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

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.** 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 o 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 nuovo sistema 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 si predispongono pertanto a fornire online svariati servizi che fino ad oggi richiedevano la presenza fisica del richiedente presso l'ente.

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.

4 Rilascio dell'Identità Digitale

Per quanto concerne la prima area, relativa al *rilascio dell'identità digitale*, le principali fasi sono di seguito indicate:

- **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 un servizio o una risorsa.

La fase di Registrazione si compone dei seguenti passi:

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

Di seguito vengono distinti, dove necessario, i casi in cui il soggetto sia una Persona Fisica 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 un **modulo di richiesta di adesione** sia esso persona fisica o persona giuridica.

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 seguenti tabelle.

	Persona Fisica	Persona Giuridica
Attributi identificativi	Nome e Cognome	Denominazione/Ragione sociale
	Codice Fiscale	Codice Fiscale o Partita IVA (se uguale al Codice Fiscale)
	Data e Luogo di nascita	Sede Legale
	Sesso	Persona Fisica (soggetto Richiedente con potere di rappresentanza della società)
	Estremi di un documento di identità utilizzato dal soggetto Richiedente (Numero, Tipo, Emettitore, Data scadenza)	Estremi di un documento di identità utilizzato dal soggetto Richiedente (Numero, Tipo, Emettitore, Data scadenza)
		Certificazione attestante lo stato di Amministratore o rappresentante legale del soggetto Richiedente l'identità per conto della società (visura camerale o, in alternativa, atto notarile di procura legale)

	Persona Fisica	Persona Giuridica
Attributi secondari	UserID	UserID
	Numero di cellulare	Numero di telefono fisso
	Email	Numero di cellulare
	Indirizzo di residenza	Email
	Indirizzo di Domicilio (se diverso dalla residenza)	Domicilio fisico (se diverso dalla Sede legale)

Il Portale effettua verifiche formali sui dati inseriti dal Richiedente e procede al salvataggio dei dati generando un *Codice di Registrazione* che il Richiedente dovrà utilizzare per completare la procedura di Registrazione.

Infine viene inviato al Richiedente una e-mail contenente un link – con validità limitata nel tempo – per confermare la richiesta di adesione. Il Portale convalida la richiesta e propone al Richiedente la scelta della modalità di Identificazione desiderata tra quelle disponibili.

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 ad identificare una persona fisica o giuridica per uno specifico livello di sicurezza di autenticazione informatica in ambito SPID.

Le modalità di identificazione predisposte dal Gesore 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,
- "*informatica*", mediante utilizzo della propria carta CNS per attestare 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 di identificazione il Richiedente si reca presso un Punto di Registrazione (PdR) del Gestore e viene identificato '*de visu*' ossia di persona tramite esibizione a vista di un valido documento d'identità e della propria Tessera Sanitaria (come evidenza del codice fiscale).

Nel caso di persona giuridica, verrà inoltre richiesto al Richiedente di esibire la documentazione attestante lo stato di Amministratore o Rappresentante legale del soggetto Richiedente l'identità per conto della società (**visura camerale** o, in alternativa, copia dell'atto notarile di procura legale) e l'Incaricato del Gestore presso il PdR dovrà verificare la validità[1] della documentazione fornita dal Richiedente.

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), 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 della Carta Nazionale dei Servizi (CNS)

In questa modalità di identificazione il Richiedente opera in autonomia collegandosi via web al servizio online predisposto dal Gestore, mediante la propria Carta Nazionale dei Servizi (CNS) attesta la veridicità degli attributi identificativi dichiarati in fase di registrazione ed esprime la propria volontà di adesione al servizio.

[1] Per la visura:
- che la data visura sia stata emessa entro i 15 giorni antecedenti alla data di presentazione della richiesta;
- che il richiedente figuri nella visura quale soggetto dotato dei poteri di rappresentanza legale della Persona Giuridica indicata nella richiesta.

Per l'atto notarile di procura legale:
- che gli estremi di riferimento del notaio riportati nell'atto sia coerenti con i dati presenti nell'Albo Unico professionale elettronico (art.3, DPR 137/2012) presente all'indirizzo http://www.notariato.it/it/trova-notaio;
- che l'atto notarile attesti che il richiedente è dotato dei poteri di rappresentanza legale della Persona Giuridica indicata nella richiesta.

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.

4.1.2.4 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).

Nel caso di persona fisica, 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).

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 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 in cui l'identificazione sia stata effettuata '***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[2] in sostituzione dei controlli automatici;
c. corrispondenza tra documenti identificativi presentati e presenza fisica del richiedente;
d. verifica del numero di cellulare, dichiarato dal Richiedente in fase di registrazione, mediante invio codice OTP via SMS che viene utilizzato per convalidare i dati identificati;
e. 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;
f. per le Persone Giuridiche, verifica validità[1] 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.

