# In.Te.S.A. S.p.A.
# Identity Provider SPID
## Qualified Trust Service Provider
### ai sensi del Regolamento (UE) N. 910/2014 (eIDAS)

# Guida utente servizio SPID

*Codice documento: INTQS_SPID-GU*

*OID: 1.3.76.21.10.200.3*

*Redazione: Simone Baldini*
*(Resp. aggiornamento documentazione)*

*Revisione: Antonio Raia*
*(Resp. verifiche e ispezioni)*

*Approvazione: Matteo Panfilo*
*(CSO - Chief Solutions Officer)*

*Data emissione: 28/07/2022*

*Versione: 05*

*Questa pagina è intenzionalmente priva di contenuto.*

## Revisioni

| | | | |
|---|---|---|---|
| ***Versione n°: 05*** | | ***Data Revisione :*** | ***28/07/2022*** |
| Descrizione modifiche : | Aggiornamento gestione SPID Minori<br>Aggiornamento logo IntesaID | | |
| Motivazioni : | Aggiornamenti | | |
| ***Versione n°: 04*** | | ***Data Revisione :*** | ***21/12/2021*** |
| Descrizione modifiche : | Aggiornamento dati societari e logo<br>Correzione refusi | | |
| Motivazioni : | Variazione proprietà, direzione e coordinamento | | |
| ***Versione n°: 03:*** | | ***Data Revisione*** | ***13/04/2020*** |
| Descrizione modifiche: | Aggiornamento layout grafico<br>Inserimento voce di sospensione per documento scaduto<br>Inserimento procedura di rinnovo della credenziale<br>Variazione codice documento<br>Inserimento codice OID del documento | | |
| Motivazioni : | Aggiornamenti | | |
| ***Versione n°: 02*** | | ***Data Revisione :*** | ***13/03/2019*** |
| Descrizione modifiche | Aggiornamento immagini schermate utente<br>Aggiornamento layout grafico<br>Eliminazione ridondanze | | |
| Motivazioni : | Aggiornamenti | | |
| ***Versione n°: 01*** | | ***Data Revisione :*** | ***23/08/2016*** |
| Descrizione modifiche : | Nessuna | | |
| Motivazioni : | Prima emissione | | |

# Sommario

## Riferimenti Normativi

| | |
|---|---|
| ***CAD***<br>e ss.mm.ii. | Decreto Legislativo 7 marzo 2005, n. 82.<br>"Codice dell'amministrazione Digitale".<br>Nel seguito indicato anche solo come *CAD*. |
| ***Determina Minori*** | Determinazione AgID n. 133 dell'11 maggio 2022 recante ' Linee Guida operative per la fruizione dei servizi SPID da parte dei minori' – Seconda emissione |
| ***DPCM***<br>e ss.mm.ii. | DECRETO DEL PRESIDENTE DEL CONSIGLIO DEI MINISTRI 24 ottobre 2014<br>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.<br>Nel seguito indicato anche solo come *DPCM.* |
| ***REGOLAMENTO***<br>e ss.mm.ii. | REGOLAMENTO RECANTE LE MODALITÀ ATTUATIVE PER LA REALIZZAZIONE DELLO SPID<br>Nel seguito indicato anche solo come *CAD* ovvero *Modalità Attuative.* |
| ***GDPR***<br>e ss.mm.ii. | GENERAL DATA PROTECTION REGULATION<br>REGOLAMENTO (UE) 2016/679 del Parlamento Europeo e Del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)<br>Nel seguito indicato anche solo come *GDPR.* |
| ***Reg. eIDAS***<br>e ss.mm.ii. | Regolamento (UE) N. 910/2014 del Parlamento Europeo e del Consiglio del 23 luglio 2104, in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la direttiva 1999/93/CE.<br>Nel seguito indicato anche solo come *Reg. eIDAS.* |

