Guida Utente

Servizio SPID

31/08/2023

History

Protocollo	Modifiche	Revisione	Data	Autori	Approvazioni
SPIDGU	Prima Versione	1.0	15/07/2022	F. Barcellini	P. Sironi
SPIDGU	Revisione paragrafo 3	1.1	21/10/2022	F. Barcellini	P. Sironi
SPIDGU	Aggiornati contatti al paragrafo 5.2. 53	1.2	31/08/2023	F. Barcellini	P. Sironi

Sommario

1 Introduzione

Il presente Manuale è dedicato agli utenti e contiene una descrizione:

1. delle modalità d'uso del sistema di autenticazione di Intesi Group;
2. delle modalità con cui l'utente può richiedere la sospensione o la revoca delle credenziali con gli strumenti messi a disposizione da Intesi Group;
3. le cautele che l'utente deve adottare per la conservazione e protezione;

1.1 Dati identificativi del gestore

Il gestore del servizio SPID è Intesi Group che si identifica nel seguente modo:

Nome della società: Intesi Group S.p.A.

Sede Legale: Via Torino, 48 – 20123 Milano (MI) – ITALIA

Rappresentante Legale: Paolo Sironi (Amministratore Delegato e Presidente)

Partita IVA e Codice Tributario: IT02780480964

Telefono: +39 02 6760641

Identificatore di Oggetto ISO (OID): 1.3.6.1.4.1.48990

Sito web della società: http://www.intesigroup.com

Sito web della servizio SPID: https://spid.intesigroup.com/

Indirizzo e-mail della società: intesi@intesigroup.com

1.2 Definizioni

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	Nome, cognome, luogo e data di nascita, sesso, ovvero ragione o denominazione sociale, sede legale, il codice fiscale o la partita IVA e gli estremi del documento d' identità utilizzato ai fini dell'identificazione.

Attributi secondari	Il numero di telefonia fissa o mobile, l'indirizzo di posta elettronica, il domicilio fisico e digitale, eventuali altri attributi individuati dall'Agenzia, funzionali alle comunicazioni.
Attributi qualificati	Le qualifiche, le abilitazioni professionali e i poteri di rappresentanza e qualsiasi altro tipo di attributo attestato da un gestore di attributi qualificati.
Credenziale	il particolare attributo di cui l'utente si avvale, unitamente al codice identificativo, per accedere in modo sicuro, tramite autenticazione informatica, ai servizi qualificati erogati in rete dai fornitori di servizi che aderiscono allo SPID.
Fattore di autenticazione	Elemento di informazione e/o processo usato per autenticare o verificare l'identità di una entità.
Service Provider SPID	Il fornitore dei servizi della società dell'informazione definiti dall'art. 2, comma 1, lettera a), del decreto legislativo 9 aprile 2003, n. 70, o dei servizi di un'amministrazione o di un ente pubblico erogati agli utenti attraverso sistemi informativi accessibili in rete. I fornitori di servizi inoltrano le richieste di identificazione informatica dell'utente ai gestori dell'identità digitale e ne ricevono l'esito. I fornitori di servizi, nell'accettare l'identità digitale, non discriminano gli utenti in base al gestore dell'identità digitale che l'ha fornita.
Identity Provider SPID	L'ente giuridico accreditato allo SPID che, in qualità di gestore di servizio pubblico, previa identificazione certa dell'utente, assegna, rende disponibili e gestisce gli attributi dell'utente al fine della sua identificazione informatica. Il Gestore fornisce i servizi necessari a gestire l'attribuzione dell'identità digitale agli utenti, la distribuzione e l'interoperabilità delle credenziali di accesso, la riservatezza delle informazioni gestite e l'autenticazione informatica degli utenti. Nel presente documento il termine è utilizzato per identificare Intesi Group nell'esecuzione delle attività di Gestore dell'identità digitale.
Gestori di attributi qualificati	I soggetti accreditati ai sensi dell'art. 16 che hanno il potere di attestare il possesso e la validità di attributi qualificati, su richiesta dei fornitori di servizi.
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.
(Utente) Titolare o Richiedente	E' 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). Prima dell'attribuzione dell'identità digitale tale soggetto è chiamato Richiedente.

