIFICATION SYSTEM

The Digital Administration Code (or “CAD”, Italian Legislative Decree no. 82 of 07 March 2005), defines the Public Digital Identity System (or “SPID”) as an open set of public and private subjects that, by accreditation by the Agency for Digital Italy (or “AgID”), in accordance with methods defined by specific decree, manage user registration services and the making available of credentials and network access tools for citizens and businesses, on behalf of the public administrations as the providers of internet services or alternatively directly, at the request of the parties concerned (1).

The SPID envisages various subjects:

a) the User, who may have one or more digital identities, which envisage certain compulsory identifying information, such as the tax code, name, surname, place of birth, date of birth and gender;

b) the Digital Identity Provider. This subject, who must be accredited by the Agency for Digital Italy, is involved in the creation and management of digital identities;

c) the Attribute Authority who, in accordance with current regulations, can certify qualified attributes, such as possession of an educational qualification or membership of a professional order;

d) the Service Provider - a public or private subject - who supplies on-line services, upon recognition of the user by the digital identity provider.

THE DIGITAL IDENTIFICATION PROVIDER (IdP)

The role of identity providers is essential throughout the SPID system, involved in generally ensuring the function and reliability of the system as a whole. The provider must guarantee the availability of the authentication functions so as to grant access to the services made available on the internet by the service providers.

---

1 Article 64, paragraph 2-ter. Paragraph inserted by Art. 17-ter, paragraph 2 of Italian Decree Law no. 69 of 21 June 2013, converted, with amendments, by Italian Law no. 98 of 09 August 2013.
Authentication function

The activity of the IdPs, under the scope of their authentication function, is guaranteed by the application of technical specifications, published in draft from on the Agency website (2) back in October 2014 and thereafter issued in accordance with the technical rules, which govern the methods by which the identity provider and service provider interact. The interaction between the service provider, the identity provider and the user is as envisaged by SAML v2 for the profile of “Web Browser SSO” (3) and is described below, in accordance with the Agency specifications relative to the authentication session:

The process is as follows:
1 - The User (holder of the SPID identity) attempts to access a service offered by a service provider (the figure shows www.abc.com).

---

2 - The Service Provider sends a response to the User’s browser (4) containing a direct request for authentication to the IdP. The request indicates the level of credentials necessary to access the specific service and gives a list of the attributes required for its use.

3 and 4 - The IdP authentication service proceeds to authenticate the User.

5 - The IdP returns the signed response to the User's browser, containing the outcome, level of assurance of the digital identity verified (Art. 6 of the technical rules) and, by consent of the User, the attributes required.

6 - The User’s browser forwards the response received from the IdP to the Service Provider.

Handling applications for digital identities

In addition to guaranteeing the authentication process, necessary before gaining access to the network services, the IdP plays an essential role in managing applications for digital identities in order to guarantee their legal sustainability. There are two main needs: to avoid identity theft and to be able to assign an identity to a natural person or legal entity.

Identity theft may take place if someone manages to obtain the issue of an identity that actually pertains to a different subject or through the unlawful use of credentials necessary to use a digital identity.

In order to fight the first type of identity theft, the IdP needs to apply procedures by which to verify the identity of the applicant, upon approval of the AgID.

Verification of identity involves the use of specific services covered by agreements stipulated by the AgID with the subjects that, in a public area, certify the validity of the identification attributes and allow for the verification of identification documents.

The IdPs are obliged to adhere to such agreements.

The technical rules devote an entire article to the issue of digital identities, as proof of the delicacy of this activity, involving the appointment of a specific Manager responsible for verifying the identity of the applicant and arranging how said verification should be performed:

\( a) \text{ Identification by means of the display of a valid form of ID by the applicant}^{(5)} \)

---

4 HTTP redirect response

5 Article 7, paragraph 2, letter a) of the technical rules.
The most obvious system is a physical meeting between an Appointed Representative of the IdP and the User. The Appointed Representative shall identify the User by examining a valid form of ID.

In this phase, the Appointed Representative acquires the information used to establish the identification attributes of the digital identity: name, surname, place and date of birth, gender or company or business name as well as the tax code or VAT number and the details of the ID used for the identification and at least one secondary attribute (mobile telephone number, e-mail address, physical and digital domicile), functional to communication between IdP and User.

Identification by displaying a form of ID has, in practice, already been in use for more than twelve years for the issue of a digital signature.

Under this scope too, the AgID has the task of authorising the various methods of identification. These include verifying the User’s identity through audio-video sessions during which the Appointed Representative interacts with the User from a remote position.

Differently to as may be considered, this method has various advantages over identification by means of physical presence, in which the Appointed Representative can “touch” the User.

The advantages are not only related to the time saved of the IdP and the User by this remote interaction, but also the identification procedure itself, particularly in terms of security.

In actual fact, in the event of any dispute between the IdP and the User regarding the identification, the “touch” method gives the Judge the following elements for judgement: details of the document used to verify the User’s identity, the declaration made by the IdP's Appointed Representative of the results of said verification and the contract stipulated by the User.

