TIM id

Service Description

(SPID – Public System for Digital Identities management - DPCM 24.10.2014)

SERVICE DESCRIPTION

VERSIONING		
Rel.	Change description	Date of issue
00	First issue	31/03/2016

Index

1 Introduction 4

2 Survey 4

2.1 Public System for Digital Identities management (SPID) 4

2.2 Main service entities (DPCM 2014 art. 2) 4

2.3 Description of authentication system 5

2.4 Regulatory framework 5

3 Public System for Digital Identities management of Citizens and Businesses (SPID) 6

3.1 Entities and Roles 6

4 Activate the service 6

4.1 Request for membership (o pre-register) 6

4.2 Demonstration and verification (Identification) 7

5 Credentials management 8

5.1 SPID Level 1 management (LoA2 | password) 8

5.2 SPID Level 2 management (LoA3 | password + One Time Password via SMS) 9

6 Authentication 9

6.1 Activity Log 9

6.2 Documents retention 10

6.2.1 Identity Registration 10

6.2.2 Identity change 10

6.2.3 Monitoring and logging of to the service accesses 10

7 Digital identity lifecycle management 10

8 Service activation 11

9 Temporal synchronization of management system 11

10 Privacy and data protection 12

10.1 Data protection mode 12

10.1.1 "Personal data". Definition and identification 12

10.1.2 General obligations 13

10.1.3 Technical and organizational obligations 13

10.1.4 Personal data release 13

11 Definitions 13

12 Acronyms 14

1 Introduction

This document describes "**TIM id", SPID Digital Identity** ("SERVICE"), as well as provisioned by **Telecom Italia Trust Technologies S.r.l.** ("TI.TT"), Identity Provider accredited to SPID, Public System for Digital Identities management, compliant with Italian Law (DPCM 24.10.2014).
This document is available for reading and download to the following link:
https://www.trusttechnologies.it/download/documentazione .

2 Survey

2.1 Public System for Digital Identities management (SPID)

Public System for Digital Identities management of Citizens and Businesses (**SPID**) is an open set of public and private entities, accreditated by AgID – Agenzia per l'Italia Digitale, according to Italian law (DPCM 24.10.2014), to manage registration and availability credentials services and tools access network of Citizens and Businesses.
SPID has a federated model to provide services of Digital Identity to:

- allow independent choice of Identity Provider, by Citizens and Businesses;
- create a free and competitive market to encourage a virtuous competition and a continuous improvement of technological solutions and systems.

2.2 Main service entities (DPCM 2014 art. 2)

SPID provides 4 main entities:
a) **User**, who can have one or more Digital Identities. Those Identities contain some mandatory identification information, such as fiscal code, name, surname, place of birth, date of birth, gender, email address, telephone number;
b) **Identity Provider**. It is an entity, accredited by AgID, who creating and managing digital identities;
c) **Qualifies attributes Manager**. According to current regulations it can certify qualified attributes, such as possession of qualification title, membership of a professional association, specific authorization, etc.
d) **Service Provider**. Public and Private entities who provide online services.

In order to homogenize SPID system to the Citizen and Businesses, Identity Provider (IdP) and Service Providers take the same rules to:

- identification procedures;
- assignment of access credentials;
- access to federated services.

The purpose is allow to Citizens and Businesses to choose the Identity Provider independently.

2.3 Description of authentication system

Electronic authentication process has the purpose to verify the digital identity associated to the entity, previously to use the online service.

Electronic authentication is associated with a security level or guarantee level – *Level of Assurance* (LoA) – progressively increasing.

Authentication processes, managed by TI Trust Technologies, qualify two SPID Level of Assurance, such as defined by AgID:

- **Level 1** (LoA 2 according to ISO/IEC 29115 standard) requires authentication systems with userID/ password; it is appropriate in case the potential damage, by an improper use of Digital Identity, has a low impact on the Citizens and Businesses activities;
- **Level 2** (LoA3 according to ISO/IEC 29115 standard) requires a multifactor electronic authentication process, like userID/ password + OTP (One Time Password); this level is appropriate in case the potential damage, by an improper use of Digital Identity, involves significant damages for all services.