2 Identificazione

Intesi Group prima di rilasciare l'identità digitale SPID, deve identificare in maniera certa le persone fisiche in conformità all'art. 7 del DPCM.

La verifica dell'identità del soggetto richiedente può avvenire in una delle seguenti modalità:

a) identificazione in presenza del soggetto richiedente;

b) identificazione da remoto tramite strumenti di registrazione audio/video;

c) identificazione informatica tramite acquisizione del modulo di adesione allo SPID sottoscritto con firma elettronica qualificata.

Si precisa che, al fine di poter documentare la corretta attribuzione della stessa, Intesi Group, conserva per il periodo venti anni decorrenti dalla scadenza o dalla revoca dell'identità digitale, in relazione alle modalità di identificazione sopra elencate, copia per immagine del documento di identità esibito, tessera sanitaria,) o il modulo firmato digitalmente di cui alla lettera c), nonché' i documenti e i dati utilizzati per l'associazione e la verifica degli attributi.

Per la verifica dell'identità il richiedente deve presentare documenti di riconoscimento tra uno dei seguenti:

- carta d'identità
- passaporto
- patente

Oltre al documento d'identità il titolare deve sempre presentare la tessera sanitaria italiana che deve essere in corso di validità.

Fermo restando quanto sopra, per le identità digitali per persone giuridiche l'Identity Provider dovrà altresì verificare che il richiedente abbia il titolo per richiedere tale identità per mezzo di apposito documento comprovante tali poteri.

2.1 Identificazione in presenza

Questa modalità di identificazione viene condotta da un operatore (RAO) qualificato e opportunamente formato e richiede la presenza fisica del richiedente, il quale deve farsi riconoscere presentando documenti di identità in corso di validità).

L'operatore, per una corretta e sicura attuazione del processo:

a) fornisce l'informativa sul trattamento dei dati (artt. 13 e 14 Regolamento (UE) 2016/679);

b) si assicura che il richiedente sia consapevole dei termini e delle condizioni associati all'utilizzo del servizio di identità digitale;

c) si assicura che il richiedente sia consapevole delle raccomandazioni e delle precauzioni da adottare per l'uso delle identità digitale e propone l'attivazione del servizio di segnalazione di ogni avvenuto utilizzo delle credenziali di accesso;

d) acquisisce i dati necessari alla dimostrazione di identità.

Il RAO deve verificare la documentazione presentata e nel caso in cui la ritenga sufficiente e valida, procedere con:

- La registrazione dei dati anagrafici del richiedente attraverso il portale RAO di Intesi Group.
- La digitalizzazione di una copia dei documenti di identificazione presentati.
- L'approvazione dell'identificazione attraverso l'apposizione di una firma digitale qualificata sui dati personali dell'utente.

L'approvazione dell'identificazione si conclude con l'invio all'utente di una email di attivazione contenente le istruzioni per attivare l'identità SPID.

2.2 Identificazione e registrazione IDentify-Web

Questa modalità di identificazione viene condotta da un operatore RAO attraverso una videointervista con il richiedente. Il sistema di video conferenza utilizzato è messo a disposizione da Intesi Group che si occupa di fornire al richiedente le istruzioni necessarie per potervi accedere. Il richiedente, da parte sua, deve essere munito di un dispositivo (PC, Smartphone o Tablet) dotato di una webcam e di un sistema audio funzionante.