The “remote presence” method adds a fundamental element: the audio and video recording.

By viewing the video images and listening to the audio, a judge will be able to understand whether or not the alleged victim is effectively as he claims. In any case, if in doubt, the audio-video recording provides experts with very important evidence, showing them the action of the subject and allowing them to hear the audio recording, elements that allow for what would clearly be a more complete appraisal than a mere signature on a piece of paper, if it is even legible.

This evidentiary information, which constitutes one of the substantive items in legal terms in the disallowance of the digital identity, must be kept by the identity provider for twenty years from when the digital identity expires or is revoked (6).

---

6 Article 7, paragraph 6 of the technical rules.
**b) Computerised identification by means of digital identification documents, valid in accordance with the law, which envisage the visible recognition of the applicant upon activation, including TS-CNS, CNS or compliant cards**[^7].

In Italy, the digital identity was not conceived with the SPID. The electronic ID card and the National Service Charter are perhaps the first instruments to have been introduced into our country to allow for the on-line identification of citizens. Although these instruments immediately revealed their limits in terms of potential use, they remain valid digital identification tools and, therefore, valid tools by which to allow their holders to acquire a SPID identity, expressing their desire for one.

**c) Computerised identification by means of another SPID digital identity of an equal or higher level of assurance than that requested**[^8].

One SPID identity does not exclude another SPID identity; a single person may have more than one SPID identity. This means that one SPID identity can be used to obtain another SPID identity of equal or lower level, as long as the IdP is the same. This limit is connected with the obligation for the IdP to keep documentation relative to the User’s identification for 20 years. The next IdP cannot, in fact, fulfil this obligation given that the identification was performed by the first IdP.

If we hypothesise that in January 2014, a first digital identity is obtained and a couple of years later (January 2016), it is used to obtain a second one from another provider and, therefore, revocation of the first identity is requested. After twenty years (January 2036), the first IdP can lawfully destroy the evidentiary information kept. The second IdP should keep the evidentiary information until January 2038 but never had such, and it was destroyed by the first provider in January 2036. This problem becomes hugely relevant over time: by repeating the process, the availability period of the information reduces further and further.

---

[^7]: Article 7, paragraph 2, letter b) of the technical rules.
[^8]: Article 7, paragraph 2, letter c) of the technical rules.
The same limit has been adopted to obtain a qualified certificate for an electronic signature, using a SPID digital identity: the IdP and the trust services provider that supplied the qualified certificate must be one and the same. Moreover, the qualified certificate obtained must contain a limit that does not allow it to be used to obtain digital identities from other IdPs.

*d) acquisition of the form for adhering to the SPID, signed by qualified electronic signature or by digital signature*

Another way by which to obtain SPID is identification by means of digital signature. With this tool, it is in fact possible to acquire evidence of the subject’s desire and their identity, at the same time.

e) computerised identification supplied by computer systems that existed prior to the introduction of the SPID, which have adopted, following a specific procedure of the AgID, rules of computerised identification characterised by equal or higher levels of assurance than those defined in this decree

Over time, numerous public administrations have provided citizens with computerised identification credentials. These include around fifty universities, which have assigned their students, after having verified their identity at the secretariats, user IDs and passwords to be used to access university services.

Article 64, paragraph 2 of the CAD rules that with the institution of the SPID system, the public administrations can grant network access to their services only through the SPID system, hence these digital identities can no longer be used. Numerous digital identities have been issued over time using methods that are compatible with those envisaged for the issue of SPID identities, and they constitute information assets.

With this provision, the legislator has solved the problem by envisaging that the Agency can assess the pre-existing data to establish whether or not it is compatible with the technical and regulatory requirements of the SPID system.

**The responsibility of the IdPs**

The identity providers are assigned extensive responsibility, certainly relating to the verification of the identity of the subject applying for a SPID identity and the suitability of the access
credentials supplied, but it does not end here. Article 11 of the technical rules gives a list of obligations assigned to the identity providers, relating to personal data protection, the information security of the entire SPID system, a meticulous running of the service, business continuity, an effective management of any security incidents and the adoption of suitable measures to fight counterfeiting.

In order to be accredited, identity providers fulfil a lengthy process with the Agency, depositing a range of documents, listed in the provision issued by the Agency for the submission of applications for accreditation, which allow it to verify that all legal requirements are met.

In civil terms, identity providers are liable, also in application of European Union legislation, for any damages caused to third parties.

**IdP requirements**

In implementation of the provisions of the CAD, by Decree of the President of the Council of Ministers on 24 October 2014\(^9\), published in Official Journal no. 285 on 09 December 2014, the requirements, role and responsibilities of the “Identity providers” wishing to obtain accreditation from the AgID, were regulated.

