

Descrizione degli obblighi del Gestore dell'Identità Digitale SPID e del Titolare dell'Identità Digitale SPID

Sulla base della normativa vigente, nel presente paragrafo sono sinteticamente riassunti:

- gli **obblighi che il Gestore SPID** _____ assume in relazione alla propria attività;
- gli **obblighi che il Titolare dell'identità digitale SPID** assume in relazione alla richiesta e all'utilizzo dell'Identità Digitale rilasciata dal Gestore, con indicazione dei rispettivi riferimenti normativi.

Nella documentazione contrattuale del servizio che il Gestore sottoporrà all'Utente nell'ambito delle operazioni necessarie per il rilascio dell'Identità Digitale, sono indicati gli ulteriori elementi di natura contrattuale derivanti dal rapporto di erogazione del servizio. La documentazione contrattuale, unitamente alle sue successive versioni, sarà resa disponibile nel sito internet del Gestore.

Obblighi del Gestore

Descrizione
Rilasciare l'identità su domanda dell'interessato ed acquisire e conservare il relativo modulo di richiesta
Verificare l'identità del soggetto richiedente prima del rilascio dell'Identità Digitale
Conservare copia per immagine del documento di identità esibito e del modulo di adesione, nel caso di identificazione <i>de visu</i>
Conservare copia del log della transazione nei casi di identificazione tramite documenti digitali di identità, identificazione informatica tramite altra identità digitale SPID o altra identificazione informatica autorizzata
Conservare il modulo di adesione allo SPID sottoscritto con firma elettronica qualificata o con firma digitale, in caso di identificazione tramite firma digitale
Verifica degli attributi identificativi del richiedente
Consegnare in modalità sicura le credenziali di accesso all'utente
Conservare la documentazione inerente al processo di adesione per un periodo pari a venti anni decorrenti dalla scadenza o dalla revoca dell'identità digitale
Cancellare la documentazione inerente al processo di adesione trascorsi venti anni dalla scadenza o dalla revoca dell'identità digitale
Trattare e conservare i dati nel rispetto della normativa in materia di tutela dei dati personali di cui al decreto legislativo 30 giugno 2003, n. 196.
Verificare ed aggiornare tempestivamente le informazioni per le quali il Titolare ha comunicato una variazione
Effettuare tempestivamente e a titolo gratuito su richiesta dell'utente, la sospensione o revoca di un'identità digitale, ovvero la modifica degli attributi secondari e delle credenziali di accesso
Revocare l'identità digitale se ne riscontra l'inattività per un periodo superiore a 24 mesi o in caso di decesso della persona fisica o di estinzione della persona giuridica
Segnalare su richiesta dell'utente ogni avvenuto utilizzo delle sue credenziali di accesso, inviandone gli estremi ad uno degli attributi secondari indicati dall'utente
Verificare la provenienza della richiesta di sospensione da parte dell'utente (escluso se inviata tramite PEC o sottoscritta con firma digitale o firma elettronica qualificata)
Fornire all'utente che l'ha inviata conferma della ricezione della richiesta di sospensione
Sospendere tempestivamente l'identità digitale per un periodo massimo di trenta giorni ed informarne il richiedente.
Rispristinare o revocare l'identità digitale sospesa, nei casi previsti