Il processo di identificazione avviene attraverso questi passi:

1. L'utente riceve una email con le istruzioni ed un link di avvio del processo di riconoscimento. L'email può essere inviata da un operatore abilitato o a seguito di un acquisto dallo store di Intesi Group (https://store.intesigroup.com/).
2. L'utente viene reindirizzato su una pagina Web di Intesi Group in cui deve inserire i propri dati personali, le immagini dei documenti di riconoscimento e fissare un appuntamento per il video riconoscimento.
3. Un operatore RAO verifica i dati e le immagini inserite dal cliente e può decidere se confermare i dati e la data del video riconoscimento oppure chiedere una correzione o rigettare la richiesta di riconoscimento.
4. Alla data concordata il richiedente ed il RAO si collegano in video call tramite la piattaforma IDentify Web.
5. All'avvio della video conferenza l'operatore acquisisce il consenso dell'utente trattamento dei dati personali e all'erogazione del servizio SPID. L'utente viene preventivamente informato circa le modalità di erogazione del servizio e dei propri diritti in quanto lo stesso riceve tutta la documentazione prima dell' avvio della sessione audio-video con operatore. In mancanza del consenso la video conferenza ed il processo di riconoscimento sono interrotti dal RAO.
6. La sessione audio- video si svolge nel seguente modo:
   a) l'acquisizione del consenso alla videoregistrazione e alla sua conservazione per 20 anni informando l'utente che la videoregistrazione sarà conservata in modalità protetta;
   b) l'operatore dichiara i propri dati identificativi;
   c) l'utente conferma le proprie generalità;
   d) l'utente conferma la data e l'ora della registrazione;
   e) l'utente conferma di volersi dotare di un'identità digitale e conferma i dati inseriti nella modulistica online in fase di pre-registrazione;
   f) l'utente conferma il proprio numero di telefonia mobile e l'indirizzo mail;
   g) l'operatore invia un sms che il richiedente è tenuto a mostrare o ripetere al RAO durante la videointervista, e una mail all'indirizzo di posta elettronica dichiarato, con un link ad una URL appositamente predisposta per la verifica;
   h) l'operatore chiede e ottiene conferma dall'utente circa la conoscenza delle tipologie di credenziali di cui disporrà per l'accesso ai servizi in rete;

i) l'operatore chiede di inquadrare, fronte e retro, il documento di riconoscimento utilizzato dal richiedente, assicurandosi che sia possibile visualizzare chiaramente la fotografia e leggere tutte le informazioni contenute nello stesso (dati anagrafici, numero del documento, data di rilascio e di scadenza, amministrazione rilasciante);
j) l'operatore chiede di mostrare la tessera sanitaria su cui è riportato il codice fiscale del soggetto;
k) l'utente conferma di aver preso visione e di accettare le condizioni contrattuali e d'uso disponibili sul sito web del gestore di identità;
l) l'operatore chiede al soggetto di compiere una o più azioni casuali volte a rafforzare l'autenticità della richiesta;
m) l'operatore riassume sinteticamente la volontà espressa dal soggetto di dotarsi di identità digitale e raccoglie conferma dallo stesso.

L'identificazione da remoto deve avvenire in una modalità tale da consentire la raccolta di elementi probanti, utili in caso di un eventuale disconoscimento dell'identità da parte dell'utente nel rispetto delle seguenti condizioni:

a) le immagini video devono essere a colori e consentire una chiara visualizzazione dell'interlocutore in termini di luminosità, nitidezza, contrasto, fluidità delle immagini;
b) l'audio deve essere chiaramente udibile, privo di evidenti distorsioni o disturbi;
c) la sessione audio/video, che ha ad oggetto le immagini video e l'audio del soggetto richiedente l'identità e dell'operatore, deve essere effettuata in ambienti privi di particolari elementi di disturbo.
d) La sessione audio/video deve essere completata senza nessuna interruzione.

Nel corso della video intervista il RAO può:

- bloccare e rifiutare l'identificazione se ritiene che un documento presentato non rispetti le caratteristiche di validità e autenticità,
- interrompere il processo di identificazione nel caso in cui la qualità audio/video sia di scarsa qualità o ritenuta non adeguata a a consentire la verifica dell'identità del richiedente.

L'approvazione dell'identificazione si conclude con l'invio all'utente di una email di attivazione contenente le istruzioni per attivare l'identità SPID.

2.3 Identificazione con Firma elettronica qualificata

L'identificazione di un utente può avvenire attraverso la verifica di una firma digitale qualificata emessa da un prestatore di servizi fiduciari qualificati apposta sul modulo di richiesta SPID.