## Definizioni

| | |
|---|---|
| ***AgID*** | Agenzia per l'Italia Digitale, istituita ai sensi dell'articolo 19 del DL 22.06.2012, n. 83, convertito in legge, con modificazioni, dall'art. 1 della legge 7.08.2012, n. 134, e successive modifiche ed integrazioni |
| ***Attributi*** | Le informazioni o qualità di un Utente utilizzate per rappresentare la sua identità, il suo stato, la sua forma giuridica o altre caratteristiche peculiari |
| ***Attributi Identificativi*** | Il nome, cognome, luogo e data di nascita, sesso, ovvero ragione o denominazione sociale, sede legale, nonché codice fiscale o partita IVA ed estremi del documento d'identità utilizzato ai fini dell'identificazione; |
| ***Attributi secondari*** | Il numero di telefonia mobile, indirizzo di posta elettronica, domicilio fisico e digitale, nonché eventuali altri attributi individuati da AgID, funzionali alle comunicazioni |
| ***Credenziali di Accesso*** | Con riferimento ai livelli di sicurezza SPID definiti dalle specifiche dell'Agenzia per l'Italia Digitale, si distinguono:<br>a) una UserID e una Password, scelte dall'Utente, per l'accesso al Servizio con livello di sicurezza 1 (LIVELLO 1);<br>b) una UserID e una Password, abbinati ad un codice OTP [One-Time Password] ricevuto via sms dall'Utente al numero di cellulare dichiarato in fase di Registrazione, per l'accesso al Servizio con livello di sicurezza 2 (LIVELLO 2); |
| ***Fornitore di Servizi*** | Il fornitore dei servizi della società dell'informazione definiti dall'art. 2, c. 1, lett. a), del decreto legislativo 9.04.2003, n. 70, o dei servizi di un'amministrazione o di un ente pubblico erogati agli Utenti attraverso sistemi informativi accessibili in rete, ai sensi dell'art. 1, lett. i) del D.P.C.M. |
| ***Gestore o Identity Provider (IdP)*** | Intesa (come di seguito definita e identificata) che, quale soggetto accreditato al sistema SPID e, in qualità di gestore di servizio pubblico, previa identificazione certa dell'Utente, assegna, rende disponibile e gestisce gli Attributi utilizzati dall'Utente al fine della sua identificazione informatica. Intesa, inoltre, fornisce i servizi necessari per la distribuzione e l'interoperabilità delle Credenziali di Accesso, la riservatezza delle informazioni gestite e la loro Autenticazione Informatica |

| | |
|---|---|
| ***Identità Digitale*** | La rappresentazione informatica della corrispondenza biunivoca tra un Utente e i suoi Attributi Identificativi, verificata attraverso l'insieme dei dati raccolti e registrati in forma digitale secondo le modalità di cui al D.P.C.M 24.10.2014 e dei suoi regolamenti attuativi; |
| ***Manuale operativo*** | Il documento pubblicato sul sito web del Gestore e depositato da Intesa presso l'Agenzia per l'Italia Digitale che ha lo scopo di descrivere le regole e le procedure operative adottate dal Gestore per la messa a disposizione e la gestione degli Attributi utilizzati dall'Utente al fine di identificazione informatica attraverso SPID |
| ***SPID o Servizio*** | Il Sistema Pubblico dell'Identità Digitale, istituito ai sensi dell'articolo 64 del D.Lgs. 5.03.2005, n. 82 e ss.mm.ii. al quale aderiscono le pubbliche amministrazioni e le imprese secondo le modalità previste dal DPCM 24/10/2014 e ss.mm.ii. |
| ***Titolare / Utente*** | la Persona Fisica o Giuridica cui è attribuita una Identità Digitale. È il soggetto che deve essere identificato dall'IdP, per utilizzare i servizi erogati in rete da un Fornitore di Servizi |

## *Dati identificativi del Gestore (IdP)*

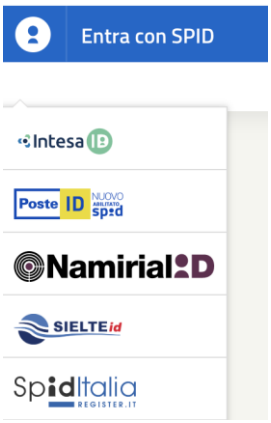
| | |
|---|---|
| *Denominazione sociale* | In.Te.S.A. S.p.A. |
| *Indirizzo della sede legale* | Strada Pianezza, 289 - 10151 Torino |
| *Legale Rappresentante* | Amministratore Delegato |
| *Registro delle Imprese di Torino* | N. Iscrizione 1692/87 |
| *N. di Partita I.V.A.* | 05262890014 |
| *N. di telefono (centralino)* | +39.011.19216.111 |
| *Sito Internet* | *www.intesa.it* |
| *Indirizzo di posta elettronica* | *marketing@intesa.it* |
| *ISO Object Identifier (OID)* | 1.3.76.21 |

## A. Modalità d'uso del sistema di autenticazione

Il momento in cui un utente può iniziare ad utilizzare la propria Identità Digitale, dopo l'attivazione dell'utenza da parte del Gestore, si presenta quando quest'ultimo si collega al sito web di uno degli enti (pubblici o privati) che forniscono la possibilità di autenticarsi utilizzando le credenziali SPID.