SPID system provides a **Level 3** (LoA4 according to ISO/IEC 29115 standard). It is an electronic authentication process "two-factor" based on digital certificates and private keys custody criteria on Directive 1999/93/CE compliant devices. This is the highest level of assurance to be associated when improper use of Digital Identity can those services involve serious and grave damages for all services.

2.4 Regulatory framework

Main regulations about SPID are listed in the table below.

For further details, please refer to SPID Certification Practice Statement ("*Manuale Operativo del servizio TIM id*"), available to the follow link https://www.trusttechnologies.it/download/documentazione/ .

Regulations	Description
Decreto legislativo 7 marzo 2005, n. 82, e successive modificazioni, recante il Codice dell'amministrazione digitale (CAD) Capo V "Dati delle pubbliche amministrazioni e servizi in rete" Sezione III - Servizi in rete	L'art.64 c.2 in particolare stabilisce: "*Le pubbliche amministrazioni possono consentire l'accesso ai servizi in rete da esse erogati che richiedono l'identificazione informatica anche con strumenti diversi dalla carta d'identità elettronica e dalla carta nazionale dei servizi, purché tali strumenti consentano l'individuazione del soggetto che richiede il servizio. Con l'istituzione del sistema SPID di cui al comma 2-bis, le pubbliche amministrazioni possono consentire l'accesso in rete ai propri servizi solo mediante gli strumenti di cui al comma 1, ovvero mediante servizi offerti dal medesimo sistema SPID. L'accesso con carta d'identità elettronica e carta nazionale dei servizi è comunque consentito indipendentemente dalle modalità di accesso predisposte dalle singole amministrazioni*"
Decreto del Presidente del Consiglio dei Ministri 24 ottobre 2014 (GU n.285 del 9.12.2014)	"Definizione delle caratteristiche del sistema pubblico per la gestione dell'identità digitale di cittadini e imprese (SPID), nonché dei tempi e delle modalità di adozione del sistema SPID da parte delle pubbliche amministrazioni e delle imprese."
Determinazione AgID n. 44/2015 del 28 luglio 2015	Emanazione dei regolamenti SPID di cui all'art l'Art. 4 commi 2,3 e 4 del DPCM 24 ottobre 2014: • Regole Tecniche;

- modalità attuative per la realizzazione dello SPID;
- modalità di accreditamento dei soggetti SPID;
- procedure necessarie a consentire ai gestori dell'identità digitale, tramite l'utilizzo di altri sistemi di identificazione informatica conformi ai requisiti dello SPID, il rilascio dell'identità digitale

3 Public System for Digital Identities management of Citizens and Businesses (SPID)

Main purpose of **SPID system** is to define a safe effective and economical environment to allow access, for Citizens and Businesses, to all services by public administrations and by service provider, using IT systems in compliance to digital strategy.

Public and private entities, owners of requirements requested by AgID, according to operational mode, manage registration services and making available credential and network access tools to natural person or legal entity on behalf of Public Administrations, as providers of network services, or directly on demand of the interested parties.

To ensure system uniformity in favor of the Citizens, Identity Providers (IDP) and Service Providers (SP) follow the same identification actions:

- in the procedures of credentials recognition and allocation;
- to services access.

3.1 Entities and Roles

In addition to the entities in art. 2 of DPCM 24.10.2014, there are more entities and roles involved in the operational model:

- ***User*** (Citizens or Business), which can be new customer or already owner of a digital identity;
- ***Identity Provider*** (IDP), who has the responsibility to issue and/or manage user credentials (eg. Password), to set hardware, software and data to produce credentials;
- ***Registration Authority*** (RA), who verifies and guarantees the user digital identity to an Identity Provider;
- ***Authentication Authority*** (or *auditor)*, which verifies the identity information;
- ***Service Provider*** (SP), *trusted* Third Party, or his representative, recognize as trusted in relation to specific activities (es. a Public Administration).

Those entities may belong to a single organization or a separate organizations.