Il processo di identificazione avviene attraverso questi passi:

1. L'utente riceve una email con le istruzioni ed un link di avvio del processo di riconoscimento. L'email può essere inviata da un operatore abilitato o a seguito di un acquisto dallo store di Intesi Group (https://store.intesigroup.com/).
2. L'utente viene reindirizzato su una pagina Web di Intesi Group in cui deve inserire i propri dati personali con cui viene generato il modulo da firmare.
3. L'utente deve scaricare il modulo, firmarlo con il proprio certificato di firma qualificata e caricarlo nuovamente sulla pagina web e inviarlo.
4. Alla ricezione del documento viene verificato che
5. Il file sia il medesimo generato dal sistema,
6. Il file non sia stato modificato dall'utente,
7. Il file sia stato firmato con una firma digitale qualificata valida.

Se queste tre condizioni si verificano il riconoscimento viene ritenuto valido e l'identificazione viene automaticamente approvata. Al contrario l'identificazione viene rigettata.

L'approvazione dell'identificazione si conclude con l'invio all'utente di una email di attivazione contenente le istruzioni per attivare l'identità SPID.

2.4 Certificato identificazione

L'approvazione dell'identificazione include l'emissione di un certificato qualificato di firma remota di Intesi Group che l'utente potrà utilizzare per eventuali attivazioni di altri servizi fiduciari di Intesi Group. Tale certificato ha le seguenti caratteristiche:

1. Durata: 1 anno
2. OID: 1.3.6.1.4.1.48990.1.1.1.7

3. userNotice (limitazione d'uso): "Il Presente certificato e' utilizzabile sololo per la sottoscrizione di contratti e/o moduli relativi ai servizi di Intesi Group".

Per evitare usi impropri, questo certificato verrà opportunamente mascherato negli strumenti di firma normalmente dati in uso ai clienti Intesi Group (IGSign, IGDesk e IGSmart) è sarà reso visibile solo nei casi di richiesta di attivazione di un nuovo servizio di Intesi Group.

3 Attivazione e conservazione credenziali di accesso SPID

Terminate le necessarie attività nonché verifiche propedeutiche all'attivazione di SPID, l'Identity Provider rilascia all'utente (o titolare dell'identità digitale) delle credenziali di Accesso.

Le credenziali di Accesso consentono al Titolare di eseguire il processo di autenticazione informatica volto alla verifica dell'identità digitale associata ai fini dell'erogazione di un servizio fornito in rete.

In altre parole, le credenziali di Accesso sono funzionali a comprovare l'associazione tra il Titolare e la sua identità digitale che lo rappresenta in rete, pertanto, si raccomanda di non comunicare a terzi o divulgare in alcun modo, curandone la relativa conservazione e protezione con la massima diligenza, per tutto il tempo di validità dell'Identità Digitale

Per lo SPID sono stati definiti tre livelli di sicurezza, corrispondenti ad altrettanti livelli specificati nella ISO-IEC 29115.

- **livello 1** (corrispondente al LoA2 dell'ISO-IEC 29115): Il livello 1 garantisce buon grado di affidabilità l'identità accertata nel corso dell'attività di autenticazione. Per questo livello è previsto un sistema di autenticazione ad un solo fattore es. password;
- **livello 2** (corrispondente al LoA3 dell'ISO-IEC 29115): Il livello 2 garantisce un alto grado di affidabilità l'identità accertata nel corso dell'attività di autenticazione Per questo livello è previsto un sistema di autenticazione informatica a due fattori;

  Intesi Group realizza il secondo fattore tramite l'invio di SMS contenente il codice OTP.
- **livello 3** (corrispondente al LoA4 dell'ISO-IEC 29115): Il livello 3 garantisce con un altissimo grado di affidabilità l'identità accertata nel corso dell'attività di autenticazione. Per questo livello è previsto un sistema di autenticazione informatica a due fattori basato su certificati digitali e criteri di custodia delle chiavi private su dispositivi che soddisfano i requisiti dell'Allegato 3 della Direttiva 1999/93/CE.

