Guida Utente al servizio TIM ID

in ambito SPID

GUIDA UTENTE

VERSIONI DEL DOCUMENTO		
Revisione	Descrizione delle modifiche	Emissione
00	Prima emissione	09/09/2015
01	Integrazione dei paragrafi 4.1.2 (e relativi sottoparagrafi) e 4.1.3 per introduzione delle modalità di Identificazione mediante Firma Elettronica Qualificata e mediante Carta CNS/CIE, per le Persone Giuridiche. Integrazione del paragrafo 6.3 per introduzione modalità di Sospensione Telefonica. Integrazione del paragrafo 8.1 per introduzione canale 'Help Desk Telefonico' tra le modalità di comunicazione tra Gestore e Utente.	02/03/2016
02	Aggiornamento dei paragrafi 4.1.2 e 4.1.3 e inserimento nuovo sottoparagrafo 4.1.2.4 per introduzione modalità di Identificazione mediante Sistemi di Registrazione Audio-Video.	03/10/2016
03	Integrato paragrafo 6.2 per introduzione motivazione di revoca da parte del Gestore per scadenza documentazione di identificazione.	26/05/2017
04	Integrato paragrafo 4.1.1 per introduzione nel processo di Registrazione della funzionalità di upload della versione digitalizzata della documentazione di identificazione, per la modalità 'de-visu'. Integrato paragrafo 4.1.2.1 per introduzione nella modalità di identificazione 'de-visu' della firma FEA tramite OTP della documentazione contrattuale del Richiedente. Integrato paragrafo 4.1.3 per introduzione del provisioning certificato di FEA associato a Richiedente identità digitale nel processo di verifica delle informazioni di identità in caso di identificazione 'de-visu'. Aggiunto nuovo paragrafo 6.6 per introduzione funzionalità di visualizzazione e download dei documenti personali e contrattuali del titolare.	27/07/2017
05	Aggiunta linea di attivazione de-visu presso i negozi TIM (par. 4.1.2.1)	04/06/2021
06	Verifica del documento, correzione imprecisioni ed errori.	11/09/2024
07	Dismissione metodi di richiesta CNS-TS	03/02/2026
08	Inserimento Continuità operativa	08/04/2026
09	SPID MINORI	11/05/2026

Indice degli argomenti

1 Scopo del Documento

Questo documento contiene una guida utente del servizio **TIM ID** del Gestore **Telecom Italia Trust Technologies S.r.l.** (di seguito anche "il Gestore") in cui sono particolarmente curate le modalità d'uso del sistema di autenticazione, le modalità con cui l'utente può richiedere la sospensione o la revoca delle credenziali, e le cautele che l'utente deve adottare per la conservazione e protezione delle credenziali.

2 Attori coinvolti

Gli attori coinvolti nel modello operativo includono i seguenti:

- ***Utente***: persona fisica, persona fisica minore e persona giuridica, titolare dell'Identità Digitale.
- ***Identity Provider*** (IDP, o *Gestore*): emette e/o gestisce credenziali, o hardware, software e dati associati che possono essere utilizzati per produrre le credenziali.
- ***Registration Authority*** (RA, o Autorità di Registrazione): stabilisce e/o verifica e garantisce l'identità di un utente ad un Identity Provider.
- ***Authentication Authority*** (Autorità di Autenticazione, o *Verificatore):* è un attore che verifica le informazioni di identità.
- ***Service Provider*** (Erogatore di un Servizio, ad esempio una pubblica amministrazione): è una *Trusted* Third Party, o un suo rappresentante, riconosciuta come attendibile da altri attori in relazione a determinate attività.

3 Introduzione al servizio TIM ID

Il ***Sistema Pubblico di Identità Digitale*** (SPID) è il sistema nazionale che si occupa della gestione delle Identità Digitali relative sia a persone fisiche che a persone giuridiche.

Tale sistema è stato ideato per consentire l'accesso sicuro degli utenti ai portali delle Pubbliche Amministrazioni e delle società di servizi, che forniscono online i propri servizi.

Lo SPID è basato su **tre livelli di sicurezza** di autenticazione informatica, adottati in funzione dei servizi erogati e della tipologia di informazioni rese disponibili:

- **Livello 1**, prevede sistemi di autenticazione a singolo fattore, ad es. una *password*.
- **Livello 2**, prevede un sistema di autenticazione informatica a due fattori non necessariamente basato su certificati digitali.
- **Livello 3**, prevede un sistema di autenticazione informatica a due fattori basato su certificati digitali e criteri di custodia delle chiavi private su dispositivi conformi ai requisiti dell'Allegato 3 della Direttiva 1999/93/CE.

TIM ID costituisce il servizio di Identity Provider SPID di Trust Technologies.

Il Gestore garantisce la continuità operativa dei servizi di sua competenza afferenti allo SPID, conformemente agli indicatori di qualità e livelli di servizio allegati alla convenzione per l'adesione a SPID.

4 Rilascio dell'Identità Digitale

Le principali fasi del *rilascio dell'identità digitale* sono le seguenti:

- **Registrazione utente**
  - Pre-registrazione, Identificazione e Verifica delle informazioni di identità
  - Creazione dell'Identità Digitale
- **Emissione e Consegna delle credenziali**

4.1 Registrazione Utente

La **Registrazione** è il processo in cui un soggetto chiede di utilizzare il servizio.

La fase di Registrazione si compone dei seguenti passi:

- *Pre-registrazione*
- *Identificazione*
- *Verifica delle informazioni di identità*.

A seconda della modalità di identificazione prescelta in fase di pre-registrazione, l'attività di verifica delle informazioni di identità potrà essere effettuata a monte o valle rispetto all'identificazione.

Nel caso di identificazione di persona, 'de visu' (descritta al paragrafo 4.1.2.1) o 'da remoto' mediante sistemi di registrazione Audio-Video (descritta al paragrafo 4.1.2.3), la verifica dei dati verrà effettuata a monte dell'identificazione, mentre nel caso di identificazione informatica (sia essa effettuata mediante dispositivi di firma qualificata o digitale, paragrafo 4.1.2.2) la verifica dell'identità verrà effettuata a valle dell'identificazione.

Di seguito vengono distinti, dove necessario, i casi in cui il soggetto sia una Persona Fisica, Persona fisica minore oppure una Persona Giuridica.

4.1.1 Pre-registrazione

Nella pre-registrazione l'Utente, accedendo al Portale di Gestione del servizio di Identità Digitale, effettua una richiesta di adesione compilando online un **modulo di richiesta di adesione** al servizio.

Il Portale del servizio propone al Richiedente la scelta della modalità di Identificazione desiderata tra quelle disponibili. Questo modulo deve registrare informazioni sufficienti per garantire che il soggetto possa essere univocamente identificato dal Gestore.

Tali informazioni variano a seconda che il soggetto sia una persona fisica, o una persona giuridica e sono sintetizzate nella seguente tabella.

	Persona Fisica-Minore (Tipo 1 SPID)	Persona Giuridica (Tipo 2 SPID)
Attributi Identificativi	Nome e Cognome	Denominazione/Ragione Sociale
	Codice Fiscale	Codice Fiscale o Partita IVA
	Data e Luogo di Nascita	Sede Legale
	Sesso	-
	UserID	UserID
Attributi Secondari	Estremi documento di identità (tipo, numero, emettitore, data emissione, data scadenza)	Estremi documento di identità (tipo, numero, emettitore, data emissione, data scadenza)*
	Numero della Tessera Sanitaria	Numero della Tessera Sanitaria*
	Numero di cellulare	Numero di cellulare*
	Email	Email*
	Indirizzo di Domicilio	Indirizzo di Domicilio*

* Attributi relativi al soggetto richiedente

Nelle modalità di identificazione *"di persona"* ('*de-visu*') e "*di persona da remoto*" ('*audio-video'*), durante la fase di registrazione, vengono caricate a sistema le copie per immagine fronte/retro del documento d'identità e della Tessera Sanitaria. Nel caso di persona giuridica, viene caricata anche la copia del documento di *Certificazione attestante lo stato di Amministratore o Rappresentante Legale* del richiedente l'identità digitale per conto della persona giuridica).

Il Portale effettua verifiche formali sui dati inseriti dal Richiedente e procede al salvataggio dei dati generando un *Codice di Registrazione* univoco associato alla richiesta. Questo codice viene inviato al Richiedente per e-mail e potrà essere utilizzato come riferimento successivo per recuperarla e modificarla nei casi dove sia previsto oppure per ottenere assistenza.

4.1.2 Identificazione

L'**Identificazione** *(Identity proofing)* è il processo di acquisizione delle informazioni sufficienti per identificare un soggetto e consiste nell'acquisizione e accertamento di informazioni sufficienti a identificare una persona fisica, persona fisica minore o giuridica per uno specifico livello di sicurezza di autenticazione informatica in ambito SPID.