4 Activate the service

4.1 Request for membership (o pre-register)

Digital identities are issued by Identity Provider on request of an interest person, submitting a **request for membership module**, through the digital identity management service portal that requires all information necessary to identify person requesting the service and manages relationship between IDP and the Citizens or Businesses.
The information required are:

Natural person
Primary attributes
Name and Surname
Gender, birth date and birth place
Fiscal code
ID document personal data
Secondary attributes
UserID
Mobile number
Email
Residency
Domicile (if different from residency)

Legal entity
Primary attributes
Company name
Fiscal code or VAT (if the same than Fiscal code)
Legal residence
Natural person (Legal representative of the Company)
ID document personal data
Certificate attesting the role of Legal representative
Secondary attributes
UserID
Telephone number
Mobile number
Email
Domicile (if different from Legal residence)

The applicant chooses identification mode and receives an email confirmation.
It contains registration summary data and *Registration Code* which will be needed in the next phase of identification.

4.2 Demonstration and verification (Identification)

In this step, Identity Provider acquires necessary information to identify the applicant, based on SPID specific level of assurance.

Identity verification[1] allows data control provided in pre-registration process, through automation applications (databases) or manual checks.

TI Trust Technologies provides two identification modes:

a) "**on sight**", through exhibition of an ID document (so called "de visu") at the Registration point. This mode provides:

- the applicant must go to the Registration point with own Registration code, obtained in step 1, and exhibits to view a valid ID document to the staff for required checks;
- the applicant examines and subscribes the appropriate Registration form and related documents;
- the staff request to proceed with the issue of SPID credentials, to IDP (TI Trust Technologies).

b) Through use of **qualified electronic signature**. In this mode applicant can requires independently SPID identity:

- connecting to the IDP web portal and opens the procedure with Registration code obtained in step 1;
- downloading and subscribing the Acceptance form with own qualified electronic signature (PAdES standard) and uploading;
- IDP system confirms the result of operation and informs the applicant about the way he will receive SPID credentials;
- In case of failure, IPD system sends an email to applicant with the refusal reasons and possible request for additional documentation.

c) Through **Carta Nazionale dei Servizi** (CNS). The applicant can require independently SPID identity, like b) mode:

- connecting to the IDP web portal and opens the procedure with Registration code obtained in step 1;
- downloading and subscribing the Acceptance form with own CNS and uploading;
- IDP system confirms the result of operation and informs the applicant about the way he will receive SPID credentials;
- In case of failure, IPD system sends an email to applicant with the refusal reasons and possible request for additional documentation.

IDP provides to archive all documents produced.

[1] Identity verification is different from identity proof because it implies the validation of information through additional source – authoritative source, in particular using first the services referred to art. 4, par. 1, letter c) of DPCM SPID (AgID agreements) and, in case where necessary information is not available by conventional services, it will be thought documents, data or information obtained from the certifying administration achive, in accordance to art. 43, par. 2 of D.P.R. 28.12.2000, n. 445.

5 Credentials management

Credentials management concerns all processes involving the entire life cycle credentials. It changes according to authentication level (Level 1 or Level 2) chooses by Service Provider and to Level of Assurance (LoA) associated to mode, according to ISO/IEC 29115 standards.

5.1 SPID Level 1 management (LoA2 | password)

IDP system provides to delivery userID and password (alphanumeric) in the following way:

a. userID by email, to address indicated by applicant during registration;
b. Password (to be changed at first login) via SMS, to mobile number indicated by applicant and verified during registration.

On first access users entered the password received via SMS and will set a new password.

When the operation ends, IDP system confirms to user SPID credentials activation.

5.2 SPID Level 2 management (LoA3 | password + One Time Password via SMS)

The delivery process follows procedures provided for SPID Level 1.

Level 2 provides a “token”, received via SMS, to be use once during service session.

6 Authentication

Authentication step verifies one credential possession and/or control from the user. This allows to establish the user identity really is the one, in order to allow access.

Verification process implemented by IDP is able to ensure the security levels required by regulations (Level 1 – LoA2 of the ISO/IEC 29115 standards; Level 2 – LoA3 of the ISO/IEC 29115 standards; Level 3 – LoA4 of the ISO/IEC 29115 standards).