Intesi Group non propone credenziali di livello 3.

3.1 Definizione e conservazione credenziali di accesso di livello L1

Il **Livello 1 SPID** è gestito tramite una coppia username e password. Per le identità digitali SPID di Intesi Group lo username corrisponde all'indirizzo e-mail richiesto come attributo secondario in fase di registrazione.

La policy di definizione delle password applicata è la seguente:

1. lunghezza minima di otto caratteri;
2. uso di caratteri maiuscoli e minuscoli;
3. inclusione di uno o più caratteri numerici;
4. non deve contenere più di due caratteri identici consecutivi;
5. inclusione di almeno un carattere speciali ad es #, $, %;

I suggerimenti per una conservazione sicura:

1. Cambiarla periodicamente;
2. Evitare di utilizzare password che contengano riferimenti a dati personali del titolare, per esempio, nome cognome, data di nascita.
3. Evitare password contenenti parole di senso compiuto.
4. Non trasmettere o condividere la password con soggetti terzi.
5. Custodire la password in maniera sicura per impedirne il furto e la duplicazione da parte di terzi. Ad esempio non salvarle su foglietti o su file di testo del proprio PC.

Si precisa, che in caso di danni, perdite, divulgazioni, modifiche o usi non autorizzati dell'Identità Digitale il Titolare è l'unico responsabile in quanto responsabile esclusivo della protezione della propria Identità Digitale.

3.2 Conservazione credenziali di accesso di livello L2

Il **Livello 2 SPID** viene realizzato tramite l'adozione di una OTP (one time password) inviata per mezzo di SMS al numero di telefono indicato come attributo secondario SPID in fase di registrazione. Per la conservazione di questa credenziale si raccomanda di:

- Inserire le funzioni di blocco per impedire a terzi di avere accesso al proprio dispositivo mobile;
- mantenere aggiornato il sistema operativo (e anche le applicazioni) del proprio dispositivo;
- disattivare l'opzione di connessione Wi-Fi automatica e fare particolare attenzione al Wi-Fi pubblico ed aperto;
- utilizzare solo i market ufficiali per il download delle app. L'installazione di programmi di provenienza non fidata è il principale mezzo con cui vengono veicolati software potenzialmente pericolosi;
- disabilitare la funzione di "anteprima sms" sul proprio smartphone al fine di evitare la visualizzazione degli sms OTP da parte di terzi;
- utilizzare la funzione di "blocco-schermo" .

3.3 credenziali di accesso di livello L3

Non implementata da Intesi Group.

4 Modalità d'uso del sistema

Dal momento in cui l'utente riceve conferma di attivazione della propria credenziale SPID può cominciare ad utilizzarla per autenticarsi ad un sito web, di pubblici amministrazioni o di siti privati, che forniscono la possibilità di autenticarsi utilizzando le credenziali SPID.

Questi soggetti, chiamati *Fornitori di Servizi*, o *Service Provider* (*SP*), devono presentare il bottone a selezione multipla "*Entra con SPID*" all'interno del proprio portale:

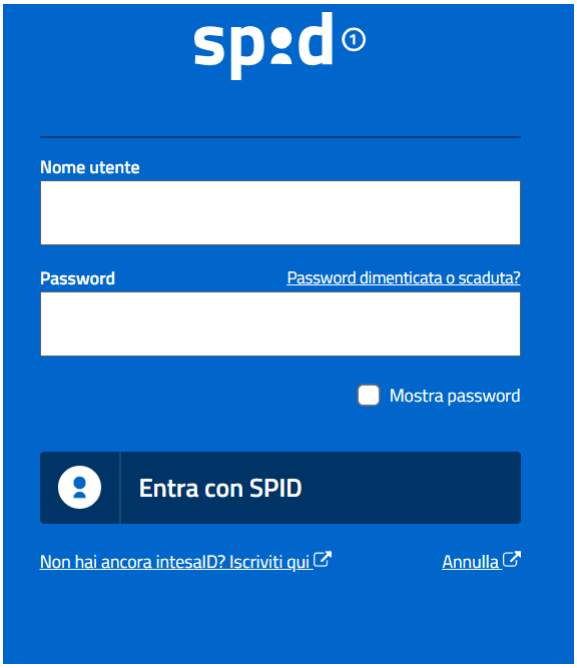
Cliccando sul bottone “Entra con SPID” verrà visualizzato l’elenco di tutti i Gestori di Identità digitale SPID dal quale l’utente dovrà selezionare quello che intende utilizzare.