Questi soggetti, chiamati *Fornitori di Servizi*, o *Service Provider* (*SP*), saranno riconoscibili dal bottone "*Entra con SPID*" esposto all'interno del proprio portale:

Il Fornitore di Servizi, per individuare il *Gestore dell'Identità* (*IdP*) in grado di autenticare l'utente, chiederà l'informazione direttamente al fruitore del servizio: cliccando sul bottone "*Entra con SPID*" sarà visualizzato un elenco dal quale sarà possibile selezionare il Gestore dell'Identità Digitale che si intende utilizzare.




Una volta selezionato il Gestore delle Identità con cui si desidera effettuare l'autenticazione, si verrà indirizzati verso una schermata di login, la quale sarà già impostata per richiedere il livello di sicurezza SPID e gli attributi necessari ad abilitare l'accesso al servizio richiesto presso il Fornitore dei Servizi.

La schermata di login visualizzata dal Gestore delle Identità Digitali sarà differente in base al livello di sicurezza SPID al quale si attesta la credenziale necessaria per accedere al servizio richiesto, per via delle diverse informazioni necessarie per l'autenticazione.

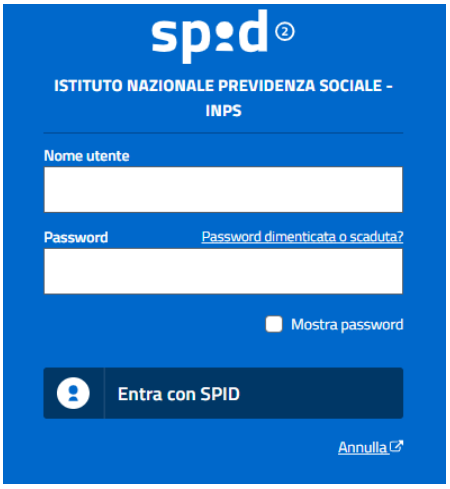
Una volta inserite le credenziali su tale schermata, si verrà reindirizzati nuovamente presso il sito web del Fornitore dei Servizi presso il quale si è richiesto l'utilizzo del servizio. Se il processo si conclude positivamente (le credenziali sono state inserite correttamente e si possiede un'Identità Digitale abilitata per il livello richiesto), ci si troverà autenticati all'interno del portale del Fornitore dei Servizi e abilitati all'utilizzo dei servizi richiesti.

### *Livello 1 SPID*

Nel caso di accesso con livello di sicurezza *SPID livello 1*, sarà richiesto solamente l'inserimento di *Nome utente* (cioè l'indirizzo e-mail con cui ci si è registrati) e della *Password*.

### *Livello 2 SPID*

Nel caso di accesso con livello di sicurezza *SPID livello 2*, sarà richiesto un ulteriore fattore di autenticazione, oltre all'inserimento del *Nome utente* (cioè l'indirizzo e-mail con cui ci si è registrati), della *Password*:



Quindi, se i suddetti dati sono stati inseriti in modo corretto, sarà richiesta la digitazione del *codice OTP* (One Time Password) ricevuto via sms ovvero via e-mail nel caso di minori, secondo le modalità descritte nel Manuale Operativo e in adempimento all'Art. 6, comma 1, lettera b) del DPCM 24 ottobre 2014 (di seguito anche *DPCM*):


***Autenticazione del minore***

Nel caso di identità SPID rilasciata a minorenni, così come previsto dalle Linee Guida di cui alla Determina Minori, esistono due procedure per consentire l'autenticazione del minore e, di conseguenza, permettergli la fruizione dei servizi online tramite accesso SPID.

**Procedura A**

Questa procedura si applica a tutti i casi in cui il Service Provider, sulla base della valutazione effettuata ai sensi della LLGG di cui alla Determina Minori, con riferimento alla tipologia e alla finalità del servizio erogato, NON DEVE richiedere al Genitore l'autorizzazione all'accesso al servizio da parte del minore, in relazione ai servizi erogati dagli istituti scolastici di ogni ordine e grado nonché ai servizi di prevenzione o di consulenza forniti direttamente al minore. Tale processo è sostanzialmente analogo a quello sopradescritto per l'accesso con Livello 2 o Livello 1 SPID, salvo il fatto che il Gestore Intesa, oltre a verificare le credenziali inserite, verifica anche che colui che richiede l'autenticazione abbia un'età coerente per il tipo di servizio acceduto.