TI Trust Technologies has realized the following authentication modes:

- **Level 1** (LoA2 of the ISO/IEC 29115 standards). It requires the insertion of userID and password. Security level is guaranteed by password complexity which is in line with relevant AgID regulations and indication. SPID system provides temporary block of the credentials after a number, configured, of authentication attempts that have not gone well.
- **Level 2** (LoA3 of the ISO/IEC 29115 standards). It requires the insertion of userID and password + entering of OTP code received via SMS by user, with limited lifetime. Security level is guaranteed by mobile number owned by user, previously verified. SPID system provides temporary block of the credentials after a number, configured, of authentication attempts that have not gone well.

6.1 Activity Log

The activity log is archiving process and secure storage relating to Registration step, in which you create a specific electronic file. It contains information and documentation collected during registration step, information about identity verification process, results of these steps and other relevant data.
The type of stored information varies:

- according to the user identification processes;
- according to data type to be stored.

Activity logs are maintained throughout the credential life cycle, with the aim of documenting its creation, digital identity, the assignee and credential status.

6.2 Documents retention

6.2.1 Identity Registration

It is archiving and secure storage of information collected by activity log during identity registration and verification steps.
All documentation relating to the registration process is stored and managed according to art. 7, par. 8 and 9 of the SPID DPCM.
IDP will have to keep them for the whole contract period and send them, at the contract expiration, to AgID or entity specified by it.

6.2.2 Identity change

All documentation submitted during digital identity editing task (suspension or revocation request modules, attached recognition documents, notifications of loss, notification of digital identity variation status) is kept by I IDP will have to keep them for the whole contract period and send them, at the contract expiration, to AgID or entity specified by it DP for the whole contract period.

6.2.3 Monitoring and logging of to the service accesses

You may need a monitoring events and logging activity due to the type of service, according to legal or compliance requirements.
Tracking of each access credentials use event and continuous monitoring to detect any misuse (or attempted violation of digital identity credentials), allows you to enable preventive digital identity suspension action, in case of suspicious activity.
Collected tracing information will be kept for the time required by regulations.
Data retention will allow to realize detailed analysis in case of fault or any dispute with third parties.

7 Digital identity lifecycle management

IDP Platform capabilities allow identities management during their entire lifecycle. In particular:

- **Viewing identities activity**, through a report available by a specific SPID web interface;
- **Change of identity**, intended as personal data self-change (non-identifying data), by specific web interface, to demand the change of initially assigned credentials (procedures depending on authentication level chosen);
- **Revocation of identity**, optional or mandatory:
    - on holder request;
    - suspected abuse or falsification;
    - death natural person/ termination legal person;
    - inactivity for 24 consecutive months, upon notice of IDP;
    - modification or expiration of the relationship between owner and administration on behalf of which the identity is used;
    - removal from office, title or by the representation role the identity is used;
    - any reasoned request by the Judicial.

  The revocation of digital identity is notified to the holder through way, considered appropriate by IDP, indicating reasons, date and time it runs.
  Revocation causes the **immediate and definitive cessation of its validity**.

- **Suspension** of identity, in case the IDP does not have the ability to determine in time the authenticity of the request for revocation. The suspension of digital identity is notified to the holder by any means considered appropriate by the IDP. The suspension of a digital identity determines the immediate cessation of its validity, independently from the expiration date, up to the time of its re-activation, but does not affect the validity of digital identity in the time prior to the suspension.
- **Reactivation**, on owner or appointed request, in case of previously suspended identity. Digital identity reactivation determines the immediate resumption of its validity, until the time it expires. Reactivation will be notified to the holder by any means considered appropriate by the IDP.

For further information, please refer to SPID Certification Practice Statement ("*Manuale Operativo del servizio TIM id*"), available to the follow link https://www.trusttechnologies.it/download/documentazione/.

8 Service activation

A Service Provider (SP), eg. Public Administration, whishing to join to SPID service will have to initiate an accession procedure, after which it may require the activation of its users (already surveyed or new) to allow them to access to available services.

In the case of users migration already registered on the SP portal, the IDP will proceed to the acquisition of a file with a specific record layout, according to regulation. The identity activation request process can be automated.

If the request comes from a new user, he may require digital identity registration by following the procedure provided by SP.