Le modalità di identificazione predisposte dal Gestore TI.TT sono di seguito indicate:

- "*di persona*", mediante esibizione 'a vista' di un documento di identità ("*de-visu*"),
- "*informatica*", mediante utilizzo della propria firma elettronica qualificata per sottoscrivere la richiesta di adesione da remoto,
- "*di persona, da remoto*", mediante utilizzo di sistemi di Registrazione Audio-Video;

4.1.2.1 Mediante esibizione 'a vista' di un documento di identità ('de visu')

In questa modalità il Richiedente ha due possibilità alternative:

- Recarsi direttamente presso uno dei negozi TIM abilitati ed eseguire l'intera procedura sul posto con l'aiuto dell'operatore del negozio;
- Compilare online e in autonomia la richiesta di registrazione per poi recarsi, ove previsto anche su appuntamento, presso uno dei Punti di Registrazione (PdR) messi a disposizione del Gestore presso enti pubblici o privati, su base di accordi specifici.

4.1.2.1.1 De-Visu presso un negozio TIM

In questa modalità di identificazione il Richiedente si reca presso un negozio TIM per attivare la sua TIM id con l'aiuto di un operatore incaricato dal Gestore.

Il Richiedente viene identificato di persona tramite esibizione a vista di un valido documento d'identità e della propria Tessera Sanitaria (come evidenza del codice fiscale, vedere 4.1.3).

L'incaricato presso il negozio effettua una serie di operazioni rispetto alle dichiarazioni del Richiedente:

- verifica la disponibilità da parte sua del numero di telefono e della casella di posta;
- inserisce a sistema i dati dichiarati dal Richiedente;
- verifica la corrispondenza che i documenti esibiti corrispondano a quelli dichiarati e che siano validi;
- carica a sistema una fotografia fronte e retro del documento d'identità e della tessera sanitaria;
- richiama a video il Modulo di richiesta, le Condizioni di Utilizzo del servizio, l'Informativa Privacy e i Termini Commerciali che devono essere accettate e firmate elettronicamente dal Richiedente;
- infine, avvia la verifica del cellulare e il processo di firma elettronica FEA della modulistica tramite OTP.

Il Richiedente riceve l'OTP sul cellulare e lo comunica all'Incaricato per completare il processo.

Tutta la documentazione prodotta e firmata viene salvata in un'area accessibile dall'Utente (Self-Customer Care) per visualizzazione e download. La procedura è eseguita interamente online e nessun documento cartaceo rimane o viene conservato presso negozio utilizzato.

4.1.2.1.2 De-Visu presso un Punto di Registrazione

In questa modalità di identificazione il Richiedente si reca presso un Punto di Registrazione (PdR) del Gestore solo dopo aver ricevuto relativa comunicazione. Tale comunicazione giungerà successivamente ai controlli per la verifica delle informazioni di identità, a cura del Gestore come descritto al paragrafo 4.1.4.

Il Richiedente viene identificato di persona tramite esibizione a vista di un valido documento d'identità e della propria Tessera Sanitaria (come evidenza del codice fiscale, vedere 4.1.3).

L'incaricato presso il PdR effettua successivamente una serie di operazioni: verifica la corrispondenza tra la documentazione esibita e il Richiedente, richiama a video il Modulo di richiesta, le Condizioni Generali di Utilizzo e l'Informativa Privacy, che devono essere accettate e firmate elettronicamente dal Richiedente; infine avvia la verifica del cellulare e il processo di firma elettronica FEA della modulistica tramite OTP.

Il Richiedente riceve l'OTP sul cellulare e lo comunica all'Incaricato per completare il processo di FEA della modulistica.

La documentazione prodotta e firmata viene salvata in un'area accessibile dall'Utente (Self-Customer Care) per visualizzazione e download. La procedura è eseguita interamente online e nessun documento cartaceo rimane o viene conservato presso negozio utilizzato.

4.1.2.2 Mediante utilizzo della firma elettronica qualificata

In questa modalità di identificazione il Richiedente opera in autonomia collegandosi via web al servizio online predisposto dal Gestore e viene identificato mediante upload del *Modulo di Richiesta di Adesione* elettronico sottoscritto digitalmente con la propria firma elettronica qualificata (formato PAdES, la firma su file PDF), per mezzo di strumenti di firma propri.

Nel caso di persona giuridica il Richiedente effettua inoltre l'upload della visura camerale (firmata digitalmente da una CCIAA) o, in alternativa, della copia dell'atto notarile di procura legale (firmata digitalmente dal Richiedente) attestante i poteri di rappresentanza conferiti alla persona fisica (amministratore/rappresentante legale).

Inoltre, il sistema del Gestore invia un sms contenente un codice OTP per la verifica del numero di cellulare e, a verifica effettuata, invia una e-mail di conferma contenente i dati riepilogativi.

4.1.2.3 Mediante utilizzo di Sistemi di Registrazione Audio-Video

In questa modalità di identificazione il Richiedente si collega via web al servizio online predisposto dal Gestore e viene identificato di persona, da remoto, tramite accesso ad una sessione web a lui riservata del *Servizio di Identificazione tramite Registrazione Audio-Video* (SIAV), interagendo con un Operatore del Gestore (o Incaricato del Gestore). L'accesso avviene tramite un apposito link web contenuto in una email di invito spedita dal servizio al termine della fase di verifica delle informazioni eseguita da parte del back office di Trust.

Nel caso di persona fisica o persona fisica minore l'Operatore avvia la registrazione della sessione web Audio-Video interagendo con il Richiedente in base ad una specifica procedura dedicata all'identificazione delle persone fisiche, che prevede anche l'acquisizione da webcam delle foto del documento di identità e della Tessera Sanitaria (come evidenza del codice fiscale, vedere 4.1.3).

Nel caso di persone giuridiche, l'Operatore avvia prima la registrazione della sessione web Audio-Video interagendo con il Richiedente in base ad una specifica procedura dedicata all'identificazione delle persone giuridiche (in questo caso il Richiedente dichiara di presentarsi in qualità di Amministratore o Rappresentante Legale per conto di una Persona Giuridica - dichiarandone esplicitamente Ragione Sociale, Partita IVA e Sede Legale), poi prende atto di quanto dichiarato dal Richiedente e procede con l'identificazione quale persona fisica.

4.1.3 Verifica del Codice Fiscale

In sede di richiesta dell'identità digitale, per provare di disporre del codice fiscale, è necessario fornire il numero della propria Tessera Sanitaria della quale vengono anche archiviate le fotografie fronte e retro.

Nel caso il richiedente non disponga della tessera sanitaria italiana perchè cittadino italiano residente all'estero o cittadino straniero, purché in possesso di documento d'identità valido emesso da una autorità italiana (carta d'identità, passaporto o patente di guida), è possibile fornire il tesserino del codice fiscale con numero identificativo

univoco oppure copia del certificato prodotto dall'Agenzia delle Entrate contenente il codice fiscale, vidimato dall'Ufficio Consolare o dell'Attestazione Consolare scaricabile dal portale dei servizi consolari - Fast-It .

4.1.4 Verifica delle informazioni di identità

La *verifica delle informazioni di identità* viene effettuata confrontando i dati forniti con le informazioni precedentemente convalidate ed il legame con il soggetto richiedente.

- Nel caso '***de visu***', si procede alla verifica dell'identità ovvero delle informazioni presenti nella Scheda di Registrazione mediante:
  a. controlli automatici (applicativi) sulle banche dati oggetto delle convenzioni;
  b. eventuali controlli manuali su fonti autoritative[1] in sostituzione dei controlli automatici;
  c. per le Persone Giuridiche, verifica associazione <Amministratore o Rappresentante legale – Persona giuridica> e successiva identificazione 'de visu' (come persona fisica) dell'Amministratore o del legale rappresentante;
  d. per le Persone Giuridiche, verifica validità della documentazione di *Certificazione attestante lo stato di Amministratore o Rappresentante Legale* del Richiedente l'identità digitale per conto della persona giuridica;
  e. ulteriori altre verifiche che si rendessero necessarie.

  Tali verifiche vengono svolte dal Gestore o da personale Incaricato dal Gestore stesso.

  Nel caso del Punto di Registrazione, al termine delle verifiche il personale di Back Office convalida o meno la registrazione. Nel caso dei negozi TIM, le verifiche vengono eseguite direttamente dall'incaricato presso il negozio.
  Dopo le verifiche il sistema del Gestore avvia il provisioning di un Certificato di FEA, associato al Richiedente, emesso per sottoscrivere elettronicamente la documentazione contrattuale richiesta dal Gestore stesso.
- Nel caso della ***'firma elettronica qualificata o digitale'***, presso il Gestore si procede alla verifica dell'identità e delle informazioni presenti nel Modulo di Adesione firmato digitalmente inviato dal Richiedente, mediante:
  a. controlli automatici (applicativi) sulle banche dati oggetto delle convenzioni;
  b. controlli manuali su fonti autoritative[1], in sostituzione dei controlli automatici;
  c. verifica firma digitale apposta dal Richiedente, in conformità al DPCM 22 febbraio 2013 (viene verificata la corrispondenza tra il Codice Fiscale indicato nel Modulo di Adesione e quello contenuto nel Certificato qualificato);
  d. verifica corrispondenza e validità dei documenti identificativi indicati dal Richiedente;
  e. per le Persone Giuridiche, verifica associazione <Amministratore o Rappresentante legale – Persona giuridica> e successiva identificazione mediante firma elettronica qualificata o digitale (come persona fisica) dell'Amministratore o legale rappresentante;
  f. per le Persone Giuridiche, verifica validità della documentazione di *Certificazione attestante lo stato di Amministratore o Rappresentante Legale* del Richiedente l'identità digitale per conto della persona giuridica;
  g. ulteriori altre verifiche che si rendessero necessarie.