Revocare l'identità digitale se riceve dall'utente copia della denuncia presentata all'autorità giudiziaria per gli stessi fatti su cui è basata la richiesta di sospensione
Utilizzare sistemi affidabili che garantiscono la sicurezza tecnica e crittografica dei procedimenti, in conformità a criteri di sicurezza riconosciuti in ambito europeo o internazionale
Adottare adeguate misure contro la contraffazione, idonee anche a garantire la riservatezza, l'integrità e la sicurezza nella generazione delle credenziali di accesso
Effettuare un monitoraggio continuo al fine rilevare usi impropri o tentativi di violazione delle credenziali di accesso dell'identità digitale di ciascun utente, procedendo alla sospensione dell'identità digitale in caso di attività sospetta
Effettuare con cadenza almeno annuale un'analisi dei rischi
Definire, aggiornare e trasmettere ad AGID il piano per la sicurezza dei servizi SPID
Allineare le procedure di sicurezza agli standard internazionali, la cui conformità è certificata da un terzo abilitato
Condurre con cadenza almeno semestrale il <i>Penetration Test</i>
Garantire la continuità operativa dei servizi afferenti allo SPID
Effettuare ininterrottamente l'attività di monitoraggio della sicurezza dei sistemi, garantendo la gestione degli incidenti da parte di un'apposita struttura interna
Garantire la gestione sicura delle componenti riservate delle identità digitali assicurando non siano rese disponibili a terzi, ivi compresi i fornitori di servizi stessi, neppure in forma cifrata
Garantire la disponibilità delle funzioni, l'applicazione dei modelli architetturali e il rispetto delle disposizioni previste dalla normativa
Sottoporsi con cadenza almeno biennale ad una verifica di conformità alle disposizioni vigenti
Informare tempestivamente l'AGID e il Garante per la protezione dei dati personali su eventuali violazioni di dati personali
Adeguare i propri sistemi a seguito dell'aggiornamento della normativa
Inviare all'AGID in forma aggregata i dati richiesti a fini statistici, che potranno essere resi pubblici.
In caso intendesse cessare la propria attività, comunicarlo all'AGID "e ai titolari" almeno 30 giorni prima della data di cessazione, indicando gli eventuali gestori sostitutivi, ovvero segnalando la necessità di revocare le identità digitali rilasciate
In caso di subentro ad un gestore cessato, gestire le identità digitali che questi ha rilasciato dal gestore cessato e ne conserva le informazioni
In caso di cessazione dell'attività, scaduti i 30 giorni, revocare le identità digitali rilasciate e per le quali non si è avuto subentro
Informare espressamente il richiedente in modo compiuto e chiaro degli obblighi che assume in merito alla protezione della segretezza delle credenziali, sulla procedura di autenticazione e sui necessari requisiti tecnici per accedervi
Se richiesto dall'utente, segnalargli via email o via sms, ogni avvenuto utilizzo delle sue credenziali di accesso.
Notificare all'utente la richiesta di aggiornamento e l'aggiornamento effettuato agli attributi relativi della sua identità digitale
Nel caso l'identità digitale risulti non attiva per un periodo superiore a 24 mesi o il contratto sia scaduto, revocarla e informarne l'utente via posta elettronica e numero di telefono mobile
In caso di decesso del titolare (persona fisica) o di estinzione della persona giuridica, revocare previo accertamento l'identità digitale
Nel caso in cui l'utente richieda la sospensione della propria identità digitale per sospetto uso fraudolento, fornirgli evidenza dell'avvenuta presa in carico della richiesta e procedere alla immediata sospensione dell'identità digitale.

Trascorsi trenta giorni dalla sospensione su richiesta dell'utente per sospetto uso fraudolento, ripristinare l'identità sospesa qualora non ricevesse copia della denuncia presentata all'autorità giudiziaria per gli stessi fatti sui quali è stata basata la richiesta di sospensione.
Nel caso in cui l'utente richieda la sospensione o la revoca della propria identità digitale tramite PEC o richiesta sottoscritta con firma digitale o elettronica inviata via posta elettronica, fornire evidenza all'utente dell'avvenuta presa in carico della richiesta e procedere alla immediata sospensione o alla revoca dell'identità digitale.
Ripristinare l'identità sospesa su richiesta dell'utente se non riceve entro 30 giorni dalla sospensione una richiesta di revoca da parte dell'utente.
In caso di richiesta di revoca di dell'identità digitale, revocare le relative credenziali e conservare la documentazione inerente al processo di adesione per 20 anni dalla revoca dell'identità digitale.
Proteggere le credenziali dell'identità digitale contro abusi ed usi non autorizzati adottando le misure richieste dalla normativa.
All'approssimarsi della scadenza dell'identità digitale, comunicarla all'utente e, dietro sua richiesta, provvedere tempestivamente alla creazione di una nuova credenziale sostitutiva e alla revoca di quella scaduta
In caso di guasto o di upgrade tecnologico provvedere tempestivamente alla creazione di una nuova credenziale sostitutiva e alla revoca di quella sostituita.
Non mantenere alcuna sessione di autenticazione con l'utente nel caso di utilizzo di credenziali di livelli 2 e 3 SPID
Tenere il Registro delle Transazioni contenente i tracciati delle richieste di autenticazione servite nei 24 mesi precedenti, curandone riservatezza, inalterabilità e integrità, adottando idonee misure di sicurezza (art. 31 D.LGS 196/2003) ed utilizzando meccanismi di cifratura.