Una volta effettuata la selezione, l'utente viene reindirizzato verso la schermata di login del proprio gestore d'identità che sarà impostata per richiedere una autenticazione con il livello di sicurezza SPID richiesto dal servizio del Fornitore dei Servizi.

Una volta in cui l'utente ha completato l'autenticazione verrà reindirizzato, insieme all'esito dell'autenticazione, al sito web del Fornitore dei Servizi presso il quale ha richiesto accesso. In caso di autenticazione positiva e si possiede un'Identità Digitale abilitata per il livello richiesto, l'utente verrà autenticato all'interno del portale del Fornitore dei Servizi e abilitati all'utilizzo dei servizi richiesti. In caso di autenticazione fallita verrà mostrato un messaggio di errore con la spiegazione del problema.

4.1 Livello 1 SPID

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



4.2 Livello 2 SPID

Nel caso sia richiesto un livello di sicurezza della credenziale SPID livello 2. sarà richiesto un ulteriore fattore di autenticazione. L'autenticazione procede in due passi. Al primo passo viene richiesto l'inserimento di username e password come per l'autenticazione di livello 1

Cliccando sul bottone "Entra con SPID" verrà presentata una finestra in cui verrà richiesto l'inserimento di un codice OTP che viene inviato all'utente attraverso SMS al numero di telefono indicato in fase di registrazione. Le modalità di invio sono descritte all'interno del Manuale Operativo e in adempimento all'Art. 6, comma 1, lettera b) del DPCM 24 ottobre 2014 (di seguito anche DPCM):

Inserito l'OTP l'utente deve cliccare sul bottone "Entra con SPID" e attendere di essere reindirizzato verso il Service Provider a cui si è richiesto l'accesso.

4.3 Livello 3 SPID

Non ancora gestito dall'Identity Provider.

4.4 Consenso Privacy

Nel caso in cui la richiesta di autenticazione preveda la trasmissione di dati dal Gestore dell'identità verso il Service Provider, viene presentata una richiesta con l'elenco dei dati che verranno inviati e la richiesta di autorizzazione a trasmetterli.

Per procedere con l'autenticazione l'utente deve cliccare sul bottone "Autorizza" e attendere di essere rediretto sul sito Web del Service Provider.

5 Gestione del ciclo di vita della credenziale

5.1 Sospensione dell'identità digitale

L'Utente Titolare, può chiedere la sospensione immediata dell'Identità Digitale qualora ritenga che la propria Identità Digitale sia stata utilizzata abusivamente o fraudolentemente.

Per procedere con la sospensione dell'identità digitale è necessario collegarsi all'area privata sul sito

https://spid.intesigroup.com

e selezionare la voce di menu "Identità SPID" sul menu di sinistra. Sulla destra comparirà un riepilogo della propria identità SPID con la possibilità di svolgere alcune azioni. Per procedere con la sospensione della propria identità SPID è necessario cliccare sul bottone "Sospendi identità".

Verrà chiesta conferma, nel caso in cui si decida di procedere l'identità SPID verrà immediatamente sospesa. L'identità SPID rimarrà sospesa per 30 giorni periodo entro il quale l'utente dovrà inviare documentazione

per procedere con la revoca. Se trascorso questo periodo Intesi Group non riceverà alcuna ulteriore comunicazione l'identità verrà automaticamente riattivata.