  Al termine della verifica viene convalidata o meno la registrazione.
- Nel caso di ***registrazione Audio-Video***, l'Operatore (o Incaricato del Gestore) procede alla verifica delle informazioni acquisite durante la sessione web di identificazione audio-video, mediante:
  a. controlli automatici (applicativi) sulle banche dati oggetto delle convenzioni;
  b. eventuali controlli manuali su fonti autoritative[2] in sostituzione dei controlli automatici;
  c. corrispondenza e validità dei documenti identificativi indicati dal Richiedente;

[11] La verifica dell'identità differisce dalla dimostrazione dell'identità in quanto implica la convalida delle informazioni di identità attraverso sorgenti addizionali - fonti autoritative, in particolare utilizzando prioritariamente i servizi di cui all'articolo 4, comma 1, lettera c) del DPCM SPID (v. convenzioni dell'Agenzia) e, nei casi in cui le informazioni necessarie non siano accessibili per mezzo dei servizi convenzionati, tramite verifiche sulla base di documenti, dati o informazioni ottenibili da archivi delle amministrazioni certificanti, ai sensi dell'art. 43, comma 2, del D.P.R. 28 dicembre 2000, n. 445.

[2] La verifica dell'identità differisce dalla dimostrazione dell'identità in quanto implica la convalida delle informazioni di identità attraverso sorgenti addizionali - fonti autoritative, in particolare utilizzando prioritariamente i servizi di cui all'articolo 4, comma 1, lettera c) del DPCM SPID (v. convenzioni dell'Agenzia) e, nei casi in cui le informazioni necessarie non siano accessibili per mezzo dei servizi convenzionati, tramite verifiche sulla base di documenti, dati o informazioni ottenibili da archivi delle amministrazioni certificanti, ai sensi dell'art. 43, comma 2, del D.P.R. 28 dicembre 2000, n. 445.

d. per le Persone Giuridiche, verifica corrispondenza e validità dei dati dichiarati dal Richiedente in qualità di Amministratore o Rappresentante Legale per conto della Persona Giuridica;
e. per le persone fisiche minori verifica della corrispondenza dei dati del genitore/tutore legale richiedente
f. verifica integrità/qualità della registrazione audio-video;
g. ulteriori altre verifiche che si rendessero necessarie.

Al termine della verifica viene convalidata o meno la registrazione.

4.1.5 Creazione dell'Identità Digitale

La fase di Registrazione termina, per tutte le modalità sopraelencate, con l'inserimento dei dati relativi all'identità, verificati e certificati all'interno della piattaforma di gestione.

In questa fase l'identità digitale risulterà in uno stato non attivo. Lo sarà non appena sarà concluso il processo di *consegna delle credenziali e delle informazioni per l'utilizzo del servizio* a cura del Gestore.

La fase successiva provvederà a fornire le credenziali al Titolare e quindi a rendere attiva l'Identità Digitale acquisita.

4.2 Emissione e Consegna delle credenziali

Le fasi di **emissione e consegna delle credenziali** comprendono la generazione delle credenziali ed il loro invio.

Le credenziali emesse variano inoltre in base al tipo di livello di sicurezza prescelto:

- ***Livello 1***: verrà fornita una *UserID* e una ***Password***.
- ***Livello 2***: verrà fornita una *UserID* e una ***Password***, come già previsto a Livello 1, abbinato ad un codice ***OTP*** [*One-Time Password]* ricevuto via SMS al numero di cellulare dichiarato dal titolare e verificato dal Gestore in fase di Registrazione[3].
- ***Livello 3***: (non disponibile)[4]

4.2.1 Emissione

Il processo di ***emissione*** delle credenziali consiste nel fornire o in altri termini nell'associare una identità digitale con una credenziale: alla convalida della procedura di Registrazione, il sistema del Gestore crea e personalizza le credenziali assegnate al Richiedente.

Livello 1

Il sistema, una volta inoltrata la richiesta di emissione dell'Identità Digitale, provvederà a generare una ***Password*** (valida sia per il Livello 1 che per il Livello 2).

Per la generazione della *Password* viene applicata la password policy così definita:

- **Limiti sulla lunghezza**: almeno 8 caratteri
- **Limiti su caratteri usabili**: almeno 1 minuscola, 1 maiuscola, 1 cifra numerica, 1 carattere speciale.
- **Limite di durata**: max 180 giorni (scadenza).
- **Limite caratteri identici**: max 2 consecutivi.
- **Limite riusabilità**: non uguale alle ultime 5, non uguale a quelle degli ultimi 15 mesi.
- **Limite contenuto**: configurato per puntare ad un file dizionario contenente le stringhe che non possono essere utilizzate per la composizione della password (*Userid*).

Livello 2

[3] Il sistema del Gestore invia un sms contenente un codice OTP per la verifica del numero di cellulare e, a verifica effettuata, invia una e-mail di conferma contenente i dati riepilogativi.

[4] Attualmente non commercializzato da TITT.

Oltre alla ***Password*** di Livello 1 il sistema genera ed invia un codice ***OTP*** (*One-Time Password*) che potrà essere usato una sola volta durante la sessione di autenticazione.

La generazione del **codice OTP** segue la policy così definita:

- **Lunghezza**: 6
- **Caratteri usati**: numerico
- **Limite di validità temporale**: 15 minuti
- **Limite utilizzo**: 1 sola volta

4.2.2 Consegna

Il processo di ***consegna*** rappresenta l'ultima fase relativamente al processo di rilascio di una identità digitale: la complessità varia con il livello di sicurezza della credenziale.

La piattaforma di gestione del servizio invia all'utente:

Livello 1

- ***UserID*** via e-mail, utilizzando l'indirizzo e-mail dichiarato e verificato in fase di Registrazione,
- ***Password*** (valida solo per il primo accesso, da cambiare obbligatoriamente) via SMS, utilizzando il numero di telefono cellulare dichiarato e verificato in fase di Registrazione.

Livello 2

- ***OTP*** (valida una sola volta durante la sessione di servizio) via SMS, utilizzando il numero di telefono cellulare dichiarato e verificato in fase di Registrazione.

5 Modalità d'uso del sistema di autenticazione

Il Gestore mette a disposizione dell'utente un set di funzionalità per l'autenticazione dell'identità digitale.

- **Modalità disponibili all'utente per l'autenticazione**
  - Autenticazione di Livello 1 SPID
  - Autenticazione di Livello 2 SPID
- **Registro delle attività**
  - Visualizzazione attività

Le funzionalità di accesso web per l'autenticazione dell'identità digitale sono fruibili mediante i software browser più diffusi sia su PC che su smartphone che devono essere sempre aggiornati alle ultime versioni disponibili.

5.1 Modalità disponibili per l'autenticazione

5.1.1 Autenticazione di Livello 1 SPID

Per il Livello di sicurezza 1 SPID il Gestore offre l'autenticazione ad un fattore tramite:

[***Password***]

L'Utente effettua l'autenticazione informatica a Livello 1 SPID mediante:

- inserimento di UserID & [**Password**] nella maschera di autenticazione

Il servizio prevede un **time-out** per inattività della **richiesta di autenticazione** pari a **5 minuti**, dopodiché è necessario procedere ad una nuova richiesta.

Il servizio prevede un **time-out per inattività** della **sessione autenticata** pari a **60 minuti**, dopodiché è necessario procedere ad una nuova autenticazione; se però durante la sessione autenticata viene effettuata un'altra autenticazione, la durata della sessione viene incrementata di ulteriori 60 minuti, con **limite massimo** pari a **120 minuti** (dopodiché è necessario procedere ad una nuova autenticazione).

Il servizio prevede il **blocco temporaneo di 30 minuti** della credenziale (che risulterà sospesa) dopo l'inserimento per 5 (cinque) volte consecutive di userID e/o password errate.

5.1.2 Autenticazione di Livello 2 SPID

Per il Livello di sicurezza 2 SPID il Gestore offre l'autenticazione a due fattori tramite

[***Password***] + [***OTP via SMS***]

L'Utente effettua l'autenticazione informatica a Livello 2 mediante combinazione multi-token, in dettaglio:

- inserimento di UserID & [**Password**] nella prima maschera di autenticazione (Livello 1), e
- inserimento del codice **OTP** ricevuto via SMS nella seconda maschera di autenticazione (Livello 2).

Il servizio prevede un **time-out** per inattività della **richiesta di autenticazione** pari a **5 minuti**, dopodiché è necessario procedere ad una nuova richiesta.

Il servizio prevede un limite di **validità temporale** per il codice **OTP** pari a **15 minuti**.

Il servizio prevede il **blocco temporaneo di 30 minuti** della credenziale (che risulterà sospesa) dopo l'inserimento per **5** (cinque) **volte consecutive** di **userID e/o password errate**.

Il servizio prevede il **blocco temporaneo di 30 minuti** della credenziale (che risulterà sospesa) dopo l'inserimento per **3** (tre) **volte consecutive** di codice **OTP errato**.