Obblighi del Titolare dell'Identità Digitale

Descrizione
Esibire a richiesta del Gestore i documenti richiesti e necessari ai fini delle operazioni per la sua emissione e gestione
Si obbliga all'uso esclusivamente personale delle credenziali connesse all'Identità Digitale
Si obbliga a non utilizzare le credenziali in maniera tale da creare danni o turbative alla rete o a terzi utenti e a non violare leggi o regolamenti. A tale proposito, si precisa che l'utente è tenuto ad adottare tutte le misure tecniche e organizzative idonee ad evitare danni a terzi
Si obbliga a non violare diritti d'autore, marchi, brevetti o altri diritti derivanti dalla legge e dalla consuetudine
deve garantire l'utilizzo delle credenziali di accesso per gli scopi specifici per cui sono rilasciate con specifico riferimento agli scopi di identificazione informatica nel sistema SPID, assumendo ogni eventuale responsabilità per l'utilizzo per scopi diversi
L'uso esclusivo delle credenziali di accesso e degli eventuali dispositivi su cui sono custodite le chiavi private
Sporgere immediatamente denuncia alle Autorità competenti in caso di smarrimento o sottrazione delle credenziali attribuite
Fornire/comunicare al Gestore dati ed informazioni fedeli, veritieri e completi, assumendosi le responsabilità previste dalla legislazione vigente in caso di dichiarazioni infedeli o mendaci
Accertarsi della correttezza dei dati registrati dal Gestore al momento dell'adesione e segnalare tempestivamente eventuali inesattezze
Informare tempestivamente il Gestore di ogni variazione degli attributi previamente comunicati

<p>Mantenere aggiornati, in maniera proattiva o a seguito di segnalazione da parte del Gestore, i contenuti dei seguenti attributi identificativi:</p> <ul style="list-style-type: none"> • se persona fisica: estremi del documento di riconoscimento e relativa scadenza, numero di telefonia fissa o mobile, indirizzo di posta elettronica, domicilio fisico e digitale, • se persona giuridica: indirizzo sede legale, codice fiscale o P.IVA, rappresentante legale della società, numero di telefonia fissa o mobile, indirizzo di posta elettronica, domicilio fisico e digitale
<p>Conservare le credenziali e le informazioni per l'utilizzo dell'identità digitale in modo da minimizzare i rischi seguenti:</p> <ul style="list-style-type: none"> • divulgazione, rivelazione e manomissione • furto, duplicazione, intercettazione, cracking dell'eventuale token associato all'utilizzo dell'identità digitale • accertarsi dell'autenticità del fornitore di servizi o del gestore dell'identità digitale quando viene richiesto di utilizzare l'identità digitale
<p>Attenersi alle indicazioni fornite dal Gestore in merito all'uso del sistema di autenticazione, alla richiesta di sospensione o revoca delle credenziali, alle cautele che da adottare per la conservazione e protezione delle credenziali.</p>
<p>In caso di smarrimento, furto o altri danni/compromissioni (con formale denuncia presentata all'autorità giudiziaria) richiedere immediatamente al Gestore la sospensione delle credenziali.</p>
<p>In caso di utilizzo per scopi non autorizzati, abusivi o fraudolenti da parte di un terzo soggetto richiedere immediatamente al Gestore la sospensione delle credenziali.</p>

Responsabilità

Il Gestore è responsabile verso l'utente per l'adempimento di tutti gli obblighi derivanti dall'espletamento delle attività richieste dalla normativa vigente in materia di Sistema Pubblico di Identità Digitale. In particolare, nello svolgimento della sua attività:

<p>Attribuisce l'Identità Digitale e rilascia le credenziali connesse attenendosi alle Regole Tecniche emanate dall'AGID</p>
<p>Si attiene alle misure di sicurezza previste dal "Codice in materia di protezione dei dati personali" ai sensi del D.lgs n.196 del 30.06.2003 e s.m.i. nonché alle indicazioni fornite nell'informativa pubblicata sul sito https://.....</p>
<p>Procede alla sospensione o revoca delle credenziali in caso di richiesta avanzata dall'utente per perdita del possesso o compromissione della segretezza, per provvedimento dell'AGID o su propria iniziativa per acquisizione della conoscenza di cause limitative della capacità dell'utente, per sospetti di abusi o falsificazioni</p>