Per richiedere la revoca è necessario inviare il modulo di richiesta revoca secondo le modalità descritte nel seguente paragrafo 6.3:

5.2 Riattivazione dell'identità digitale

L'Utente Titolare, può chiedere la riattivazione della propria Identità Digitale collegandosi all'area privata sul sito

https://spid.intesigroup.com

e selezionare la voce di menu "Identità SPID" sul menu di sinistra. Sulla destra comparirà un riepilogo della propria identità SPID con la possibilità di svolgere alcune azioni. Per procedere con la riattivazione della propria identità SPID è necessario cliccare sul bottone "Riattiva identità".

In alternativa si può chiedere la riattivazione dell'identità SPID inviando richiesta di riattivazione all'indirizzo e-mail:

spid@intesigroup.com

inviando un copia scannerizzata del modulo di richiesta riattivazione compilata e firmata manualmente con allegata una copia del proprio documento d'identità e del codice fiscale/tessera sanitaria.

Se si dispone di un certificato di firma digitale qualificata, si può inviare copia del modulo di richiesta di riattivazione firmato digitalmente all'indirizzo PEC (Posta Elettronica Certificata):

spid@ig-trustmail.com

Intesi Group invia conferma dell'avvenuta riattivazione a:

1. Indirizzo email definito come attributo secondario dell'identità SPID
2. Indirizzo email mittente della richiesta di riattivazione.

5.3 Revoca dell'identità digitale

L'utente può richiedere la revoca di una identità SPID per:

1. recesso dal servizio per esigenze personali oppure a seguito della perdita della disponibilità del numero di cellulare o della e-mail di contatto o nome utente;
2. sospetto utilizzo abusivo o fraudolento da parte di un soggetto terzo;
3. furto o smarrimento credenziali;

Per chiedere la revoca dell'identità SPID è necessario scaricare il modulo di richiesta di revoca dal portale istituzionale di Intesi Group all'indirizzo:

https://www.intesigroup.com/it/documenti

oppure collegandosi all'area privata della propria identità SPID sul sito:

https://spid.intesigroup.com

e selezionando la voce di menu "Identità SPID" sul menu di sinistra. Sulla destra comparirà un riepilogo della propria identità SPID con la possibilità di svolgere alcune azioni. Per scaricare il modulo di revoca è necessario cliccare sul bottone "Revoca identità" da cui è possibile scaricare il modulo di richiesta revoca precompilato.

Per procedere con la revoca occorre inviare una e-mail all'indirizzo **spid@intesigroup.com** allegando:

1. copia scannerizzata del modulo di richiesta revoca compilato e firmato;
2. copia del documento d'identità del richiedente;
3. copia del codice fiscale/tessera sanitaria;
4. copia della denuncia sporta presso autorità nei casi copia di revoca per "Sospetto utilizzo abusivo / fraudolento da parte di un soggetto terzo" o di "furto/smarrimento credenziali".

Se il richiedente dispone di un certificato di firma digitale qualificata e di un indirizzo PEC (Posta Elettronica Certificata), può inviare copia del modulo di richiesta di revoca firmato digitalmente all'indirizzo PEC (Posta Elettronica Certificata):

spid@ig-trustmail.com

allegando:

1. copia digitale del modulo di richiesta revoca compilato e firmato;

2. copia della denuncia sporta presso autorità nei casi copia di revoca per “Sospetto utilizzo abusivo / fraudolento da parte di un soggetto terzo” o di “furto/smarrimento credenziali”.

Intesi Group invia conferma dell’avvenuta revoca a:

1. Indirizzo email definito come attributo secondario dell’identità SPID
2. Indirizzo email mittente della richiesta di revoca.

5.4 Rinnovo dell’identità digitale

Intesi Group 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, accedendo all'area personale all’url:

https://spid.intesigroup.com

e selezionare la voce di menu “Identità SPID” sul menu di sinistra. Sulla destra comparirà un riepilogo della propria identità SPID con la possibilità di svolgere alcune azioni. Per procedere con il rinnovo della propria identità SPID è necessario cliccare sul bottone “Rinnova identità”.

Verrà richiesto di definire una nuova password e l’identità verrà rinnovata e riattivata.