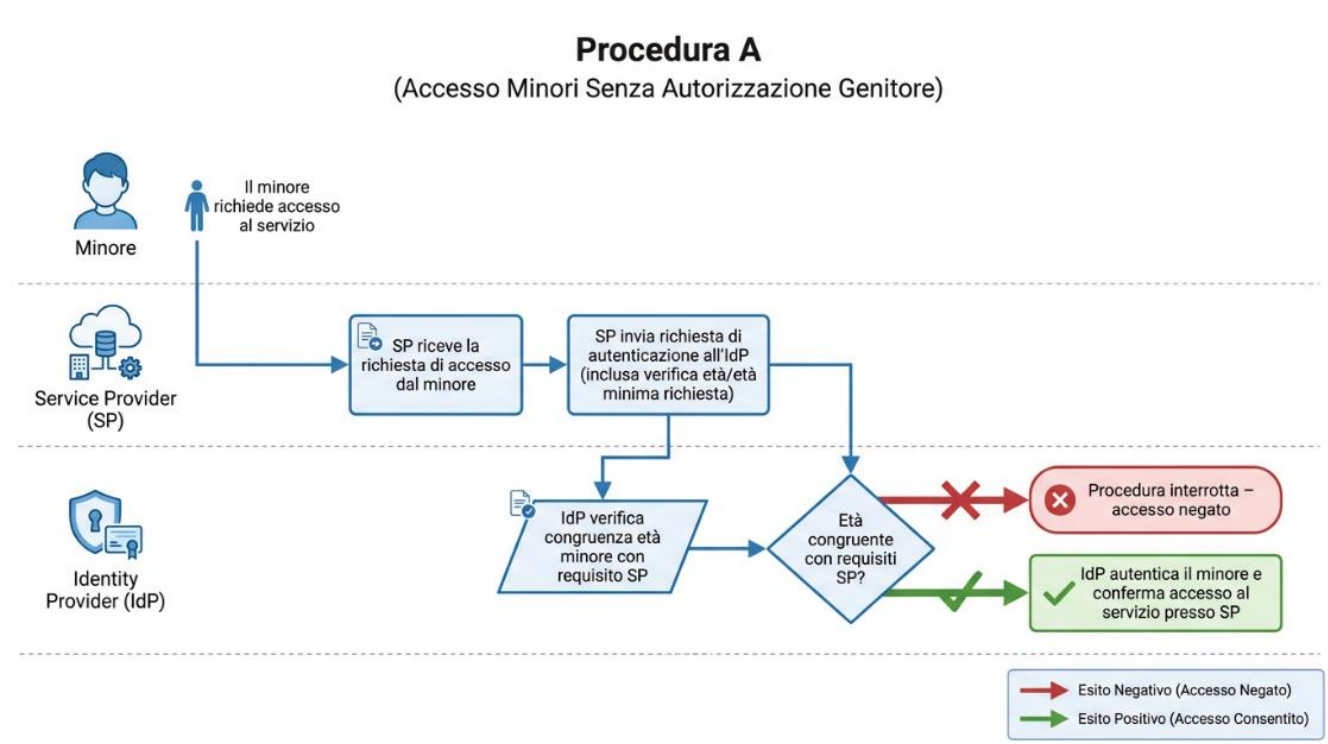
5.1.3 Autenticazione SPID Minore

Per l'utenza di tipo SPID Minore oltre i livelli di sicurezza si applicano due procedure di autenticazione di seguito descritte

Procedura A

Questa procedura si applica nei casi in cui il Service Provider(SP), dopo aver valutato la tipologia e la finalità del servizio fornito, NON È TENUTO a richiedere l'autorizzazione del Genitore per l'accesso al servizio da parte del minore:

1. Il minore richiede di accedere al servizio del SP.
2. Il SP invia una richiesta di autenticazione all'Identity Provider (IdP).
3. L'IdP esegue la procedura di autenticazione del minore, che include la verifica della corrispondenza tra l'età richiesta dal SP e l'età reale del minore. Se la verifica ha esito negativo, la procedura di autenticazione viene interrotta con esito negativo; se invece ha esito positivo, l'IdP completa il processo di autenticazione del minore presso il SP.



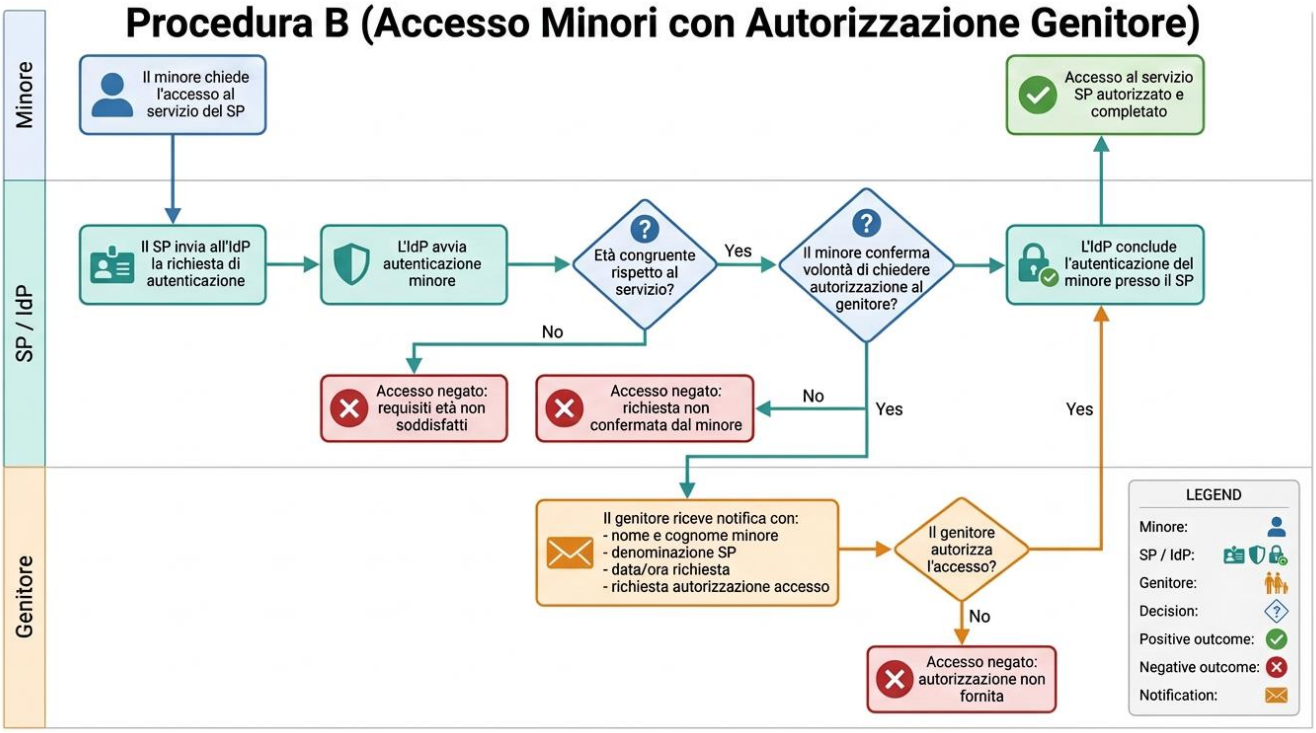
Procedura B

Questa procedura si applica quando il Service Provider (SP), a seguito di una valutazione relativa alla tipologia e all'obiettivo del servizio fornito, è OBBLIGATO a richiedere l'autorizzazione del Genitore per l'accesso del minore al servizio.

La presente Procedura B si applica esclusivamente ai minori di età superiore ai quattordici anni per l'accesso a servizi che non rientrano tra quelli di prevenzione o consulenza forniti direttamente al minore:

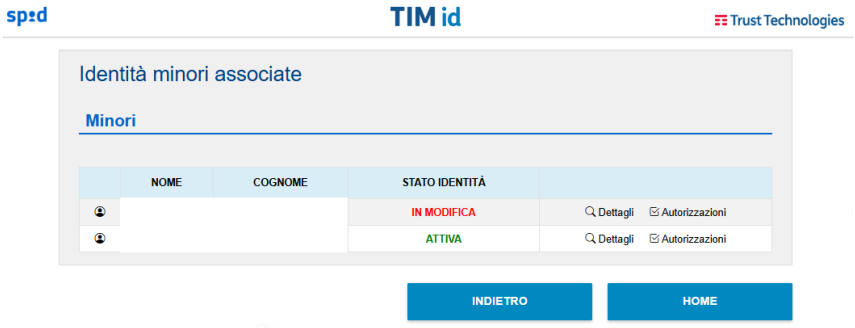
1. Il minore richiede di accedere al servizio del SP.
2. Il SP invia una richiesta di autenticazione all'Identity Provider (IdP).
3. L'IdP esegue la procedura di autenticazione per il minore, che include le seguenti operazioni:

    - L'IdP verifica la corrispondenza tra l'età richiesta dal SP e l'età reale del minore: se la verifica ha esito negativo, la procedura di autenticazione si interrompe; se ha esito positivo, l'IdP prosegue con l'autenticazione.
    - L'IdP invia al minore una richiesta di conferma della sua intenzione di chiedere al Genitore l'autorizzazione all'accesso: se il minore non conferma, la procedura è interrotta; se conferma, si procede con i passaggi successivi.
    - L'IdP notifica il Genitore con le seguenti informazioni:
        - a. Nome e cognome del minore;
        - b. Denominazione del SP al quale il minore ha richiesto di accedere;
        - c. Data e ora della richiesta di accesso;
        - d. Richiesta di autorizzazione per l'accesso del minore.
    - Se il Genitore non autorizza l'accesso, la procedura di autenticazione si interrompe; se fornisce l'autorizzazione, l'IdP completa il processo di autenticazione del minore presso il SP.