Paragraph 3 of Article 10 of the technical rules establishes that, in order to obtain accreditation, the parties concerned must:

1. *have the legal form of a capital company and share capital of at least five million euros*\(^{10}\);
2. *show the necessary organisational and technical capacity to manage the Digital identity*;
3. *use staff with specific knowledge, experience and skills necessary for the services to be supplied. More specifically, staff assigned to the development and management of the computer system must, in connection with the activities to be carried out, have the managerial competence, appropriate knowledge and mastery of the operating and security procedures and technical rules to be applied. The provider ensures the regular professional refresher courses for staff;*

---

\(^9\) Hereinafter, the decree is referred to using the term “technical rules”.

\(^{10}\) It is expected that this will shortly be drastically reduced or eliminated.
4. inform the Agency of the names and professional profiles of the subjects responsible for the specific duties identified in the transposition regulations adopted by the Agency in accordance with Article 4;
5. be in possession of certificates of conformity of the management system used to ensure the security of information relating to such, with standard ISO/IEC 27001, issued by an independent third party authorised to this end in accordance with current applicable regulations;
6. process personal data in compliance with Italian Legislative Decree no. 196 of 30 June 2003 (the “Privacy Code”);
7. be in possession of ISO 9001 quality certification, subsequent amendments or equivalent standards.

Let us now consider these provisions:

1. Capital companies\(^{11}\) are legal forms typical of medium and large enterprises operating in various sectors, whose element of capital prevails over the subjective element (the shareholders). The participation of shareholding in forming the share capital consists of the possession of shares or stocks in the company, depending on the corporate form adopted. These companies have legal personality and perfect financial autonomy, thereby only answering with their own equity. This is why the legislator chose to specify a minimum share capital necessary to allow these activities, fixing it at five million euros. The reason behind the choice lies in the provisions previously in force regarding the digital signature. Under this scope, the CAD prescribed the same corporate form and a share capital of no less than that necessary for the authorisation to conduct banking business, by the Bank of Italy. In the

\(^{11}\) Società per azioni (S.p.A. - joint stock company), Società a responsabilità limitata (S.r.l. - limited liability company), Società a responsabilità limitata semplificata (S.r.l.s. - simplified limited liability company), Società in accomandita per azioni (S.a.p.A. - limited partnership), Società cooperativa (cooperative company) and Società consortile (consortium company).
current wording of the CAD, only the corporate form has remained, whilst the share capital is to be established by specific Decree of the President of the Council of Ministers.

2. “the organisational and technical capacity” is the first requirement aimed at guaranteeing suitable operative capacity by the IdP. The AgID constantly monitors maintenance of this important requirement, which, differently to the previous one, which is aimed at guaranteeing users in the event of any damages, instead seeks to prevent any onset of malfunctions or incidents.

On a case-by-case basis, and with considerable levels of discretion, the AgID assesses the effective “organisational and technical adequacy” of the IdP, as each organisation is a analysed individually.

3. The third requirement aims to verify the suitability of the staff involved in going about the business. The IdP is obliged to regularly train the staff in question, delivery of which will be verified during the Agency supervision.

4. The IdP performs multiple, complex activities. These activities must be rationalised and orderly and their fulfilment requires a suitable number of people. The AgID has therefore identified functional areas for which the IdP is required to appoint managers who have been suitably prepared, and on which continuous, careful supervision takes place at all times.

5. Possession of certificates of conformity with standard ISO/IEC 27001 helps show the organisational capacity and preparation of the subject in terms of its capacity to safeguard the information handled. We would recall that this includes personal data, defined in the technical rules as “attributes”.

6. The obligation to comply with privacy legislation may appear to be superfluous in terms of the general order, but this provision, in this specific context, exposes the transgressing IdP to the risk of the additional sanction of revocation of accreditation.

7. Possession of the certification for the quality management system, ISO 9001, is a further element in support of the IdP’s organisational capacity, implying the presence of a Quality Officer assigned the task of continuously analysing processes, so as to guarantee their adequacy, update and respect.
CREDENTIALS AND LEVELS

The SPID envisages three levels of credentials that do not differ in terms of the strength of the verification of the identity, but rather in terms of the strength of the authentication instruments used:

- Level 1 envisages the use of a suitably robust user ID and password;
- Level 2 adds to the level 1 credentials, requiring a second SYH (Something You Have) type of authentication factor. Telephone devices (mobile telephones, smartphones, etc.) are widely used;
- Level 3 is a level 2 reinforced by the use of X.509 certificates, and therefore asymmetrical cryptography systems whose private keys must reside on devices compliant with Annex III to European Directive 1999/93/EC or Annex II to the eIDAS Regulation.

THE CONSEQUENCES OF IDENTITY THEFT

In the Italian legal system, the party responsible for “identity theft” by means of the counterfeiting of personal identification documents, may be called to answer for various different civil and criminal offences, which can result in up to 14 years of imprisonment.

In this case, the availability of an audio/video recording of the identification procedure can constitute an important element of evidence.

The operators in charge of verifying the identity of applications are also exposed to criminal sanctions in the event of fraud.