9 Temporal synchronization of management system

As required by regulations, time references applied to IDP systems registrations and to time stamps issued, are considered temporal validation able to be opposed to third parties.
TI Trust Technologies as accredited Certifier has a temporal reference system that guarantees all its services operating in accordance with the requirements of current legislation.

10 Privacy and data protection

Considering the great importance gived to personal data treatment in Telecom Italian Group, it is operating an internal organizational and regulatory system to ensure that all personal data are carried out in compliance with current legislation and according to fairness and lawfulness principles declared in the Group's Code of Conduct. The measures planned and implemented by Telecom Italian Group system also incorporate the minimum measures laid down by **Code for Personal Data Protection** (D.Lgs. 196/03).

10.1 Data protection mode

Personal data of the applicant, the holder of certificates, the third party and anyone who accesses to the service, required for registration step, they are processed, preserved and protected by IDP in accordance with the regulations D.Lgs. n. 196 of 30.06.2003 (so-called "Privacy Code") and subsequent measures issued by the Authority for personal data protection.

The figures identified according to D.Lgs. 196/03 are partially different from those listed in CAD and in the DPCM 2009:

a) **Data Controller**, means the natural and legal person, public administration or any other public authority, association or organization responsible for decisions regarding the purposes and methods of personal data processing, including the security profile (IDP);
b) **Data processor**, means the natural person, legal person, public administration or any other public authority, association or organization appointed by the Holder to personal data processing;
c) **Commissioner**, means a natural person authorized to perform personal data processing by Data Controller or Data processor;
d) "**Interested person**", means natural person, legal person, public authority or association to whom personal data (i.e. the applicant, the personal data owner or anyone accessing the service).

10.1.1 “Personal data”. Definition and identification

According to art. 1, par. 2, letter. b) of D.Lgs. 196/03, for “personal data” means “*any information concerning a natural person, legal person, public authority or association, identified or identifiable, also through reference to any other*

information including a personal identification number". Therefore personal data are also the identification codes provided by the IDP, the pointers and the PIN (Personal Identification Number).

Personal data can also be those relating the user, or to any third parties, and contained in the information fields on forms and archives - electronic or paper – for registration, request for suspension, reactivation and revocation, change of vital statistic, change attributes or digital identity credentials. In order to ensure appropriate treatment, the security measures provided by IDP, and analytically described in the Security Plan, are made in accordance with D.Lgs. no. 196/03.

10.1.2 General obligations

In general terms, the IDP prepares, maintains and updates, as part of activities of Identity Provider, a Register of informatics and paper archives containing personal data, embedded in the Data Controller data banks used in the management of all Identity Provider activities phases.

10.1.3 Technical and organizational obligations

From a technical point of view, the IDP (or the Data processor) through its Commissioner, take appropriate actions in relation to personal data recording, processing, preservation, protection, deletion / destruction, according to the detailed modalities in the CPS.

10.1.4 Personal data release

The Interested has the right to request and obtain, from IDP, the information to his personal data, in accordance to Art. 7 of D.Lgs. no. 196/03.

The IDP, in carrying out identity providers activities, can make communication operations and dissemination of personal data.

In particular:

- the personal data may be communicated to the Judicial, in accordance with current regulation provisions;
- particular contractual agreements may provide further recipients and communication forms other than CAD and DPCM 2009, in accordance with current regulations anyway.

Except as required by CAD and by DPCM 2009, about the publication of the certificate revocation lists, the reasons for certificates revocation or suspension can only be disclosed with the explicit agreement permission.

11 Definitions

According to current regulations and to interpret IDP's CPS, it will follow a list of terms and expressions with the corresponding meaning. For definitions adopted by the relevant regulations, please refer to the texts in force.

Terms and expressions not defined shall have the meaning give to them in the paragraph or section that contains them. Where it is appropriate is generally used in the technical literature also referred to the corresponding English word, and in standards.

Subscription: is the first step of the registration process, where an entity joins to SPID system, providing all data and documentation required.

Authentication: guarantee available on the entity's identity (ISO-IEC 18014-2).

Multi-factor authentication: authentication with at least two independent authentication factors (ISO-IEC 19790).