**Procedura B**

La presente procedura si applica a tutti i casi in cui il Service Provider (SP), sulla base della valutazione effettuata ai sensi della LLGG di cui alla Determina Minori, con riferimento alla tipologia e alla finalità del servizio erogato, DEVE richiedere al Genitore l'autorizzazione all'accesso al servizio da parte del minore.

Fermo restando che i minori che non hanno ancora compito il 14-esimo anno di età possono accedere unicamente ai servizi online resi disponibili dagli istituti scolastici e che tale accesso è inserito fra quelli previsti dalla precedente Procedura A, la presente Procedura B si applica ai soli minori a partire da 14 anni, nell'accesso ai servizi non ricompresi fra quelli di prevenzione o di consulenza forniti direttamente al minore.

Tale processo è sostanzialmente analogo a quello sopradescritto per l'accesso con Livello 2 o Livello 1 SPID, salvo il fatto che il Gestore Intesa:

a) Verifica che il minore che richiede l'autenticazione abbia un'età coerente per il tipo di servizio acceduto;
b) Comunica al minore la necessità di richiedere l'autorizzazione del Genitore (o esercente la responsabilità genitoriale) a cui è collegata la propria identità SPID per l'accesso al servizio richiesto
c) Previa conferma del minore, notifica il Genitore di cui al punto precedente la richiesta di autorizzazione all'accesso specificando nome e cognome del minore, la data, l'ora e la denominazione del SP per cui si richiedere l'autorizzazione.
d) Ottenuta l'autorizzazione da parte del Genitore, consente al minore l'accesso al servizio.

***Livello 3 SPID***

Non ancora gestito dall'Identity Provider.

# B. Revoca e sospensione dell'Identità Digitale

La *Revoca* è il processo che annulla definitivamente (in modo *irrevocabile*) la validità delle credenziali. Diversamente, la *Sospensione* è associata ad un processo di annullamento temporaneo.

Il minore infraquattordicenne non avrà accesso alle suddette funzioni.

Il minore ultraquattordicenne avrà solamente accesso alla funzione di sospensione della propria identità digitale.

## *B.1 Modalità per la richiesta di revoca o sospensione dell'Identità Digitale*

Ai sensi dell'articolo 8, comma 3, e dell'articolo 9 del DPCM, il Gestore **revoca** l'Identità Digitale nei casi seguenti:

1. risulta non attiva per un periodo superiore a 24 (ventiquattro) mesi;
2. per decesso della persona fisica;
3. per uso illecito dell'Identità Digitale;
4. per richiesta dell'utente;
5. per scadenza contrattuale.

**In tutti i casi previsti dai punti 1) e 6)**, il Gestore revoca di propria iniziativa l'Identità Digitale, mettendo in atto meccanismi con i quali comunica la causa e la data della revoca all'utente, con avvisi ripetuti 90 (novanta), 30 (trenta) e 10 (dieci) giorni prima della data di revoca, nonché il giorno precedente la revoca definitiva, utilizzando l'indirizzo di posta elettronica e il recapito di telefonia mobile (attributi secondari essenziali forniti per la comunicazione).

**Nei casi previsti dai punti 2) e 3)**, il Gestore procede alla revoca dell'Identità Digitale, previo accertamento operato anche utilizzando i servizi messi a disposizione dalle convenzioni di cui all'articolo 4, comma 1, lettera c) del DPCM. In assenza di disponibilità dei predetti servizi, dovrà essere cura dei rappresentanti del soggetto utente (eredi o procuratore, amministrazione, società subentrante, etc.) presentare la documentazione necessaria all'accertamento della cessata sussistenza dei presupposti per l'esistenza dell'Identità Digitale. Il Gestore, una volta in possesso della documentazione suddetta, dovrà procedere tempestivamente alla revoca.

**Nel caso previsto dal punto 4)**, cioè nel caso in cui l'utente ritenga che la propria Identità Digitale sia stata utilizzata fraudolentemente, lo stesso può chiederne la ***sospensione*** con una delle seguenti modalità:

- richiesta al Gestore inviata via PEC;
- richiesta, in formato elettronico e sottoscritta con firma digitale o firma elettronica qualificata, inviata tramite la casella di posta appositamente predisposta dal Gestore.