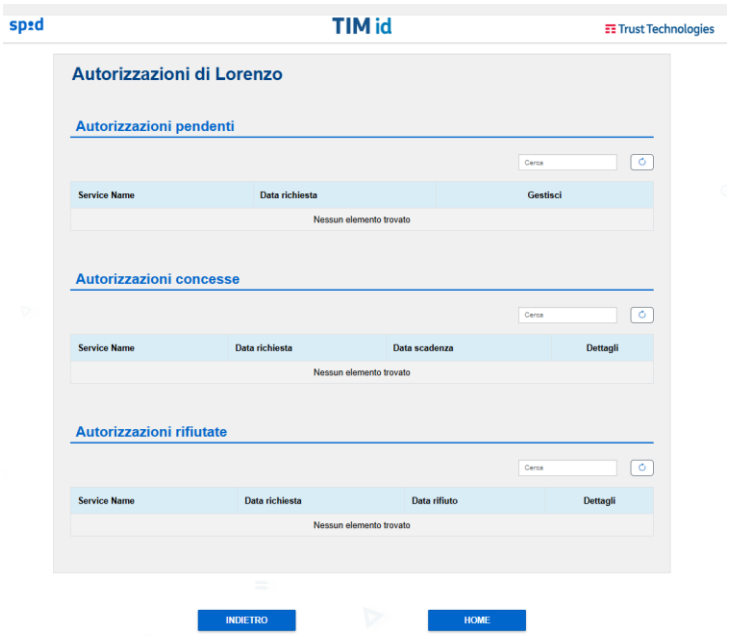


5.1.3.1 Gestione delle autorizzazioni di accesso minore

Il Genitore del minore che riceve una notifica di richiesta di accesso di una identità minore a lui associata, accede tramite la propria area Self Customer Care del portale id.tim.it al pannello Identità minori associare



Il genitore seleziona la ID del minore che deve verificare e viene visualizzato un pannello con il riepilogo delle autorizzazioni associate alla sua ID con il relativo stato.

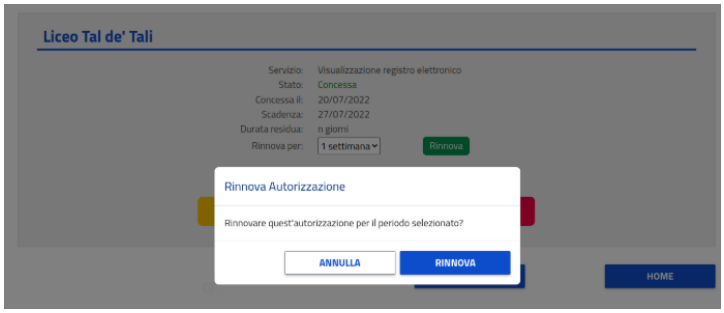


Se il genitore seleziona una autorizzazione attiva e viene visualizzato il pannello con i dettagli.

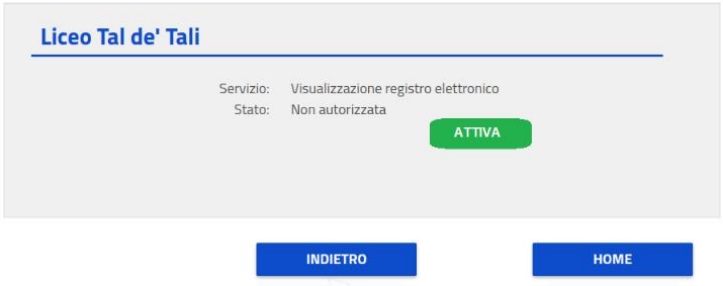
Il genitore può chiedere: il Rinnovo oltre l'attuale scadenza, la Sospensione oppure la Revoca definitiva dell'autorizzazione, premendo sul bottone corrispondente.

Nel caso di Rinnovo, il genitore seleziona prima il numero di giorni per i quali vuole estendere la validità dell'autorizzazione.

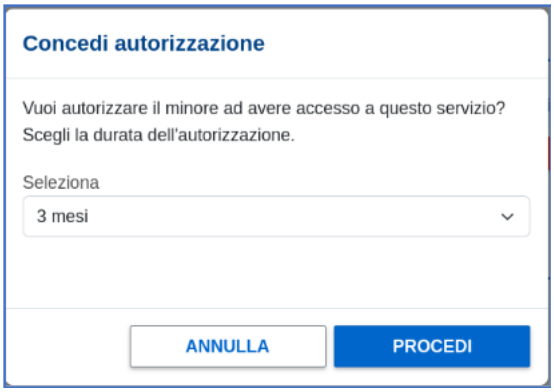
In ogni caso viene mostrato un popup che chiede di confermare l'operazione. Nel caso del Rinnovo:



Se il genitore seleziona una autorizzazione non ancora attiva, il bottone AUTORIZZA gli da la possibilità di approvarla o bocciarla.



Viene mostrato un popup che chiede di confermare l'operazione e consente di sceglierne la durata in giorni.



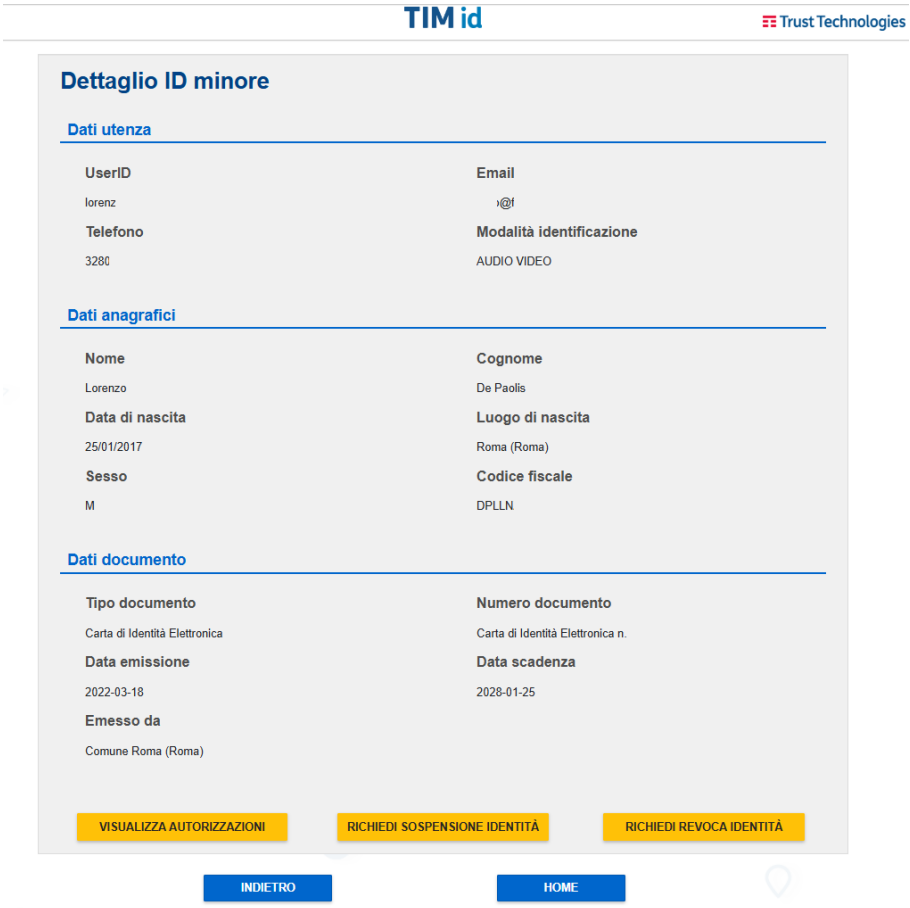
6 Gestione del ciclo di vita dell'Identità Digitale

Il Gestore mette a disposizione dell'Utente un set di funzionalità per la gestione del *ciclo di vita* dell'identità digitale.

- **Funzionalità disponibili all'Utente per la gestione dell'Identità Digitale**
  - Modifica (attributi, credenziali)
  - Revoca
  - Sospensione
  - Riattivazione
  - Rinnovo e/o Sostituzione
- **Registro delle attività**
  - Visualizzazione attività

6.1.1 Gestione ciclo di vita SPID Minore

Il Genitore accedendo nella propria area Self Customer Care, andando sul dettaglio delle identità minori a lui associate,

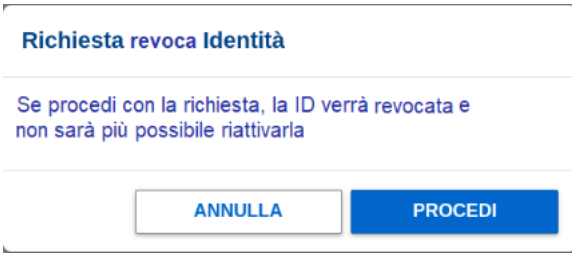


Il genitore può visualizzare i dati relativi al minore e richiedere la sospensione o la revoca della sua ID.