Tali verifiche vengono svolte dal Gestore o da personale Incaricato dal Gestore stesso. Al termine delle verifiche viene convalidata o meno la registrazione.

Nel caso in cui l'identificazione sia stata effettuata ***mediante l'utilizzo 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[2], in sostituzione dei controlli automatici;

[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.

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[1] 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 in cui l'identificazione sia stata effettuata ***mediante l'utilizzo della carta CNS o CIE***, presso il Gestore si procede alla verifica dell'identità e delle informazioni presenti nel Modulo di Adesione attestato digitalmente inviato dal Richiedente, mediante:

a. controlli automatici (applicativi) sulle banche dati oggetto delle convenzioni;

b. controlli manuali su fonti autoritative[2], in sostituzione dei controlli automatici;

c. verifica validità attestazione 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 CNS o CIE);

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 carta CNS o CIE - come persona fisica - dell'Amministratore o del legale rappresentante;

f. per le Persone Giuridiche, verifica validità[1] 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 in cui l'identificazione sia stata effettuata ***mediante l'utilizzo di Sistemi 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[3] in sostituzione dei controlli automatici;

c. corrispondenza e validità dei documenti identificativi indicati dal Richiedente;

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. verifica integrità/qualità della registrazione audio-video;

f. ulteriori altre verifiche che si rendessero necessarie.

Al termine della verifica viene convalidata o meno la registrazione.

[3] 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.

4.1.4 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[4].
- ***Livello 3***: N/D[5]

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

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**: 5
- **Caratteri usati**: numerico

[4] 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.

[5] Attualmente non commercializzato da TITT.

- **Limite di validità temporale**: 10 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 email, utilizzando l'indirizzo email 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 le tipologie di browser indicate nella seguente tabella, che riporta le versioni minime necessarie per accedere al servizio SPID:

Browser	Versione
Internet Explorer	10 (e successive)
Firefox	34 (e successive)
Chrome	31 (e successive)
Safari	7.1 (e successive)
Opera	26 (e successive)

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 **timeout** per inattività della **richiesta di autenticazione** pari a **5 minuti**, dopodichè è necessario procedere ad una nuova richiesta.

Il servizio prevede un **timeout per inattività** della **sessione autenticata** pari a **60 minuti**, dopodichè 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** (dopodichè 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 **timeout** per inattività della **richiesta di autenticazione** pari a **5 minuti**, dopodichè 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**.

5.2 Visualizzazione delle attività

L'Utente ha la possibilità, accedendo all'interfaccia web del servizio, di visualizzare direttamente un report dell'utilizzo effettivo della propria identità digitale.

Per visualizzare i dati di utilizzo è richiesta l'autenticazione almeno a livello 2 SPID.

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 Modifica dell'identità digitale (attributi e credenziali)

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

6.1.2 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 email 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.

6.1.3 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/o la ri-emissione delle credenziali possono essere effettuati utilizzando la stessa procedura di modifica indicata al par. 6.1.2.

6.2 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 (Persona fisica o giuridica)**. 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 e copia del documento di identità in corso di validità ovvero 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 e copia del documento di identità in corso di validità ovvero 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 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.

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 i 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 avranno 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.

Nei casi di furto o smarrimento del dispositivo SSCD, il Gestore si impegna ad eseguire la **revoca tempestivamente** all'atto della ricezione della 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).

6.3 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 **richiesta dell'Incaricato**,
- su **iniziativa del Gestore**.

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

- sospensione **telefonica** chiamando il Numero Verde dedicato per l'Help Desk;
- 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 e copia del documento di identità in corso di validità ovvero copia della denuncia di suo furto o smarrimento;
- richiesta inviata tramite fax 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. Successivamente, sarà cura del richiedente inviare la richiesta cartacea, tramite Posta ordinaria, presso la sede del Gestore.

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

La ***sospensione da parte dell'Incaricato*** 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 e copia del documento di identità in corso di validità ovvero copia della denuncia di suo furto o smarrimento;
- richiesta inviata tramite fax 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. Successivamente, sarà cura del richiedente inviare la richiesta cartacea, tramite Posta ordinaria, presso la sede del Gestore.

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).

L'Utente o l'Incaricato che intenda ottenere la sospensione di una identità digitale deve inoltrare regolare richiesta di sospensione secondo le modalità descritte sopra. Il Gestore effettua la sospensione non appena riceve la richiesta.