Credential: a set of data presented as evidence of a claimed identity or of a right. The holder/user uses this attribute (single or dual factor) along with identification code (both released by IDP) to have secure access, via computer authentication, to qualified services provided by Service Providers (government and private) joined to SPID.

Service Provider (SP): the service provider of the information society defined by art. 2, par. 1, letter a), of D.Lgs. no. 70 of 09.04.2003, or services of an administration or of a public authority provided by users through information systems accessed on the network. Service providers submit the user requests for information identifying to IDP and they receive the results. Service providers, accepting digital identity, do not discriminate people based on IDP that makes SPID Identity available.

Digital Identity Management (Identity Provider, IDP): provider of digital identity management services, TI Trust Technologies company, which provides the service in accordance with regulations.

Digital identity: the electronic representation of biunivocal correspondence between a user and his identity attributes, verified through the set of data collected and stored in digital form.

Commissioner: the natural or legal person to whom the manager made responsible for making his own, under its responsibility, according to the instructions given by himself and using the tools that he himself indicated, the identification and registration operation. The Commissioner, in some cases it is also responsible for delivery of holder credentials, or systems to produce credentials.

CPS (Certificate Practice Statement): the public document that defines operating mode of IDP service.

OTP: a One-Time Password (password used only once) is a password that is valid only for a single transaction.

Public Administration: the administrations referred to art. 1, par. 2 and to art. 70, par. 4 of the D.Lgs. 30.03.2001, no. 165.

Applicant: is the natural person requesting membership. If natural person is not an entity (eg. legal person) it must have ownership or powers of attorney to act on behalf of the entity.

Registration: the process that starts with initial adhesion and is completed with successful recording of the new digital identity and with release of credentials, as a result of demonstration and validation steps (ISO-IEC 29003).

SPID: Public Sistem for Digital Identities management, established in accordance with art. 64 of CAD, amended by art. 17-ter of D.L. 21.06.2013, no. 69, ratified with amendments, by the L. 09.08.2013, no. 98.

Owner: is the natural person or legal person to which is assigned SPID digital identity, corresponding to the User entity of DPCM art. 1 par. 1, letter v).

Titolare: è il soggetto (persona fisica o giuridica) a cui è attribuito l'identità digitale SPID, corrisponde all'utente del DPCM art. 1 comma 1 lettera v).

12 Acronyms

Agenzia per l'Italia Digitale (AgID). Art. 20, par. 2, of the L. 134/2012 assigns to the Agency the execution of the coordination functions, guidance and control previously entrusted to DigitPA, as well as the issuance of mandatory opinions on contractual schemes concerning IT and electronic goods and services, in accordance with art. 3 of the D.Lgs. no. 177/2009. In particular it is also attributed to the Agency consulting and proposal functions, (already provided for in art. 3, par. 2, letter a) of the D.Lgs. no. 177/2009) and the issue of assessments and optional opinions (in accordance with the art. 3, par. 2, letter c) of D.Lgs no. 177/2009 and art. 20, par. 3, letter l) of L. 134/2012) .

DPCM SPID: DPCM of 24.10.2014 (published in the GU, Serie Generale no. 285 of 09.12.2014), which define the SPID characteristics, as well as the times and procedures for adopting SPID system by public administrations and businesses.

HTTP (HyperText Transfer Protocol): transmission protocol which allows the exchange of files (text, graphic images, sound, video or other multimedia files) on the World Wide Web.

IDP: Identity Provider (SPID digital identity manager).

INTERNET: a global system of computer networks in which users of computers can get information from different places. Its widespread use was mainly caused by the introduction of transmission protocols with hypertext references documents (HTTP) and the development of the World Wide Web (WWW).

ISO – **International Standards Organization**: consists of national agencies from more than 75 Countries. It has established numerous standards in the information systems area. The ANSI (American National Standards Institute) is one of the main agency belonging to ISO.

ITU-T – International Telecommunication Union, Telecommunication Standardization Sector.

LoA – Level of Assurance.

PIN – Personal Identification Number.

TI.TT – Telecom Italia Trust Technologies S.r.l.

TI – Telecom Italia