Il Gestore deve fornire esplicita evidenza all'utente dell'avvenuta presa in carico della richiesta e procedere alla immediata sospensione dell'Identità Digitale.

Trascorsi 30 (trenta) giorni dalla suddetta sospensione, il Gestore provvede al *ripristino* dell'identità precedentemente sospesa qualora non riceva copia della *denuncia presentata all'autorità giudiziaria* per gli stessi fatti sui quali è stata basata la richiesta di sospensione.

**Nel caso previsto dal punto 5)**, l'utente può chiedere al Gestore dell'Identità Digitale, in qualsiasi momento e a titolo gratuito, la *sospensione* o la *revoca* della propria Identità Digitale seguendo modalità analoghe a quelle previste dal precedente punto 4), ovverosia attraverso:

- richiesta al Gestore inviata via PEC;
- richiesta inviata tramite la casella di posta nota al Gestore in formato elettronico e sottoscritta con firma digitale o elettronica.

**Nel caso di richiesta di *sospensione***, trascorsi 30 (trenta) giorni dalla *sospensione*, il Gestore provvede al *ripristino* dell'identità precedentemente sospesa qualora non pervenga con le modalità sopra indicate una richiesta di revoca.

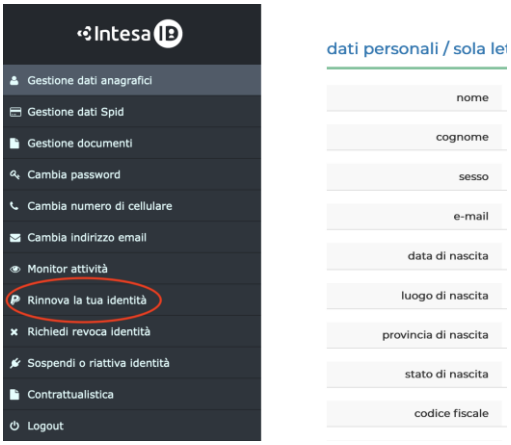
La revoca di un'Identità Digitale comporta conseguentemente la revoca delle relative credenziali.

**L'identità viene sospesa per documento scaduto**: il gestore, con un preavviso di almeno 30 giorni, avverte l'utente della scadenza del documento d'identità presente sul sistema, invitandolo a cambiarlo dall'area personale al link *https://spid.intesa.it/area-privata/* prima della scadenza dello stesso, pena la sospensione dell'identità; nel caso in cui lo stesso non viene aggiornato entro la sua scadenza, il Gestore provvede immediatamente alla sospensione della credenziale indicando all'utente la sospensione della stessa.

Il Gestore conserva la documentazione inerente al processo di adesione per un periodo pari a venti anni decorrenti dalla revoca dell'Identità Digitale.

# C. Rinnovo della credenziale

Il Gestore avverte il titolare della credenziale 90, 30, 10 ed il giorno stesso della scadenza della credenziale, dando all'utente la possibilità del rinnovo della stessa che può essere effettuata, entro i 90 giorni, facendo accesso all'area personale presente al link *https://spid.intesa.it/area-privata/* e, dopo aver effettuato la login, cliccando sul tab "Rinnova la tua utenza" presente nel menù a sinistra.




Nel caso si tratti di una persona fisica basterà unicamente inserire una nuova password.

In caso di minore, il rinnovo automatico è garantito fino al raggiungimento della maggiore età. Al neo maggiorenne verrà automaticamente sospesa l'identità digitale previa comunicazione via e-mail.

L'email verrà inviata con la cadenza prevista per i casi 1) e 6) descritti al par. *B.1*.

Questi potrà decidere entro 2 anni se riattivare l'identità con il profilo *adulto* ovvero se chiederne la definitiva revoca secondo le modalità previste.

In assenza di comunicazioni o attività da parte del Titolare l'identità sarà automaticamente revocata.

# D. Cautele per la conservazione e la protezione delle credenziali

Il Gestore mette in atto tutti i processi volti a garantire la protezione delle credenziali contro abusi e utilizzi non autorizzati ovvero ad assicurare la sicurezza della conservazione delle credenziali o dei mezzi usati per la loro produzione. Per via della diversa natura tecnologica che caratterizza le diverse credenziali, per ogni livello di sicurezza SPID vengono adottate diverse misure anticontraffazione.