Nella richiesta di sospensione telefonica il Titolare deve seguire la procedura seguente:

- L'Utente contatta il numero verde **800.405.800** dedicato per l'Help Desk,
- L'Operatore dell'Help Desk richiede informazioni anagrafiche all'utente (ad esempio: nome, Cognome, Codice Fiscale, Data di nascita, etc.),
- L'Utente fornisce i dati richiesti dall'Operatore,
- L'Operatore dell'Help Desk inserisce i dati in una maschera di ricerca sul Portale messo a disposizione dal Gestore,
- Il Portale visualizza i risultati della ricerca:
    - se si individua l'Identità Digitale da sospendere, la procedura prosegue,
    - altrimenti vengono reiterati i punti da 2 a 4 fino a che non venga individuata univocamente una identità digitale.

La procedura varia poi a seconda della disponibilità – da parte dell'utente – di telefono cellulare e/o email, dichiarati e verificati in fase di registrazione:

- Se l'Utente ha la disponibilità del telefono cellulare:
    - L'Help Desk invia un codice "*one-shot*" via SMS al numero di telefono cellulare, utilizzando le funzionalità messe a disposizione dal Portale del Gestore (l'operatore di Help Desk non ha visibilità dell'sms inviato),
    - L'Utente fornisce telefonicamente all'Operatore dell'Help Desk il codice "*one-shot*" ricevuto via SMS,
    - L'Operatore dell'Help Desk verifica la validità del codice "*one-shot*" utilizzando le funzionalità messe a disposizione dal Portale del Gestore,
    - L'Operatore dell'Help Desk procede alla sospensione dell'Identità Digitale utilizzando le funzionalità messe a disposizione dal Portale del Gestore;
- Se l'Utente non ha la disponibilità del telefono cellulare, ma soltanto della email:
    - L'Operatore dell'Help Desk invia un codice "*one-shot*" all'indirizzo email utilizzando le funzionalità messe a disposizione dal Portale del Gestore (l'operatore di Help Desk non ha visibilità dell'email inviata),
    - L'Utente fornisce telefonicamente all'operatore di Help Desk il codice "*one-shot*" ricevuto via email,
    - L'Operatore dell'Help Desk verifica la validità del codice "*one-shot*" utilizzando le funzionalità messe a disposizione dal Portale del Gestore,
    - L'Operatore dell' Help Desk procede alla sospensione dell'Identità Digitale utilizzando le funzionalità messe a disposizione dal Portale del Gestore;
- Se l'Utente non ha la disponibilità né del telefono cellulare né della mail:
    - La sospensione telefonica non può essere effettuata.

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 avranno 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).

6.4 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 **richiesta dell'Incaricato**
- 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.
- richiesta inviata tramite fax contenente richiesta con firma autografa e copia del documento di identità in corso di validità ovvero copia della denuncia di suo furto o smarrimento. Successivamente, sarà cura del richiedente inviare la richiesta cartacea, tramite Posta ordinaria, presso la sede del Gestore.

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.

Le richieste di **riattivazione da parte dell'Incaricato** sono accettate qualora pervengano al Gestore tramite email oppure fax, e contengano:

- esplicita dichiarazione della volontà di riattivare l'identità digitale,
- la motivazione della richiesta di riattivazione e la decorrenza richiesta,
- i seguenti dati anagrafici del titolare dell'Identità Digitale:
  - nome e cognome,
  - data e luogo di nascita,
  - Codice Fiscale,
  - indirizzo di residenza (costituito da via, numero civico, CAP, comune di residenza),
  - fotocopia di un documento di riconoscimento (ove richiesta nei casi precedentemente descritti).

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 avranno 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).

6.5 Visualizzazione delle attività

L'Utente ha la possibilità, accedendo all'interfaccia web del servizio, di visualizzare direttamente un report delle modifiche effettuate alla propria identità digitale. utilizzo effettivo della propria identità digitale.

Per visualizzare i dati di utilizzo è richiesta l'autenticazione almeno a livello 2 SPID.

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 le circostante, utilizzando le modalità indicate nella Guida utente o nel Manuale operativo del servizio.

Ai sensi dell'art. 13 del D.Lgs. del 30 giugno 2003, n. 196, "**Codice in materia di protezione dei dati personali**" (in seguito denominato Codice), e in relazione ai dati personali che si intendono trattare, La informiamo di quanto segue:

1. Il trattamento cui saranno sottoposti i dati, richiesti o acquisiti, è diretto esclusivamente all'espletamento da parte di TI Trust Technologies S.r.l. delle finalità attinenti all'esercizio delle attività di emissione e gestione dell'Identità Digitale in ambito Sistema Pubblico per la gestione dell'Identità Digitale (SPID), come istituito e normato dal D. Lgs. 82/2005 "Codice dell'Amministrazione digitale", dal DPCM del 24/10/2015 (GU n.285 del 9122014) e dalla normativa di attuazione, nonché per adempiere ad eventuali obblighi previsti dalla legge, dai regolamenti o dalla normativa comunitaria.
2. Il trattamento dei dati personali può essere effettuato anche con l'ausilio di mezzi elettronici o comunque automatizzati e può consistere in qualunque operazione o complesso di operazioni tra quelle indicate all'art. 4, comma 1 lettera a) del Codice.
3. Il conferimento dei dati personali è facoltativo, salvo che sia richiesto da specifiche normative.
4. L'eventuale rifiuto di conferire i propri dati può comportare l'impossibilità di stipulare o di eseguire il contratto di erogazione dei servizi sopra menzionati.
5. All'interno di TI Trust Technologies S.r.l. i dati personali sono trattati da personale nominato "Incaricato del trattamento" da parte di TI Trust Technologies S.r.l..
6. I dati personali possono essere comunicati, per le medesime finalità di cui al punto 1), ai Gestori sostitutivi accreditati presso l'Agenzia per l'Italia Digitale in caso di cessazione dell'attività da parte di TI Trust Technologies S.r.l. e al solo fine di assicurare la continuità del servizio (D. Lgs. 82/2005, art. 12).

7. Escludendo ogni finalità di trattamento per scopi diversi da quelli di cui al punto 1) direttamente e tecnicamente connessi all'erogazione dei servizi, i dati personali possono essere comunicati ai seguenti soggetti:
   a. alle società del Gruppo cui TI Trust Technologies S.r.l. appartiene (società controllanti, controllate e collegate, anche indirettamente ai sensi delle vigenti disposizioni di legge) e a soggetti terzi;
   b. a Pubbliche Amministrazioni ai sensi di legge;
   c. all'Autorità Giudiziaria in seguito a sue precise richieste.
8. I dati personali non sono soggetti a diffusione.
9. Sempre per le medesime finalità di cui al punto 1) i dati personali possono essere trasferiti al di fuori del territorio nazionale alle condizioni e con le garanzie di cui al Codice.
10. L'art. 7 del Codice conferisce all'interessato l'esercizio di specifici diritti, tra cui:
    a. ottenere dal titolare la conferma dell'esistenza o meno di propri dati personali e la loro comunicazione in forma intelligibile;
    b. avere conoscenza dell'origine dei dati, nonché della logica e delle finalità su cui si basa il loro trattamento;
    c. ottenere la cancellazione, la trasformazione in forma anonima o il blocco dei dati trattati in violazione di legge, nonché l'aggiornamento, la rettificazione o, se vi è interesse, l'integrazione dei dati;
    d. di opporsi, per motivi legittimi, al trattamento.
11. Il Titolare del trattamento dei Suoi dati personali è TI Trust Technologies S.r.l., con sede in SR 148 Pontina km 29,100 – 00071 Pomezia (RM); il Responsabile dei trattamenti medesimi è la Dott.ssa Cinzia Villani, domiciliata presso la stessa sede. Per ulteriori informazioni sul tema del trattamento dei dati personali si può fare riferimento a quanto indicato sul sito: http://www.trusttechnologies.it.

8 Riferimenti del Gestore

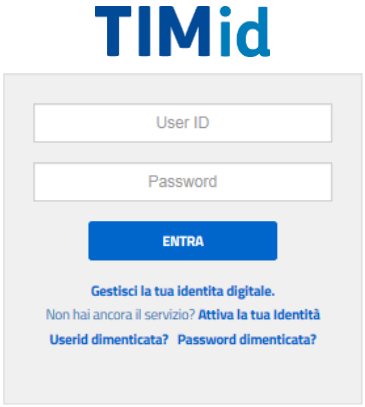
Riferimenti	
Sede Legale:	S.S. 148 Pontina km. 29,100 – 00071 Pomezia (Roma)
Indirizzo PEC:	TI.TT@ttpec.telecomitalia.it
Indirizzo di Posta elettronica:	info-ttstore@telecomitalia.it
Numero fax:	06.91197331

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 Nuvola 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 Qualora un titolare intenda procedere ad una delle attività sopra elencate, potrà chiamare il Numero Verde dedicato per l'Help Desk e richiedere supporto telefonico su "Inserimento di una Richiesta di Emissione" | "Sospensione telefonica" | "Verifica stato d'avanzamento di una Richiesta di Emissione" | dell'Identità Digitale, seguendo la indicazioni dell'operatore Help Desk.
 **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 email 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 CODICI La consegna delle credenziali di Livello 1 (UserID) avviene attraverso una comunicazione via email, all'indirizzo dichiarato e verificato in fase di Registrazione. La consegna delle credenziali a seguito di una richiesta di reset avviene attraverso una comunicazione via mail.

 **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.