Se il genitore seleziona il bottone RICHIEDI SOSPENSIONE IDENTITA' viene visualizzato il popup di conferma

e solo selezionando il bottone PROCEDI la richiesta sarà inviata al Servizio.

Se il genitore seleziona il bottone RICHIEDI REVOCA IDENTITA' viene visualizzato il popup di conferma



6.2 Modifica dell'identità digitale (attributi e credenziali)

6.2.1 Modifica attributi dell'identità

L'Utente ha la possibilità, accedendo all'interfaccia web del servizio, di visualizzare direttamente i propri dati personali (gli attributi registrati) e di modificare quelli non identificativi (vedere 4.1.1).

E' possibile modificare i seguenti attributi, alle condizioni indicate:

Indirizzo di Domicilio	È sufficiente indicare le nuove informazioni, queste verranno automaticamente aggiornate dal servizio.
Numero di cellulare	x
Indirizzo email	x
Estremi del documento di identità	Indicare le nuove informazioni, queste verranno verificate dagli operatori del Gestore e se approvate, aggiornate dal servizio.

Per visualizzare e per modificare i dati personali è richiesta l'autenticazione a livello 2 SPID.

6.2.2 Recupero e modifica delle credenziali

L'Utente può recuperare o modificare le proprie credenziali in funzione del loro livello, attenendosi alle indicazioni seguenti:

- **Userid SPID:** per **recuperare la Userid SPID** relativa alla propria Identità Digitale (purché non bloccata, sospesa o revocata), l'utente può utilizzare la funzione di recupero accessibile direttamente dalla maschera di login proposta dal Gestore al momento dell'autenticazione, in cui dovrà inserire il numero di telefono cellulare e l'e-mail forniti e verificati al momento della registrazione. In caso di verifica positiva dei dati inseriti, la corrispondente Userid verrà inviata per e-mail all'indirizzo di posta elettronica specificato.
- **Credenziali Livello 1 / Livello 2:** per **modificare** in autonomia **la Password SPID** relativa alla propria Identità Digitale (purché non bloccata, sospesa o revocata), se l'utente conosce quella attualmente valida, può utilizzare il servizio online del Gestore. Se invece, l'ha **dimenticata**, può utilizzare la funzione di recupero accessibile direttamente dalla maschera di login proposta dal Gestore al momento dell'autenticazione per ricevere un nuovo codice di attivazione password, da utilizzare per scegliere la nuova password per la sua Identità Digitale. Per completare l'operazione, dovrà inserire la propria UserID e l'e-mail fornita al momento della registrazione. In caso di verifica positiva dei dati inseriti, il codice di attivazione password verrà inviato all'utente tramite SMS al numero di telefono fornito e verificato in sede di registrazione.

6.2.3 Rinnovo / ri-emissione delle credenziali

Al termine della vita utile delle credenziali (scadenza temporale), in caso di applicazione di regole di sicurezza (ad esempio, obbligo di cambio della password ogni tre/sei mesi), il rinnovo e la ri-emissione sono obbligatorie al primo successivo utilizzo dell'identità digitale per autenticarsi a un servizio online o al portale di self-caring.

6.3 Revoca

Questa sezione descrive la revoca dell'Identità Digitale, specificando le circostanze in cui può e deve essere revocata e le modalità in cui deve essere richiesta dall'Utente.

I motivi per cui può essere richiesta una revoca sono di seguito elencati:

- **Richiesta da parte dell'Utente** L'Utente ha la possibilità di richiedere la revoca dell'identità digitale. La richiesta dovrà essere inoltrata al Gestore:
    1. via PEC alla casella di Posta Elettronica Certificata indicata dal Gestore;

2. all'indirizzo di Posta elettronica indicato dal Gestore, se la richiesta è in formato elettronico. In questo caso la richiesta stessa dovrà essere sottoscritta con firma elettronica qualificata o firma digitale;
3. tramite Posta ordinaria (si suggerisce Raccomandata a/r), all'indirizzo indicato dal Gestore, contenente la richiesta cartacea sottoscritta con firma autografa, copia del documento di identità in corso di validità e copia della denuncia di suo furto o smarrimento.

Il Gestore procede tempestivamente con la sospensione cautelativa delle credenziali relative all'identità, dandone opportuna notifica. Successivamente, verifica la legittimità della richiesta ricontattando il richiedente attraverso uno o più attributi secondari dell'Utente. Solo dopo questa ulteriore verifica il Gestore revoca l'identità e comunica all'Utente (o alle amministrazioni di appartenenza dell'Utente) il completamento e l'esito finale dell'operazione.

- **Sospetti abusi e/o falsificazioni**. L'Utente, nel caso in cui ritenga che la propria identità digitale sia stata utilizzata abusivamente o fraudolentemente da un terzo, può disconoscere la propria identità digitale inviando una dichiarazione di disconoscimento:
  1. via PEC alla casella di Posta Elettronica Certificata indicata dal Gestore;
  2. all'indirizzo di Posta elettronica indicato dal Gestore, se la richiesta è in formato elettronico. In questo caso la richiesta stessa dovrà essere sottoscritta con firma elettronica qualificata o firma digitale;
  3. tramite Posta ordinaria (si suggerisce Raccomandata a/r), all'indirizzo indicato dal Gestore, contenente la richiesta cartacea sottoscritta con firma autografa, copia del documento di identità in corso di validità e copia della denuncia di suo furto o smarrimento.

  Il Gestore provvede a sospendere cautelativamente l'identità digitale disconosciuta e ne dà tempestiva comunicazione. Successivamente, verifica la legittimità della richiesta ricontattando il richiedente attraverso uno o più attributi secondari dell'Utente. Se nel periodo di trenta giorni dalla sospensione il gestore riceve dal richiedente il disconoscimento copia della denuncia penale presentata all'Autorità Giudiziaria per gli stessi fatti su cui è basata la dichiarazione di disconoscimento, procede con la revoca dell'identità digitale altrimenti essa viene ripristinata.
- **Decesso persona fisica, persona fisica minore o Estinzione persona giuridica**. La procedura applicata in questo caso prevede che il Gestore proceda con la revoca dell'identità dietro comunicazione ufficiale da parte dei rappresentanti dell'Utente (eredi o procuratore, amministrazione, società subentrante) oppure di una delle autorità competenti. In tal caso il Gestore verifica la veridicità del decesso/estinzione tramite i servizi delle banche dati online che utilizza anche in fase di attivazione del servizio e procede di conseguenza. Invece, in caso di mancata comunicazione si ricade automaticamente nella revoca per inattività.
- **Al compimento del 18esimo anno di età** il titolare dell'identità digitale viene informato via e-mail che da quel momento è rimosso qualunque controllo parentale sulla sua ID e che, se non ha interesse a mantenere attivo il servizio abilitato a SPID, ha la facoltà di recedere dallo stesso tramite la procedura di richiesta di revoca.

Il Gestore può procedere autonomamente alla revoca dell'Identità Digitale nei seguenti casi:

- **Inattività**. In caso di inattività che si protragga per almeno ventiquattro mesi di seguito, l'identità digitale viene automaticamente revocata ma fatta precedere da comunicazioni a 90, 30 e 10 giorni relative alla possibile revoca da effettuarsi, nonché il giorno precedente alla revoca stessa inviate all'indirizzo di posta elettronica o al recapito di telefonia mobile, contenenti la data e la causa della revoca.
- **Scadenza contrattuale**. In caso di scadenza contrattuale, l'identità digitale viene automaticamente revocata ma fatta precedere da comunicazioni a 90, 30 e 10 giorni relative alla possibile revoca da effettuarsi, nonché il giorno precedente alla revoca stessa inviate all'indirizzo di posta elettronica o al recapito di telefonia mobile, contenenti la data e la causa della revoca.
- **Scadenza documentazione di identificazione**. Con l'approssimarsi della scadenza della documentazione di identificazione, il Gestore preavvisa il Titolare della revoca dell'identità digitale alla scadenza inviando comunicazioni a intervalli di 90, 30 e 10 giorni dalla scadenza ed infine il giorno precedente alla revoca. Una volta effettuata la revoca, il Gestore ne dà comunicazione al Titolare precisando la data e la causa della revoca, utilizzando l'indirizzo di posta elettronica o il recapito di telefonia mobile.

Oltre alle circostanze sopra riportate, sono motivo di revoca del certificato:

- la modifica o la scadenza del rapporto che intercorre tra l'Utente e l'Amministrazione per conto della quale l'identità digitale viene utilizzata;
- il decadere del titolo, della carica o del ruolo inerente ai poteri di rappresentanza o la qualifica professionale in nome di cui l'identità digitale viene utilizzata;
- il ritiro della procura o della delega da parte del rappresentato.

Inoltre, la **revoca** può avvenire **su iniziativa del Gestore** quando si verifichino una o più delle circostanze seguenti:

- riscontro che l'identità digitale non è stata rilasciata secondo le modalità previste dalla normativa vigente;
- riscontro che uno dei prerequisiti per l'accettazione della registrazione dell'Utente è venuto meno;
- riscontro che l'Utente ha infranto uno degli obblighi assunti al momento della richiesta di registrazione, previsti dalla normativa e riportati nel presente Manuale Operativo;
- eventuale richiesta motivata e documentata dell'Autorità Giudiziaria.