Qualunque sia il livello SPID al quale si collochi una credenziale del Titolare, la primaria misura da mettere in atto per assicurare la sicurezza nell'utilizzo della credenziale è adoperare la massima cautela nella conservazione e nella protezione della stessa, come specificato negli obblighi del Titolare descritti nel *Manuale Operativo*.

## *D.1 Livello 1 SPID*

A questo livello è associata una credenziale composta da una *password*, la cui principale misura anticontraffazione è rappresentata dalla riservatezza di conservazione da parte del Titolare dell'Identità Digitale.

A tal proposito, il Titolare della credenziale deve:

a. Assicurarsi che i dispositivi (personal computer, tablet, smartphone, ecc.) utilizzati per accedere ai servizi SPID:
   - utilizzino esclusivamente software sicuri e dotati di licenza, per evitare infiltrazioni indesiderate all'interno del sistema che potrebbero compromettere la sicurezza generale;
   - abbiano adeguate protezioni di accesso al sistema e al disco fisso previste, per minimizzare il rischio di accessi non autorizzati;
   - si eviti di rendere evidenti utenze personali e password utili all'accesso ai dispositivi;
   - se esistono dati salvati su supporti esterni che potrebbero mettere a rischio la sicurezza dell'Identità Digitale SPID (tipicamente una password salvata all'interno di un file memorizzato su supporto esterno), siano adeguatamente protetti da un accesso con password al fine di ridurre il rischio di esposizione dei dati a rischio anche a fronte di un furto o di uno smarrimento;
   - vengano opportunamente protetti sia i dispositivi che eventuali supporti esterni contenenti dati a rischio;
   - i dispositivi non siano mai incautamente lasciati incustoditi.
b. Non trasmettere a nessun soggetto terzo, nemmeno se appartenente al Gestore, la *password* che costituisce la credenziale SPID, poiché rappresenta un'informazione strettamente personale e sensibile.
c. Riportare immediatamente ogni eventuale smarrimento o furto di dispositivi che contengono informazioni riservate, al fine di richiedere la sospensione o la revoca della credenziale.
d. Riportare immediatamente ogni eventuale sospetto di compromissione alla sicurezza dei dati relativi alle Identità Digitali, al fine di richiedere la sospensione, la revoca oppure la modifica della credenziale.

## D.2 Livello 2 SPID

Alla sicurezza data dalla segretezza della *password*, il secondo livello aggiunge quella data dal possesso di un telefono cellulare provvisto di SIM telefonica, sul quale viene inviata una seconda credenziale variabile e a durata limitata: il Gestore INTESA adotta un sistema di *OTP* (*One Time Password*) via sms ovvero via e-mail nel caso di minori, forniti in fase di sottoscrizione del servizio e verificato durante il riconoscimento del Titolare.

L'architettura dell'autenticazione OTP permette di generare codici di autenticazione dinamici di durata limitata a 60 (sessanta) secondi: ciò rende inutilizzabile la credenziale OTP trascorso tale periodo.

Anche in questo caso, la primaria forma di cautela che il Titolare deve assumere è costituita dalla premurosità nella custodia delle credenziali. Oltre alle specifiche comportamentali indicate per garantire la corretta conservazione della credenziale di *Livello 1 SPID*, per il secondo livello di sicurezza il Titolare deve mettere in atto ulteriori cautele, poiché a questo livello di sicurezza è associato un rischio maggiore in caso di perdita di possesso della credenziale.

Il Titolare deve, oltre a quanto indicato al paragrafo precedente per il *Livello 1*:

a. Assicurarsi con la massima cautela di mantenere sempre il controllo esclusivo dell'indirizzo di posta elettronica fornito in fase di registrazione.
b. Custodire con la dovuta cautela la *Password* associata all'identità Digitale.
c. Fornire, in fase di registrazione, un numero di telefono (SIM) proprio, di cui si ha accesso esclusivo: su questo sarà spedito, via SMS, l'*OTP - One Time Password*. In caso di minore l'OTP sarà inviato tramite e-mail personale indicata in fase di registrazione.

Si ricorda a tal proposito che qualunque operazione effettuata on-line utilizzando l'Identità Digitale è equiparata ad un'azione fisica, con le relative responsabilità civili e penali, nonché soggetta a possibili conseguenze negative per l'interessato (divulgazione di dati personali, richiesta di operazioni non desiderate, etc.).

## D.3 Livello 3 SPID

Non ancora gestito dall'Identity Provider.

*--- FINE DEL DOCUMENTO ---*