Ai sensi della normativa, nel caso in cui non abbia la possibilità di accertare in tempo utile l'autenticità della richiesta di revoca, il Gestore invece che alla revoca procede alla **sospensione** dell'Identità Digitale.

I gestori dell'identità digitale conservano la documentazione inerente al processo di adesione per il periodo previsto dalla normativa.

La revoca di una Identità Digitale determina l'**immediata e definitiva cessazione della sua validità**, indipendentemente dalla data di scadenza della stessa originariamente fissata.

La revoca non inficia la validità dell'Identità Digitale nel lasso di tempo precedente il momento della revoca stessa.

La revoca viene effettuata mediante l'inserimento dell'Identità nello stato di **REVOCATA**. Da quel momento l'esito delle verifiche richieste dai Service Provider relative a tale Identità Digitale avrà risposta negativa e motivata.

Il Gestore garantisce la tempestiva esecuzione della revoca in questione.

La richiesta di revoca proveniente direttamente dall'Utente è accettata qualora redatta ed inoltrata **per iscritto** ed inoltre:

1. Contenga esplicita dichiarazione della volontà di revocare l'Identità Digitale;
2. Contenga la motivazione della richiesta di revoca e la decorrenza richiesta per tale revoca;
3. Contenga almeno i seguenti dati anagrafici del richiedente:
    - nome e cognome,
    - data e luogo di nascita,
    - indirizzo di residenza (costituito da via, numero civico, CAP, comune di residenza),
    - codice fiscale.
- fotocopia di un documento di riconoscimento del richiedente la sospensione (ove richiesta nei casi precedentemente descritti).

Sono comunque considerate tali quelle che adducono esplicitamente una delle motivazioni seguenti:

- possibile compromissione della segretezza delle credenziali;
- furto degli strumenti per l'uso del servizio;
- smarrimento degli strumenti per l'uso del servizio.

Il Gestore si impegna a compiere ogni ragionevole sforzo per rispettare i tempi di decorrenza della revoca riportati sulla relativa richiesta.

La revoca dell'identità digitale è sancita dal suo inserimento in uno stato di **REVOCATA**.

L'avvenuta revoca di una Identità Digitale viene notificata all'Utente tramite l'indirizzo di posta elettronica da lui dichiarato in fase di registrazione.

Analogamente viene notificato qualunque fatto noto al Gestore che possa compromettere la validità o affidabilità dell'identità stessa.

Secondo quanto previsto dalla normativa vigente, l'intenzione di revocare una identità digitale è notificata anticipatamente all'Utente, salvo casi di motivata urgenza, ogni qual volta la revoca avvenga per iniziativa del Gestore o dell'Autorità Giudiziaria.

In ciascun caso, la notifica contiene:

- i dati identificativi univoci dell'Utente e dell'identità digitale in questione,
- i motivi della revoca,
- dati identificativi del richiedente la revoca,
- la data e l'ora a partire dalla quale l'identità digitale non è più valida.

L'operazione di revoca di una identità digitale è registrata in un apposito archivio informatico del Gestore. La traccia dell'evento è conservata per un periodo pari a 20 (venti) anni, secondo quanto previsto dalla normativa (cfr. Art. 7, comma 8 del DPCM 24 ottobre 2014).

6.4 Sospensione

Questa sezione descrive la sospensione dell'identità digitale, specificando le circostanze in cui può essere sospesa e le modalità in cui deve essere richiesta dall'Utente.
La sospensione dell'identità digitale può essere effettuata dai soggetti seguenti:

- su **richiesta dell'Utente**,
- su **iniziativa del Gestore**.

La ***sospensione da parte dell'Utente*** può essere richiesta con le modalità seguenti:

- richiesta inviata in formato elettronico, sottoscritta con firma digitale o elettronica, alla casella di Posta elettronica del Gestore;
- richiesta inviata da una casella PEC all'indirizzo di Posta Elettronica Certificata indicato dal Gestore;
- richiesta inviata via posta ordinaria, all'indirizzo indicato dal Gestore, contenente la richiesta sottoscritta con firma autografa, copia del documento di identità in corso di validità e copia della denuncia di suo furto o smarrimento;

Per le ultime tre modalità di richiesta è prevista una verifica della provenienza della richiesta anche attraverso uno o più attributi secondari dell'Utente.

I **casi di emergenza** in cui l'Utente può richiedere la sospensione dell'identità digitale sono i seguenti:

- possibile compromissione della segretezza delle credenziali,
- furto degli strumenti per l'uso del servizio,
- smarrimento degli strumenti per l'uso del servizio,
- sospetti abusi e/o falsificazioni,
- altre cause che possono generare la perdita dei requisiti di riservatezza, integrità e disponibilità delle informazioni contenute nell'identità digitale (e relative credenziali).

Nella richiesta di sospensione per iscritto devono essere chiaramente indicati:

- esplicita dichiarazione della volontà di sospendere l'identità digitale;
- la motivazione della richiesta di sospensione ed il periodo di sospensione richiesto;
- i seguenti dati anagrafici dell'Utente (o dell'Incaricato se è lui a chiedere la sospensione):
    - nome e cognome;
    - data e luogo di nascita;

- indirizzo di residenza (costituito da via, numero civico, CAP, comune di residenza);
- codice fiscale;

- fotocopia di un documento di riconoscimento del richiedente la sospensione (ove richiesta nei casi precedentemente descritti).

La ***sospensione da parte del Gestore*** può essere effettuata qualora, dalle attività di monitoraggio, si ritenga che l'identità digitale sia stata utilizzata abusivamente o fraudolentemente.

In tal caso il Gestore provvederà a sospendere tempestivamente l'identità digitale ed inviare opportuna notifica dell'avvenuta sospensione al titolare dell'utenza. In tale comunicazione verranno inoltre fornite le indicazioni per poter procedere alla riattivazione dell'utenza da parte del titolare.

La sospensione di una identità digitale determina **l'immediata cessazione della sua validità, indipendentemente dalla data di scadenza, sino al momento della sua riattivazione**.

La sospensione non inficia la validità dell'identità digitale nel lasso di tempo precedente il momento della sospensione stessa. La sospensione viene effettuata mediante l'inserimento dell'Identità nello stato di SOSPESA. Da quel momento l'esito delle verifiche richieste dai Service Provider relative a tale Identità Digitale avrà risposta negativa e motivata.

Il Gestore garantisce la tempestiva esecuzione della sospensione in questione. Trascorsi trenta giorni dalla suddetta sospensione, il Gestore provvede al ripristino dell'identità precedentemente sospesa qualora non riceva richiesta formale di revoca.

L'avvenuta sospensione di una identità digitale viene notificata all'Utente tramite l'indirizzo di posta elettronica da lui dichiarato in fase di registrazione. La notifica contiene:

- i dati identificativi univoci dell'Utente e dell'identità digitale in questione,
- i motivi della sospensione,
- dati identificativi del richiedente la sospensione,
- la data e l'ora a partire dalla quale l'identità digitale non è più valida.

L'operazione di sospensione di una identità digitale è registrata in un apposito archivio informatico del Gestore. La traccia dell'evento è conservata per un periodo pari a 20 (venti) anni, secondo quanto previsto dalla normativa (cfr. Art. 7, comma 8 del DPCM 24 ottobre 2014).

6.5 Riattivazione

Questa sezione descrive il processo di riattivazione di una identità digitale precedentemente sospesa.

La riattivazione dell'identità digitale può essere richiesta dai soggetti seguenti:

- su **richiesta dell'Utente**
- su **iniziativa del Gestore**

Le richieste di **riattivazione da parte dell'Utente** dovranno essere inoltrate nelle seguenti modalità:

- richiesta inviata in formato elettronico, sottoscritta con firma digitale o elettronica, alla casella di Posta elettronica fornita dal Gestore,
- richiesta inviata da una casella PEC all'indirizzo di Posta Elettronica Certificata indicato dal Gestore,
- richiesta inviata ad un indirizzo di Posta elettronica indicata dal Gestore, contenente la richiesta sottoscritta con firma autografa e copia del documento di identità in corso di validità ovvero copia della denuncia di suo furto o smarrimento.

Per le ultime tre modalità di richiesta è prevista una verifica della provenienza della richiesta anche attraverso uno o più attributi secondari del titolare.

La richiesta di riattivazione dovrà contenere le seguenti informazioni:

- esplicita dichiarazione della volontà di riattivare l'identità digitale,
- la motivazione della riattivazione e la decorrenza richiesta,
- i seguenti dati anagrafici del richiedente:
    - nome e cognome; data e luogo di nascita,
    - indirizzo di residenza (costituito da via, numero civico, CAP, comune di residenza),
    - codice fiscale,
    - fotocopia di un documento di riconoscimento (in corso di validità).

Nel caso in cui l'Identità digitale sia stata sospesa su iniziativa del Gestore, causa sospetti usi illeciti o fraudolenti, il titolare dell'Identità Digitale potrà procedere in autonomia con la riattivazione delle credenziali tramite l'utilizzo di un link fornito nella comunicazione di notifica dell'avvenuta sospensione inviata dal Gestore.

La **riattivazione da parte del Gestore** verrà effettuata nel caso in cui siano trascorsi i termini di per convertire la richiesta di sospensione in una richiesta di revoca. Trascorsi 30 giorni dalla data di sospensione dell'Identità Digitale, e non avendo ricevuto richiesta di revoca della stessa, il Gestore è tenuto a riattivare l'Identità Digitale.

Il Gestore si impegna a compiere ogni ragionevole sforzo per rispettare i tempi di decorrenza della riattivazione riportati sulla richiesta di riattivazione.

La riattivazione di una identità digitale determina **l'immediata riassunzione della sua validità, sino al momento della sua scadenza**.

La riattivazione viene effettuata mediante l'inserimento dell'Identità nello stato di ATTIVA. Da quel momento l'esito delle verifiche richieste dai Service Provider relative a tale Identità Digitale avrà risposta positiva.

La riattivazione di una identità viene notificata all'Utente tramite l'indirizzo di posta elettronica da lui dichiarato in fase di registrazione.

La notifica contiene:

- i dati identificativi univoci dell'Utente e dell'identità in questione,
- i motivi della riattivazione,
- la data e l'ora a partire dalla quale l'identità digitale riassume la sua validità.

L'operazione di riattivazione di una identità digitale è registrata in un apposito archivio informatico del Gestore. La traccia dell'evento è conservata per un periodo pari a 20 (venti) anni, secondo quanto previsto dalla normativa (cfr. Art. 7, comma 8 del DPCM 24 ottobre 2014).

6.6 Portale di Self Customer Care

È disponibile un'area web di 'Self Customer Care' del titolare che consente di visualizzare le informazioni personali relative al servizio TIM id.

Tramite l'interfaccia web del servizio, per la quale è necessaria l'autenticazione al livello L2 SPID, è possibile effettuare le seguenti operazioni:

- Visualizzare le informazioni personali relative alla propria identità digitale (attributi)
- Modificare gli attributi non identificativi che dovessero cambiare dopo l'attivazione dell'identità digitale
- Visualizzare le informazioni relative alle autenticazioni effettuate con successo ai servizi online SPID
- Attivare e/o disattivare la notifica di avvenuta autenticazione SPID, inviata tramite email alla casella di posta elettronica associata all'identità digitale
- Visualizzare e/o scaricare la documentazione personale e contrattuale in formato elettronico sottoscritta digitalmente durante la fase di Registrazione (Richiesta di Identità digitale SPID, Condizioni Generali di Fornitura e Informativa sulla Privacy)

7 Informativa sui rischi, le contromisure ed il trattamento dei dati

L'identità digitale rilasciata da TI Trust Technologies S.r.l. nell'ambito del servizio TIM ID, è a tutti gli effetti una vera e propria identità personale, e come tale comporta la necessità di adottare le cautele necessarie per evitarne un uso fraudolento e indesiderato. TIM ID può essere utilizzata tramite:

- un dispositivo mobile personale, cellulare o smartphone con la SIM card, corrispondente all'utenza telefonica associata all'identità digitale;
- un dispositivo in grado di navigare su internet, dal quale accedere ai siti dei "Service Provider" SPID.

Si invitano dunque gli utilizzatori del servizio TIM ID a seguire le **precauzioni minime** di seguito elencate:

a) utilizzare esclusivamente le informazioni per l'utilizzo del servizio fornite dal TI Trust Technologies S.r.l.;
b) comunicare tempestivamente a TI Trust Technologies S.r.l. l'eventuale modifica dei dati forniti in fase di richiesta attivazione, utilizzando le modalità e gli strumenti indicati da TI Trust Technologies S.r.l.;
c) evitare comportamenti che possano compromettere l'integrità e la riservatezza delle credenziali dell'identità digitale TIM ID o dei dispositivi di navigazione utilizzati, curando in particolare di non lasciare incustoditi o non protetti il dispositivo mobile personale ed il dispositivo di navigazione soprattutto se sono in corso operazioni su un sito o un applicativo per cui è richiesta l'identificazione;
d) richiedere immediatamente la revoca o la sospensione cautelativa dell'identità digitale TIM ID qualora ne ricorrano il circostante, utilizzando le modalità indicate nella Guida utente o nel Manuale operativo del servizio.

I dati personali sono trattati, conservati e protetti dal Gestore conformemente a quanto previsto dal Regolamento 2016/679/UE (Regolamento generale sulla protezione dei dati) e dell'articolo 122 del Codice in materia di protezione dei dati personali (D.Lgs. 196/03, il c.d. Codice privacy) e secondo quanto riportato nell'Informativa pubblicata nel sito internet del Gestore, all'indirizzo https://www.trusttechnologies.it/download/legale-e-privacy/, in base alla quale l'utente del servizio presta il proprio consenso al trattamento dei propri dati personali, per le finalità dichiarate dal Gestore.

8 Riferimenti del Gestore

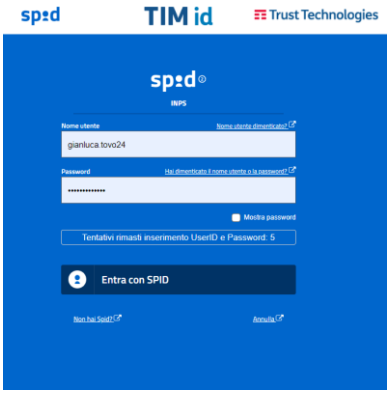
Riferimenti	
Sede Legale:	S.S. 148 Pontina km. 29,100 – 00071 Pomezia (Roma)
Indirizzo PEC:	TI.TT@ttpec.telecomitalia.it
Indirizzo di Posta elettronica:	info-ttstore@telecomitalia.it

8.1 Modalità di comunicazione tra Gestore e Utente

L'utente può interagire con l'Identity Provider attraverso i seguenti canali:

CANALI

Help Desk Telefonico 800.405.800	Il canale Help Desk Telefonico di TIM Digital Store viene utilizzato per fornire supporto relativamente alle seguenti richieste: • EMISSIONE dell'identità Digitale • SOSPENSIONE dell'identità Digitale • Stato avanzamento di richieste dell'identità Digitale già inserite Il servizio è attivo chiamando il numero verde 800405800, postselezione 3, dal lunedi al venerdi, dalle ore 9.00 alle 18.30.
Posta Elettronica Certificata	Il canale di posta certificata viene utilizzato per le seguenti richieste: • SOSPENSIONE dell'identità digitale • REVOCA dell'identità digitale • RIATTIVAZIONE dell'identità digitale Qualora un titolare o un incaricato intenda fare una delle attività sopra descritte, potrà formalizzare la richiesta, inviando una comunicazione via pec alla casella di posta certificata di Trust Technologies in qualità di Identity Provider.
 **E-mail**	Il canale e-mail viene utilizzato nelle seguenti operazioni: • REGISTRAZIONE L'utente che richieda un'identità digitale si collega al portale dedicato ed effettua la preregistrazione. A completamento riceve una e-mail nella quale viene indicato il link per la conferma della richiesta. • ADESIONE L'utente conferma la richiesta di adesione al servizio e riceve una e-mail a conferma dei dati riepilogativi della registrazione e le altre informazioni necessarie alla successiva fase di identificazione. • IDENTIFICAZIONE L'utente sceglie la tipologia d'identificazione tra quelle disponibili e sulla base della scelta effettuata riceve le informazioni per completare la fase d'identificazione. Nel caso l'utente abbia richiesto l'identificazione utilizzando la firma elettronica qualificata o digitale e l'esito delle verifiche fosse negativo, riceverà una mail con le motivazioni del rigetto e l'eventuale richiesta di ulteriore documentazione. • CONSEGNA e RIGENERAZIONE CREDENZIALI La consegna delle credenziali di Livello 1 (UserID) avviene attraverso una comunicazione via e-mail, all'indirizzo dichiarato e verificato in fase di Registrazione. Le procedure di recupero della Userid o della Password dimenticate utilizzano la e-mail come elemento di sicurezza per la verifica della provenienza della richiesta.



Interfaccia Web

Viene resa disponibile all'utente un'interfaccia WEB che consente di eseguire in maniera guidata le fasi finalizzate al rilascio dell'identità digitale di seguito elencate:

- PRE-REGISTRAZIONE
- REGISTRAZIONE
- ADESIONE AL SERVIZIO
- VISUALIZZAZIONE DATI ANAGRAFICI
- MODIFICA DATI ANAGRAFICI
- CAMBIO PASSWORD
- VISUALIZZAZIONE ULTIMI ACCESSI
- GESTIONE NOTIFICHE EMAIL

Trust Technologies

www.trusttechnologies.it

Sito istituzionale Trust Technologies

Trust Technologies in qualità di Identity Provider mette a disposizione il proprio sito istituzionale raggiungibile all'indirizzo www.trusttechnologies.it all'interno del quale è possibile consultare la seguente documentazione:

- DESCRIZIONE DEL SERVIZIO SPID (Credenziali uniche di accesso ai Servizi di pubbliche amministrazioni e soggetti privati aderenti)
- CARTA DEI SERVIZI
- MANUALE OPERATIVO

disponibili alla pagina dedicata del sito istituzionale http://www.trusttechnologies.it/SPID.